# International Radio Security Services Application Programming Interface Functional Requirements: Analysis, Development and Specification for an International Radio Security Services API Set

**Document WINNF-13-S-0004**

Version V1.0.0
13 June 2013

# TERMS, CONDITIONS & NOTICES

This document has been prepared by the IRSS API Work Group to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter “the Forum”). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the IRSS API Work Group.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter’s copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum’s participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

# Table of Contents

TERMS, CONDITIONS & NOTICES ........ i
1 Introduction ........ 1
1.1 Scope ........ 1
1.2 Background ........ 1
1.3 High level radio features in military environments ........ 2
1.3.1 Data Transport Availability ........ 2
1.3.2 Seamlessness and flexibility ........ 3
1.3.3 Authentication and Protection ........ 3
1.3.4 Domain neutrality ........ 3
1.4 Approach ........ 3
1.5 Radio Platform and Waveform Security Policies –API Implications ........ 5
1.6 Structure of this document ........ 6
2 Actors and Roles for Use Case Analysis ........ 6
3 Waveform Examples ........ 15
3.1 Introduction ........ 15
3.1.1 Applicable Radio Security Services ........ 16
3.1.2 SCA Considerations for the API ........ 19
3.2 Security Architecture Independence ........ 19
3.3 Military/Government Waveforms ........ 22
3.3.1 IP Based Ad Hoc Networking (IPBAHN) Waveform ........ 24
3.3.2 TDMA SATCOM Waveform ........ 35
3.3.3 UHF TACSAT Waveform ........ 42
3.3.4 HF 2G/3G ALE Waveform ........ 50
3.3.5 VHF/UHF LOS Waveform ........ 58
3.4 Public Safety Waveforms ........ 68
3.4.1 P25 Waveform ........ 68
3.4.2 TETRA (Future Work Group Objective) ........ 78
3.5 Commercial SATCOM Waveforms (Future Work Group Objective) ........ 78
3.6 Commercial Terrestrial Waveforms (Future Work Group Objective) ........ 78
4 API Use Case Operations Usage Overview ........ 79
4.1 Platform Use Case API Operations ........ 79
4.1.1 PF 01 - Install/Uninstall/Manage cryptographic algorithms ........ 81
4.1.2 PF 02 - Update/Load/Fill/Manage Keys ........ 82
4.1.3 PF 03 - Zeroize Key(s) ........ 82
4.1.4 PF 04 - Install/Manage/Replace Trust Anchor(s) ........ 82
4.1.5 PF 05 - Zeroize Trust Anchor ........ 83
4.1.6 PF 06 - Load/Fill/Manage Certificate(s) ........ 83
4.1.7 PF 07 - Zeroize Certificate(s) ........ 83
4.1.8 PF-08 Load/Fill/Manage User/Device/Entity Credentials ........ 83
4.1.9 PF 09 - Zeroize Credentials ........ 84
4.1.10 PF 10 - Install/Uninstall/Manage waveform/application/platform resident software 84
4.1.11 PF 11 - Install/Uninstall/Manage waveform/application/platform resident software Update 84

4.1.12 PF 12 - Install /Update/ Uninstall/Manage waveform/application/platform Policy/Policies ....84
4.1.13 PF 13 - Platform Operating Environment boot (Includes all Radio Security Services) ....85
4.1.14 PF 14 - Instantiate/De-instantiate Waveform/Application Software ....85
4.1.15 PF 15 - Start/Stop Waveform ....85
4.1.16 PF 16 – OTAZ Platform ....85
4.1.17 PF 17 - OTAR Platform ....86
4.1.18 PF 18– Install, Retrieve and Update Compromised Key Lists (CKLs) and Certificate Revocation Lists (CRLs) ....86
4.1.19 PF 19 - Install/Update Platform Operating Parameters ....86
4.1.20 PF 20 - Install/Update Channel Operating Parameters ....87
4.1.21 PF 21 - Setup/teardown Platform Encryption/Decryption Channels ....87
4.1.22 PF 22 - Encrypt/Decrypt User Data/Platform Data/Files/applications ....87
4.1.23 PF-23 Request CSF Authenticate User/Device/Entity and Authorize Operations 87
4.1.24 PF 24 - User Authentication (with/without physical token) ....88
4.1.25 PF 25 - Local or Remote Device/ Entity Authentication ....88
4.1.26 PF 26 - Manage Security Faults/Alarms ....88
4.1.27 PF-27 Report/Manage Auditable event/alarm condition ....89
4.1.28 PF 28 - Manage/Review/Extract Audit Log(s) ....89
4.1.29 PF-29 - Platform Memory Resource Management enforcement/enablement ....89
4.1.30 PF-30 Software/Firmware Management ....89
4.1.31 PF-31 Logging, Auditing and Security Alarm Services ....89
4.2 Waveform Operations ....90
4.2.1 WF 01 - Setup (configure)/teardown waveform Control Channels ....93
4.2.2 WF 02 - Update Waveform Policy ....93
4.2.3 WF 03 – OTAR/OTAT (Waveform specific) ....94
4.2.4 WF 04 - OTAZ (Channel specific keys/Certs) ....95
4.2.5 WF 05 - Extract/Forward Audit Log ....95
4.2.6 WF 06 - Setup (configure)/teardown Waveform Encryption/ Decryption Channels ....96
4.2.7 WF 07 – Change Algorithm Selection ....96
4.2.8 WF 08 – Change Key Selection ....97
4.2.9 WF 09 – Reserved ....97
4.2.10 WF 10 - Key Negotiation / Session Establishment ....97
4.2.11 WF 11 - Encrypt / Decrypt User Traffic ....97
4.2.12 WF 12 – Setup (configure)/teardown Waveform TRANSEC Channels ....97
4.2.13 WF 13 - Perform TRANSEC Operations ....98
4.2.14 WF 14 - Provide TRANSEC Keystream ....98
4.2.15 WF 15 - Provide/Generate Random Number ....98
4.2.16 WF 16 - Provide TRANSEC Key ....99
4.2.17 WF 17 – Setup (configure)/teardown Waveform Bypass Channels ....99
4.2.18 WF 18 - Plain Audio Text Bypass ....100
4.2.19 WF 19 - Control Bypass ....100
4.2.20 WF 20 – Header or In-channel Bypass ....100

4.2.21 WF 21 - Setup (configure)/teardown Waveform Authentication/Integrity Channels ........ 101
4.2.22 WF 22 - Authenticate Remote Device/Application ........ 101
4.2.23 WF 23 - Authenticate Local/Remote User (with/without physical token) ........ 102
4.2.24 WF 24 – Authenticate Local Device/ Application ........ 103
4.2.25 WF 25 – Authenticate file/token/data/certificate ........ 104
4.2.26 WF 26 - Integrity Check file/token/data/certificate ........ 104
4.2.27 WF 27 - Provide Digital Signature for file/token/data ........ 105
4.2.28 WF 28 - Provide Hash for file/token/data ........ 105
4.2.29 WF 29 - Verify Hash for file/token/data ........ 106
4.2.30 WF 30 - Retrieve Certificate (s) ........ 106
4.2.31 WF 31 - Accept/pass in Certificate ........ 106
4.2.32 WF 32 Encrypt/Decrypt File/Token/Data ........ 107
5 Requirements in Support of Waveform Security Operations ........ 108
5.1 General Requirements Related to the Waveform IRSS API ........ 114
5.2 Radio Security Services API Requirements ........ 116
5.2.1 Access Control, Identification & Authorization Services ........ 116
5.2.2 Authentication, Integrity and Non-repudiation Services ........ 118
5.2.3 Information Integrity Services ........ 126
5.2.4 Information Security (INFOSEC) Bypass and Confidentiality Services including encryption and decryption ........ 126
5.2.5 Transmission Security (TRANSEC) Services ........ 131
5.2.6 Key and Credential Management Services ........ 135
5.2.7 Platform Resource Security Management Services ........ 139
5.2.8 Logging, Auditing and Security Alarm Services ........ 139
5.2.9 Policy Enforcement and Management Security Services ........ 142
Appendix A: Abbreviations ........ 145
Appendix B: Glossary ........ 148

# List of Figures

Figure 1: IRSS API Development Process ........ 4
Figure 2 Alternative Forms for SDR Security Functional Architectures ........ 21
Figure 3: Cryptographic Channel Configurations ........ 24
Figure 4: Dynamic formation of Community of Interests ........ 59
Figure 5: Potential layers of (confidentiality) protection ........ 60
Figure 6: High level overview on the security components in a combat radio ........ 60
Figure 7: Project 25 Reference Model ........ 70
Figure 8: Project 25 Protocol Stacks ........ 71

# List of Tables

Table 1: Actor/Role List For a Tactical Radio Security Services API ........ 7
Table 2: Entry Descriptions for Waveform RSS tables ........ 16
Table 3: SDR Device Security Service Classes ........ 17
Table 4: IPBAHN Waveform - Applicable API Use Case Operations ........ 33
Table 5: TDMA SATCOM Waveform - Applicable API Use Case Operations ........ 40
Table 6: UHF TACSAT Waveform - Applicable API Use Case Operations ........ 49

Table 7: HF 2G/3G Waveform - Applicable API Use Case Operations ...................................... 56
Table 8: VHF/UHF LOS Waveform - Applicable API Use Case Operations.............................. 67
Table 9: P25 Waveform - Applicable API Use Case Operations ................................................. 76
Table 10: Platform Use Case API Operations Summary.............................................................. 80
Table 11 Waveform Applicable API Use Case Operations Summary ......................................... 91
Table 12: Waveform Security Service Needs Summary ........................................................... 110

# International Radio Security Services Application Programming Interface Functional Requirements: Analysis, Development and Specification for an International Radio Security Services API Set

## 1 Introduction

The purpose of this document is develop and provide a functional requirements specification that can be applied to the development of an Application Programming Interface (API) for Radio Security Services (RSS) for use in radios in the international marketplace. These include commercial radio applications, public safety applications and tactical radio applications, the latter of which is perhaps the most demanding from a security perspective and consequently will be the primary focus of this document. Such radios are here-after referred to as an International Tactical Radio (ITR). The resultant API, although developed with the ITR focus, represents a superset of capabilities for which only a subset may be needed for other radio applications such a public safety, commercial satellite and other commercial radio applications. This is supported in part by the results of the Project 25 API requirements analysis presented here-in. At the present time there has not been any contributions made to this document regarding the requirements analysis for any commercial waveform/application and thus those specific aspects have been deferred for future work. However as will be seen, the military radio market makes extensive use of commercial security standards developed for application to the global internet. Thus features of the resultant API that address those security functions should be directly application to commercial applications.

### 1.1 Scope

For the present time, this document will only consider examples which are relevant to defining the Application Programming Interface in support of waveform or other application portability. Thus those Radio Security Services API's which are specific to the underlying radio platform and are independent of waveform/application portability and interoperability will not be addressed in depth. Notwithstanding, different security architectures may relegate RSS API functions to a waveform API or to a platform API. Consequently the API's developed shall consider when such circumstances might occur so that an appropriate waveform API may be specified.

The basis for the definition and identification of the Radio Security Services classes referenced in this document are derived from the Wireless Innovation Forum (WINNF, WInnForum) Security Working Group Document WINNF-08-P-0013-V1.0.0 Securing Software Reconfigurable Communications Devices (Available for download at: http://groups.winnforum.org/p/cm/ld/fid=84).

### 1.2 Background

The Radio Security Services API's that will result from the requirements derived and specified within this document are intended to function in accordance with the requirements and operating environment specified by the Software Communications Architecture (SCA) standards and the related published APIs based there-on. During the evolution of the SCA, the Radio Security

Services (RSS), which had been the only API provided in the original SCA, was removed because all other APIs were separately defined. However, after removal from the SCA the published RSS API was not publicly released, which is also the case with some other Joint Tactical Radio System (JTRS) APIs. Since radio security services are an essential component of any tactical radio, the Wireless Innovation Forum undertook the development of an open standards API for use by the international radio community. The production of this document is part of that effort.

The SCA was originally developed for the JTRS program and is being used by all radio platforms developed under that program. The standard was socialized to the commercial world by the US Department of Defense to foster their desire for the standard to be adopted as a commercial standard. The Wireless Innovation Forum, known then as the Software Defined Radio Forum was approached by the DoD and consequently, had a significant role during the development of the initial SCA.

After the initial release of the SCA a version was eventually standardized by the Object Management Group. During this process it was realized that the DoD needed to maintain control of the standard in order to manage costs of ongoing development programs and that was not possible with the OMG or any other open standards body. The DoD currently maintains and manages all revision control on the standard but welcomes input from all of industry regardless of whether or not they are developing radios for the DoD.

The WInnForum has undertaken an active role representing International commercial interests to harmonize the needs of commercial developers and fostering the evolution of the SCA and related APIs[1]. In 2010 the WInnForum established a new technical committee known as the Coordinating Committee on International SCA Standards. In February of 2012, the JTRS Joint Program Executive Office and the WInnForum jointly approved SCA version 4.0[2].

## 1.3 High level radio features in military environments

It is essential that the examples considered and the API’s to be developed are fully capable of supporting the following high level features found in contemporary and emerging tactical radio networks.

### *1.3.1 Data Transport Availability*

In this modern world of ours we place great trust in the availability and reliability of the communication networks we utilize. Ironically, in the tactical environments where our war fighters need it most, supporting infrastructure is least established, if any exists at all, and it is subjected to electronic warfare as well as direct physical attacks by adversarial forces. Notwithstanding, our war fighters are relying on communication links whose performance and availability can be maintained with high assurance. Security services in the area of Information Security (INFOSEC) and Transmission Security (TRANSEC) are integral to the ability of waveforms to meet the challenges encountered on today’s battlefields.

[1] http://www.wirelessinnovation.org/what_is_the_sca
[2] http://www.wirelessinnovation.org/assets/documents/CC_SCA_Charter_V2_0_0_-_16_November_2010.pdf

### *1.3.2 Seamlessness and flexibility*

Future operations will be less geographically less static and more dynamic in terms of mission tasking. Soldier's mobile devices will connect and disconnect frequently to different infrastructure hosted by several management authorities. Terminals need to support this mode, where end users are dynamically connected to different bearers as they dynamically and seamlessly create new networks in support of coalition operations. In particular the feature of communicating securely with constantly changing Communities of Interests (CoI), and Dynamic Communities of Interests (DCoI) will entail additional requirements on the cryptographic components in the terminal and their Application Programming Interfaces. As an example, dynamic group keying or IPsec discovery can be utilized to support DCoIs in their communication.

### *1.3.3 Authentication and Protection*

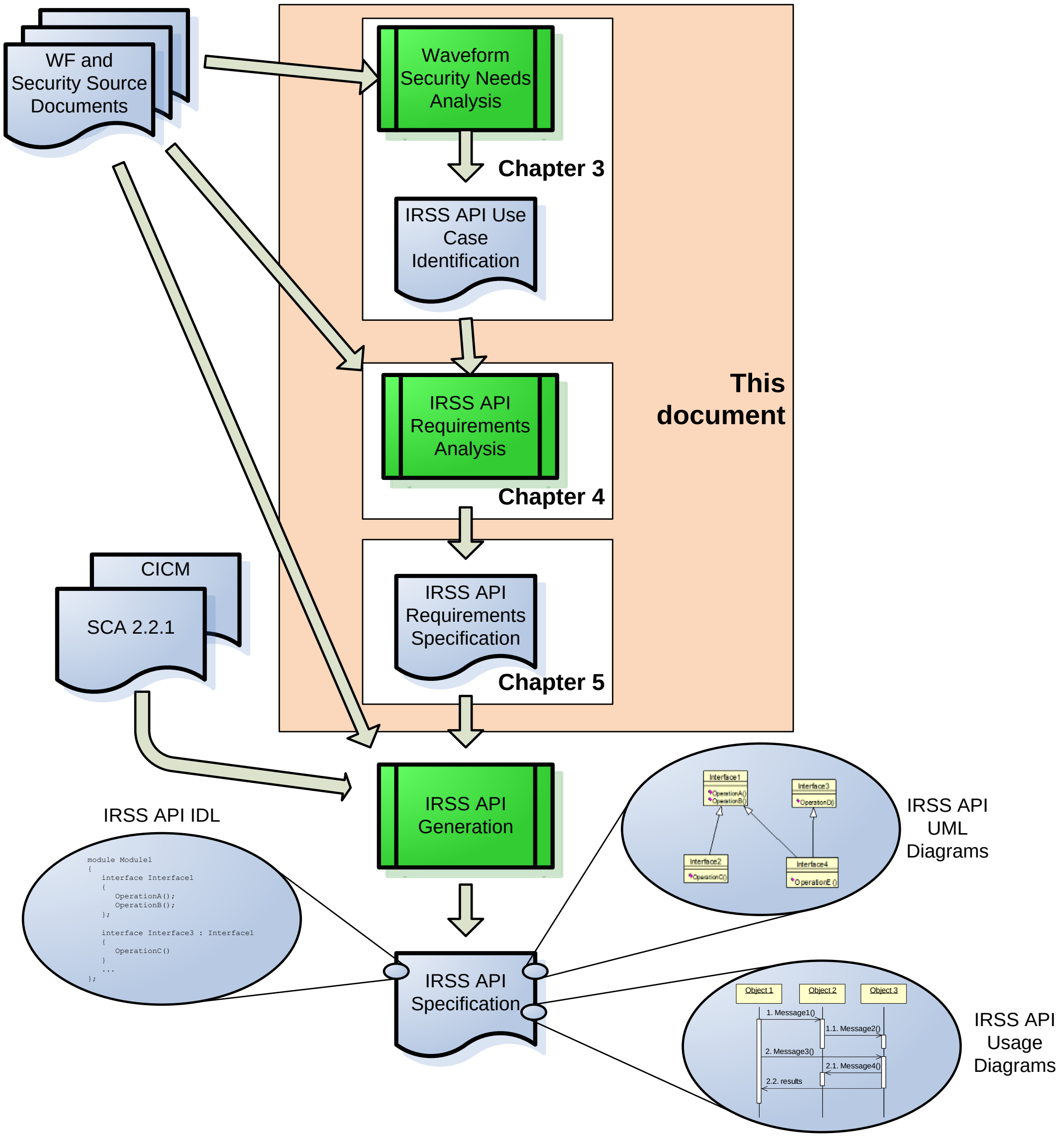
Tactical radio links need to be protected from unauthorized access and traffic analysis by hostile forces. In addition, Quality of Service (QoS) mechanisms should ensure that data is transferred with the priority and reliability it deserves. Trust in the peer terminals and their users must be assured at all times. Thus robust authentication schemes must be in place which can accommodate constantly changing DCoIs.

### *1.3.4 Domain neutrality*

Mission participants will have the need to communicate quickly among different security domains, such as into their 'core'-mission domain, their national back-end, with other mission member nations including both allied and non-allied coalition force members, and potentially various Civilian-Military Cooperative (CIMIC) parties, etc. Key to these aspects is the fact that today’s tactical radio cryptographic module, in addition to being software upgradeable to accommodate new waveforms, must also provide the capabilities of simultaneously supporting multiple keys, different encryption algorithms and multiple encryption equipment protocols for a specified channel.

## 1.4 Approach

The final technical document delivery of the task group will be the detailed Radio Security Services API specification for the security functions of an International Tactical Radio necessary to support waveform portability and interoperability among multinational platforms. The steps in order to achieve this objective are listed below and illustrated in Figure 1.



```
module Module1
{
   interface Interface1
   {
      OperationA();
      OperationB();
   };

   interface Interface3 : Interface1
   {
      OperationC()
   }
   ...
};
```

**Figure 1: IRSS API Development Process**

1) Waveform examples will be used to identify needed Security Services and to identify specific API Operations and the associated functional requirements for the API. Multiple waveform examples will be used to represent diverse security service requirements to ensure a comprehensive and complete API is developed. API operations examples will be used to define specific API components and their operational requirements leading to API definition. The results of this activity are presented in Section **3**.
2) High level functional requirements will focus on the radio security services needed by waveform components to meet their operational needs. The radio security service APIs are an abstraction which hide the underlying interfaces between the radio platform and the embedded crypto module with the aim to make the waveform API agnostic to both the

crypto module and security services implementations. The methodology will consider implications of potential transformations from the IRSS APIs to non-published regional and sovereign API's should that be necessary.

**3)** The publically released USAF API known as the Common Interface to Cryptographic Modules (CICM) and previously published Joint Tactical Radio System Software Communications Architecture Version 2.2.1 Security Supplement API will be used as source material for API development in the bottom up and top down approach[3]. The API's as defined there-in will serve as a starting point for bottom-up API development.

4) All RSS API Operations examples examined in Section **4** support the waveform RSS functional needs and serve as a basis for the IRSS functional specification requirements. The IRSS functional requirements are contained in Section **5**.

**5)** In the next stage of the overall project, the process will include a gap analysis comparing API Requirements to that which is already included in the API. From the list of requirements not yet included in the API, the IRSS API specification/standard will be modified to include those which have been selected to be included in the next revision of the specification/standard.

## 1.5 Radio Platform and Waveform Security Policies –API Implications

In an earlier Wireless Innovation Forum report, the importance and relevance of having a defined Radio Platform Security Policy (RPSP) was emphasized as was its application to the development of the security architecture and design of the Radio Platform[4]. The topic of a specific Waveform Security Policy (WSP) was not addressed within that report as it was not relevant; however, the waveform's security policy is indeed a critical component of overall system security. There are, however, no published standards for what constitutes a waveform security policy nor is there any standard regarding how such a policy is expressed or enforced either by waveform components or the radio platform on which it is instantiated. The Radio Platform security policy is likely to have explicit criteria applicable to waveforms in general, but each waveform requires security policy specific to its own application.

In this document it is required that each waveform to be ported to any given radio platform be accompanied by a Waveform Security Policy. The form in which the policy is expressed is not specified and may include a document that lists the policy statements, as well as specific design criteria for porting the waveform to any given platform. We do not intend to fully define the components of a WSP in this document, however, we do include a minimum criteria that the waveform security policy must include a complete listing of the API services that it requires as well as explicit identification of the extent which each such service is used and which aspects are not used/needed by the waveform.

It is expected that the Radio Platform will enforce the WSP to the extent required by its own RPSP.

These aspects are reflected in the API requirements in Section 5.

[3] Note: The SCA no longer includes any API's as part of the document. API's are published separately. The JTRS RSS API is among several that have not been published.

[4] "Securing Software Reconfigurable Communications Devices", Document WINNF-08-P-0013-V1.0.0, http://groups.winnforum.org/d/do/3014

## 1.6 Structure of this document

The main purpose of this document is to facilitate and embrace the first important phases of the approach described in Section 1.4 above and to clearly determine the development framework. For this reason the following structure is chosen:

1) Section **2** identifies various actors or roles of entities interacting with the radio. These are entities such as individuals acting in specific roles, devices, device components, and network components that may play a role in various high level and low level use case analysis.

2) Section **3** gives an overview of the Waveforms which are the basis for the API functional security requirements developed in this report. While some are based on specific standards, others are only loosely based on known standardized waveforms. As such they have a hypothetical aspect for the security functions which are like to emerge in the next generation of waveforms. This section also identifies which of the Use case Operations in Section **4** are believed to apply to the given wave form example.

3) Section **4** lists both platform and waveform API Operations for use in defining functional use case examples. The use cases are planned to be the subject of future work and will develop specific use case examples for each waveform which requires the use of the corresponding security API operations functions.

4) Section **5** contains the high level API functional requirements organized by each Security Service class defined in Section **3** which have been derived (high-level) requirements for API's in Waveform Security Operations.

# 2 Actors and Roles for Use Case Analysis

The definition of the actors and/or roles is an important aspect in the process. As such it identifies the main players in the use case scenarios and in higher level systems analysis. They are defined at different levels of abstraction to facilitate the analysis at different levels as well as use case simplification. Details are added only when necessary to understand relevant interactions. Table 1 provides a listing and description for those Actors and/or roles identified to date.

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| Administrator | The Administrator, also known as the System Administrator is any entity that interacts with the Software Defined Radio (SDR) for general administrative or SDR management purposes including identification of authorized personnel and other entities authorized to control/manage and utilized the SDR and defines their specific role assignment. | Typically a user side entity but may reside on bearer side in some applications such as remotely managed Radio Configuration and Network management operations. Responsible for overall administration of the SDR including assignment of roles to other actors |
| Application Component | In an object oriented design an "application component" is a package, module or software based service encapsulating a logical set of functions. In the context of this document it is used to refer to Non- Radio Platform Operating Environment (RPOE) software such as a waveform software component. | An integral part of a Radio Platform Application |
| Audit Authority | Any entity who interacts with the SDR for audit log review or retrieval purposes | This actor can access SDR locally (via the Human Machine Interface (HMI)) or remotely via the communications networks Responsible for assigning audit log parameters and for reviewing audit logs. |
| Bearer Side (of) Terminal | The bearer abstraction represents every possible transport layer appropriate to transmit data directly via the supported bearer. | Unclassified or Protected data transmission/receiver interface |
| Certification Authority (CA) | The Certification Authority represents the issuer of any certificate. It is a part of a Public Key Infrastructure (PKI) system and can be used when the PKI actor does not provide sufficient detail. | One or more entities that are authorized to sign and issue certificates. |

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| Communications Service Provider | This entity provides the device with a communication or related service via radio communication links, which may include commercial wireless networks or the network infrastructure in a public safety network, broadcast satellite subscription services, and/or peers in an ad hoc network. | Communication Service Providers provide services to their users/subscribers either as a basic service (e.g. SATCOM access such as INMARSAT) or as a value added service over the network. A tactical networked radio may have access to multiple communication service providers. |
| Centralized Security Function /Cryptographic Subsystem | The Centralized Security Function provides all functionality typically provided by a legacy Cryptographic Subsystem (CSS) as well as those additional security services required by contemporary Software Defined Radio Device (SDRD) technology. As such it is the connecting actor between the consumer side (aka RED side) and the bearer side (aka BLACK side) of the tactical radio terminal. | For purposes of this document the legacy CSS, here-in referred to as a Centralized Security Function (CSF), is the source of all Radio Security Services available to the waveform component. This includes Protection layer components, such as TRANSEC, Link Security (LINKSEC), Network Security (NETSEC), Communications Security (COMSEC) and others including key management, authentication etc. |

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| Device Owner/Device Administrator | The Device Owner/Device Administrator role corresponds to the individual or an entity that desires to control which of the set of authorized or permitted communication services are enabled by the device. The Device Owner/ Device Administrator will have objectives different from the user. Administrators may wish to limit the sources, distribution, content and time of downloadable software and policies. Similarly, enterprises might provide devices to their employees but want to enforce corporate policies. In these cases, the device owner may serve as the stakeholder for the user role. | Determines policy defining scope and use of SDR operations. |
| Download Authorization Authority (DAA) | In the context of this document, the DAA is an entity with the authority to approve the download of software/firmware of a designated type. This role is defined solely within the context of enforcing security policy. | Responsible for ensuring the validity of the software/firmware to be downloaded to a radio platform |
| Key Distribution Authority/Entity | Ensures the delivery of operational key material to the intended radio units. An Interface between Key Management authority and Device, such as Over-The-Air (OTA) or Key Loading Device | Responsible for the delivery of key material to the tactical radio |
| Key Generation Authority/Entity | Generates key material in accordance with key material requests for pre-placed usage. Prepares key material for distribution | Responsible for the creation of key Material. |

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| Key Management Authority | Analyzes Operation Mission Plan and defines requirements for key material. Submits Key Material requests to Key Generator authority. | Defines Operational requirements for Key material |
| Maintainer | Any entity who interacts with the SDR for SDR maintenance purposes | Typically a user side entity but remote diagnostic operations may be performed via Bearer side. Monitors, troubleshoots and repairs SDR |
| Manufacturer | The manufacturer is the entity that assumes liability for the performance of the device, which in most cases is an integrator of hardware and software components to create a platform for radio software. In other instances governing authorities may define the responsible entity. | Designs and Manufacturers the Radio Platform |
| Mission Planner | The entity that creates and disseminates operational mission plans for the SDR and the network in which the SDR operates (but not necessarily for the external networks with which it may interact) | Plans operational mission operating parameters to meet mission requirements |
| Network Operations Authority | The Operations Authority (OA) is the direct authority for a network, e.g. a commander. It is not a computer service, but a human decision maker. | Interface to Mission Objective related radio support |
| Operator | Any entity that interacts with the SDR for purposes of operating and controlling an SDR, including radio channel configuration and operating parameter selections. This entity may also be assigned a User/communicator role. | Typically a user side entity but may reside on bearer side in some applications. Provides real time control and operation of the SDR |

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| Policy Distributor | This role parallels the Software Distributor role, because it characterize those entities which are designated as being authorized to distribute policies of a designated type to an SDRD and to components of the network in which the SDRD operates. This entity also must ensure that all platforms receive any policy update. | The entity responsible for distributing Policy to all platforms within its area of responsibility. |
| Policy Issuer | This is a broad class of roles or entities, each defined by the type and the nature of the policy being issued. Examples of such policies are regulatory policies, network security policies, network management policies, as well as individual SDRD security policies. From an SDRD security policy enforcement perspective, a Policy Issuer is an entity who is authorized to issue a corresponding type of policy. As with the preceding roles, this role is defined solely within the context of enforcing security policy. | A network entity that has the authority to create, or alter a previously established policy governing a designated aspect of radio platform operations. |
| Public Key Infrastructure | The Public Key Infrastructure is an actor that represents all activities that are related to PKI, including user registration, issue of certificates, revocation of certificates, and answering revocation inquiries. It hides the detail of a PKI system. | A general component abstraction capable of interacting with the radio platform in all matters and aspects of PKI based operations. |

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| Radio Platform | An abstraction of the SDR operating environment and services exclusive of Radio Security Services | The host for the waveform, the operating environment and all radio services |
| Radio Security Services (RSS) | The applications which provide the API service for the Cryptographic Subsystem. Depending upon the SDR system design it may or may not support platform interaction with the Crypto Subsystem. | Services which provide an interface between the waveform, other applications or other platform services which provides them the ability to obtain required security services. Components of RSS reside on both user side and bearer side of radio. |
| Registration Authority (RA) | The Registration Authority, as used, represents the control of user identity before passing a request for certificate issue to the CA. The RA is responsible for verifying that the requestor is who claims to be and that all necessary information is provided and is accurate. | One or more entities which are authorized to verify the identity of users or organizations who require certificates/digital credentials and certify their identify to certificate issuing authorities |
| Regulator/ Frequency Manager | The Regulator/Frequency Manager is the legal authority that assigns spectrum rights to communication service providers and establishes limits for safe operation of radio equipment. In some jurisdictions multiple stakeholders may fill the role (e.g., FCC and the National Telecommunications and Information Administration in the US). A primary objective of the regulator includes avoiding radio interference. | In the tactical military domain this entity is responsible for allocating and controlling frequency assignments to national forces and for coordinating with corresponding roles in coalition/allied forces. In the commercial domain it is the governmental agency responsible for regulatory policy and licensing. |

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| Security Officer | Installs/loads Key's, PKI certificates, Security Software including algorithms, cryptographic unit protocols, downloadable security policies and other data which configures and controls the security behavior of the SDR including selection of the subset of parameters subject to audit. Can review but not alter or delete audit log | Any entity who interacts with the SDR for security control or management purposes including key loading and audit log parameter selection. Typically a user side entity but may reside on bearer side in some applications such as BLACK (Encrypted) Key distribution and loading operations. |
| Software Distributor (SD) | The SD is any entity who is an approved distribution point for any software which is authorized to be downloaded onto the SDRD. It may be a network operator's server, a software vendor or service provider's server, or an individual who is authorized to connect storage media to the SDRD for download purposes. | Responsible for the physical or electronic distribution of authorized software to the targeted platforms. |
| Software/Content Provider (SCP) | The software content provider is the entity that takes responsibility for the performance of the radio software, in most cases the entity that wrote the code. | Creates software for the radio platform. The software may be part of the radio services, waveforms or user applications. |
| User Side (of) Terminal | The plain text classified user abstraction represents every possible end consumer whose information requires encryption e.g. one tactical radio user, one high layer data processing computer, or a larger network. | Unencrypted/plain text side of the radio where classified and unclassified data is processed and resides. |

**Table 1: Actor/Role List For a Tactical Radio Security Services API**

| Actor/Role | Description | Function |
|---|---|---|
| User/ Communicator | Any entity that interacts with the SDR for communication purposes. This may include Bearer Side and/or User side wired external network interfaces to the Global Grid or Tactical Internet the user serves. | Typically a user side entity but may reside on bearer side in network applications. Uses SDR to communicate voice, data, imagery or network traffic. The user role corresponds to the individual or entity that uses the communications device to access communication based services |
| Waveform/ Application | The waveform/application provides those services and functions that allow the transmission and reception of traffic via the associated air interface. | Depending upon the waveform/application characteristics and the platform services the waveform/application may have components on just the bearer side, or both bearer side and User side |
| Additional actors/roles will be identified if needed for the development of use cases | | |

# 3 Waveform Examples

In this Section we shall address the Radio Security Service needs of waveforms by first identifying the types of security service classes and their place in the context of the Software Communications Architecture as well as the need for the resultant API to be agnostic to the underlying security architecture of the radio platform. Waveform security needs are then analyzed and are divided into four main classes of waveforms:

- Military/Government Waveforms
- Public Safety Waveforms
- Commercial Satellite Communications (SATCOM) Waveforms,
- Commercial Terrestrial Waveforms

Of these four classes we have been able to include examples from both of the first two, but no examples of the latter two since there were no contributors to the document with the relevant knowledge base to address these waveforms' needs. These can be addressed in future work when individuals with the requisite knowledge based can contribute to the analysis.

It is believed that the lack of input for the commercial waveforms does not significantly diminish the completeness of the resultant requirement set, since it is the Forum's view that commercial waveform security needs will be a subset of those required by the Military/Government and Public Safety waveforms and any unique needs can be accommodated by an extension to the resultant IRSS API.

## 3.1 Introduction

The security services considered for each waveform are derived from the Wireless Innovation Forum Security Working Group published report[5].

While an actual waveform may not utilize centralized security services for all required security operations, for purposes of these analyses, it will be initially assumed that all radio security services will be provided by the Centralized Security Function unless the waveform is required to implement one or more such services (e.g. TRANSEC key stream generation).

Thus, when appropriate to the waveform example, the analysis will examine what API requirements might emerge from the waveform application incorporating the security service. For example, in some applications the waveform might need to perform an authentication. The actual authentication process (or portion thereof) could occur within the waveform or it might be relegated to a CSF. In the first instance the waveform would need to retrieve key material, certificates etc. in order to perform the required authentication. It might also need to have any certificates received in the process authenticated down to the root level (The Forum recommends that root level authentication should always be a centralized security service). Clearly these two different approaches impose different requirements on the APIs. Any necessary derivation or clarification of the services used shall be clearly shown in the details of the use case example.

[5] *"Securing Software Reconfigurable Communications Devices",* WINNF-08-P-0013, July 2010

### *3.1.1 Applicable Radio Security Services*

Table 3 is a somewhat modified version derived from Chapter 5 of footnote 5, and lists the various Radio Security Services identified and described there-in. Operations such as the various bypass operations, Over-The-Air Rekey (OTAR), Over the Air key Transfer (OTAT) and Over the Air Zeroize (OTAZ) have been added since they are tactical radio specific application functions not addressed in the published document whose focus was on non DoD/military radios.

Each waveform example will consider each of these security services for applicability and will define the extent to which each service may be needed and, where relevant, specific functions required by the waveform example.

For each waveform, each Security Service in Table 3 will be given one of the three following category classifications. In certain instances, in tables which are provided for the waveform categories, two entries might exist; the first identifying how the service applies to current/legacy waveforms and the second identifying what a hypothetical future waveform may need. Please note that it is unlikely that there will be a one-to-one corresponding API for each security service identified in these tables nor is there any explicit or implicit requirement that there should be.

**Table 2: Entry Descriptions for Waveform RSS tables**

| Table Entry | Meaning |
|---|---|
| “Platform API” | A service class whose API requirements are not determined by the specific waveform portability and/interoperability needs. Any requirements for this service that may be related to the waveform (e.g. key fill) will be specific to the underlying platform operational requirements and design. |
| “Waveform API” | A service class whose API requirements, will at least in in part be driven by the specific waveform whose characteristics/properties are relevant to and derived from Waveform/Application portability and /or interoperability needs consistent with Radio Platform operational and design requirements. |
| “Not Applicable” | A service class, none of whose underlying services are required by the waveform in support of the specific waveform operations. |
| 1st Entry/2nd Entry | 1st entry defines applicability for current/legacy waveform examples, while 2nd defines applicability for future/next generation waveforms |

**Table 3: SDR Device Security Service Classes**

| | |
|---|---|
| **Access Control Service including Identification and Authorization related to:** | |
| HMI SDRD Interface interactions | Remote access/use of platform resources |
| Software Downloads/ Updates | Policy Downloads & Updates |
| | Configuration Data downloads/Updates |
| **Authentication and Non-repudiation Service related to:** | |
| Users | Software content providers |
| User Devices | Network Operators |
| Network Devices | Service Providers |
| **Information Integrity Service for :** | |
| Platform resident user data | Platform resident software and firmware |
| All resident radio & network configuration Data | Any downloadable data or software |
| | Over the Air Control and configuration commands |
| **Information Security Bypass and Confidentiality Service including Bypass, Encryption and Decryption services for:** | |
| User communications | Configuration Data downloads |
| Network Control communications | Software Downloads |
| Device Uploads to networks (e.g., Log data, configuration data) | User data Storage |
| Policy (security, regulatory, etc.) downloads | Configuration Data Storage |
| Waveform Header Bypass Operations | Key Material Storage |
| Plain Text Audio Bypass | Waveform Control Bypass Operations |

**Table 3: SDR Device Security Service Classes**

| | |
|---|---|
| **Transmission Security (TRANSEC) Service for waveform/air interface related security functions such as:** | |
| • Spread spectrum applications<br>• Frequency hopping applications | • Cover for waveform control information<br>• Cover for waveform data |
| **Key and Credential Management Service for:** | |
| • User PKI Certificates<br>• User PKE private/shared keys<br>• User's National shared and private keys<br>• Regional and Coalition Forces shared keys<br>• Over the Air Rekey (OTAR)<br>• Over the Air (key) Transfer (OTAT) | • Device certificates and private/shared keys<br>• Root & intermediate Certification Authority Certificates<br>• PINs, Passwords, Biometric access and other electronic credential data<br>• Over the Air Zeroize (OTAZ) |
| **Platform Resource Security Management Service for :** | |
| • Memory Management Security Enforcement | • Radio Platform Software Configuration Management & Version Control<br>– Radio Platform Operating Environment<br>– Radio Platform Applications |
| **Logging, Auditing and Security Alarm Service providing:** | |
| • Usage logs<br>• Security Event logs<br>• Cognitive/DSA Operations logs | • Non-repudiation logs<br>• Security Related Alarm services<br>• Audit log preparation |
| **Policy Enforcement and Management Security Service for:** | |
| • The Platform security policy<br>• Waveform/application security policies<br>• Regulatory Policies | • SDRD Behavioral control (cognitive/learning radio )<br>• Other downloadable policies (e.g., Network Management, Network Security |

### *3.1.2 SCA Considerations for the API*

As indicated in the Introduction of this document, the API set developed from this specification is intended to be used in an SCA based operating environment. The SCA is component based architecture, operating in a defined POSIX environment utilizing a specified and defined set of commonly available components and related services known as the Core Framework. CORBA is the specified middleware providing the interfaces and transport mechanism between application components and platform services. The overall radio operating environment includes additional services and components that are platform specific and tailored to the underlying hardware and security architecture as well as the platform functional and design requirements.

In such an environment, any given waveform may be instantiated for a period of time and then shut down so that a different waveform can be instantiated on the same hardware as needed to meet tactical mission requirements. Whenever a waveform is instantiated, the waveform must be allocated the required resources and configured for operation. While some of these configuration operations may fall within the responsibility of the platform operating environment, the waveform software components possess unique knowledge concerning the configuration needs of the waveform itself. Moreover, for some waveforms the configuration needs can change dynamically.

Thus the RSS API for waveforms must provide the capability for the waveform to configure the RSS API to meet the specific needs of that waveform. Several of the API operations defined in 4.2 are specific to this need.

## 3.2 Security Architecture Independence

So as not to presume the underlying security architecture for any given SDR, the analysis will consider the following four high level security architecture variants as a minimum.

- Multiple Independent Levels of Security (MILS)
- Multiple Single Levels of Security (MSLS)
- Multi-level Security(MLS),
- Single Levels of Security (SLS)

These different high level architectural implementations will be examined to determine if there is any influence on RSS API requirements resulting from a given architecture and to ensure that any requirements which emerge are appropriately captured and reflected in the resultant API. For readers who are unfamiliar with these categorizations, please refer to Figure 2.

The block diagram at the bottom represents the simplest of these architecture alternatives, the Single Level of Security (SLS) model. In this example there is a single RF channel interfacing to a single Cryptographic unit and Plain Text (PT) information processor which are each processing all information at the same (single) level of classification. Only one level of classification is permitted for any operating session.

The next example diagram (MLS) is quite similar in that there are single cryptographic and PT information processing resources. However, the implementation of these resources has been certified to be multi-level secure. While simple in view, it is highly complex to achieve and certify such an implementation.

The third block diagram represents Multiple Single Levels of Security where-in each classification level has dedicated physical resources for the plain text information processing and the crypto unless the crypto is separately certified as MLS or MILS. In some implementations each crypto/RED processor channel will be associated with a specific waveform. This is necessitated with many legacy waveforms since it is not possible to determine to which crypto/RED process received transmissions should be sent for decryption when a single RF channel is shared by multiple baseband voice/data channels. However IP based waveforms can readily ascertain which baseband channel is involved from the routing information included in the transmission. In such an instance, multiple baseband channels can be serviced by one or more waveform instantiations.

The fourth block diagram represents Multiple Independent Levels of Security where-in the processing environments for the cryptographic and plain text information processing have the means for logically and/or physically isolating or separating each classification level from the other. This is primarily achieved by the application of an operating system which includes a separation kernel and associated support mechanisms (both hardware and software) which maintain and enforce the required degree of separation between the resources allocated to each level of classification. As such MILS provide a means by which a radio might appear to possess either an MLS or MSLS operating environment without the hardware and/or software complexities of these other architectures.

These approaches are relevant in several ways. For all but the first, two (i.e., SLS and MLS), it is implicit that the Waveform Processing must be able to form the logical relationships needed to associate transmit and received CT streams with the logical entity that is processing the information at each classification level. Not all waveforms support the ability to form such associations, particularly when receiving cipher text information over the air. Without native support for this necessary function, a waveform is relegated to either an SLS or MLS application, but only if the MLS operation does itself require such an association.

These relationships as we shall see, primarily result in the need for the waveform to configure multiple “cryptographic channels” each with its respective traffic encryption/decryption key and crypto configuration parameters.

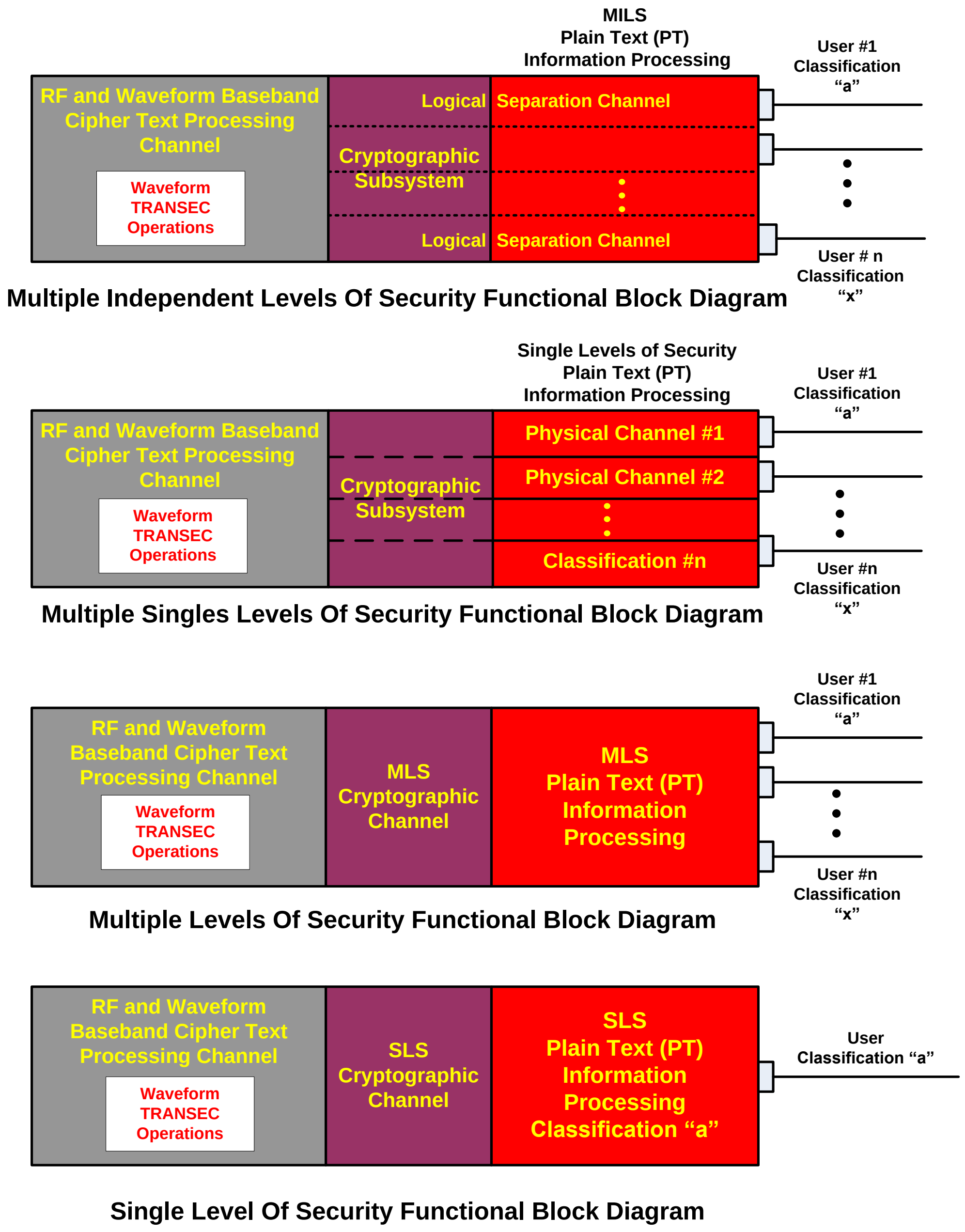


**Figure 2 Alternative Forms for SDR Security Functional Architectures**[6]

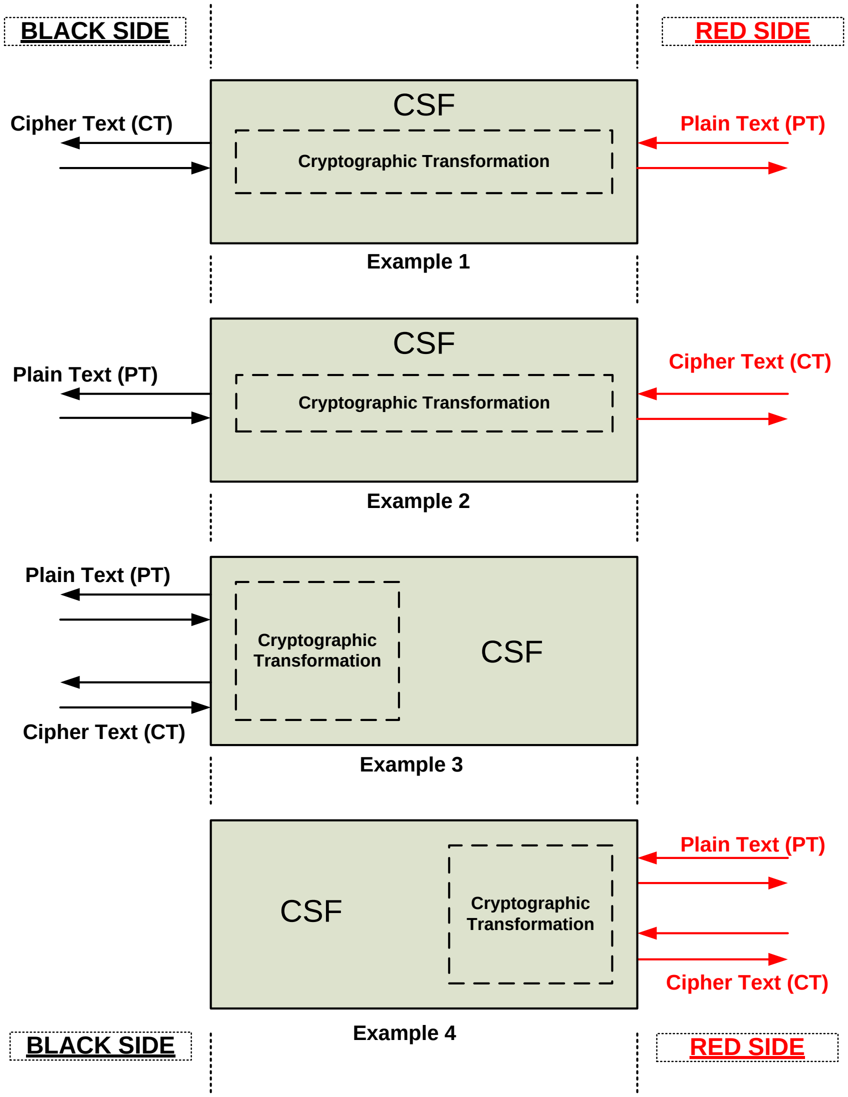
[6] Note: There is one model which is not illustrated in this figure. That particular model is one in which there is no specific physical or logical separation of the waveform, security or plain text/security sensitive information processing functions. This model is often employed in commercial applications which unfortunately also offer low levels of security. The Wireless Innovation Forum cannot recommend any such architecture, especially for tactical radio applications where security breaches could jeopardize the lives of the radio users.

## 3.3 Military/Government Waveforms

A number of waveforms which could be used by military or central government agencies have been identified for analysis purposes. They are not intended to represent any specific waveform but some are based on publicly released standards and specifications. In several instances capabilities are identified that are hypothetical in nature so as to explore the different ways such a waveform could require the use of a tactical radio's security services both by waveforms in current use and by possible future variants. When relevant to a specific waveform group, we have also considered and examined legacy waveform needs as well as hypothetical needs of next generation waveforms whose requirements are emerging.

Specific characteristics of the air interfaces, such as frequency band, bandwidth, data rates and other similar technical parameters, are not relevant to these examples as they have little bearing on the definition or identification of the required security services. Likewise, when relevant we shall assume the waveform has an Electronic Counter Counter Measures (ECCM) mode, but the specific nature of that mode will not necessarily be defined. In some instance several possible forms may be considered for purposes of exploring how alternative forms might affect the definition of the APIs.

An aspect of importance to this class of waveforms is the notion of a Tactical Radio having a RED side and a BLACK side. These legacy terms derive from communications equipment with integral COMSEC or TRANSEC devices and whose design must comply with TEMPEST or compromising emanations criteria. In general the RED side of such equipment is where plain text (PT)/unencrypted data resides, while the BLACK side refers to the side where the sensitive or classified information is encrypted or protected by TRANSEC. Thus plain text information from the RED side is transformed through a cryptographic operation to cipher text (CT) and output to the BLACK side, and cipher text information received on the BLACK side is passed through the cryptographic unit which transforms it to PT information. While this describes the normal flow for information to be communicated, it does not suffice for all operations which may require cryptographic or TRANSEC functions. Some unclassified information related to waveform operations may reside on the BLACK side of a crypto but may need to be encrypted (or placed under "cover") and sent out over the air, while similarly, the same kind of information may need to be received and decrypted to the BLACK side. Generalized file encryption/decryption operations may have similar needs thus, as we shall see later, when cryptographic/TRANSEC channels are configured there will be a need to identify whether the CT and PT ports of the channel are located on the BLACK or RED side of the cryptographic component. Thus Cryptographic operations can occur from BLACK to BLACK, BLACK to RED, RED to RED and RED to BLACK as appropriate to the specific needs of a waveform/application.



**This is illustrated in**

Figure **3** which depicts full duplex channel examples although in principle any of these four examples could be either simplex transmit or receive only.

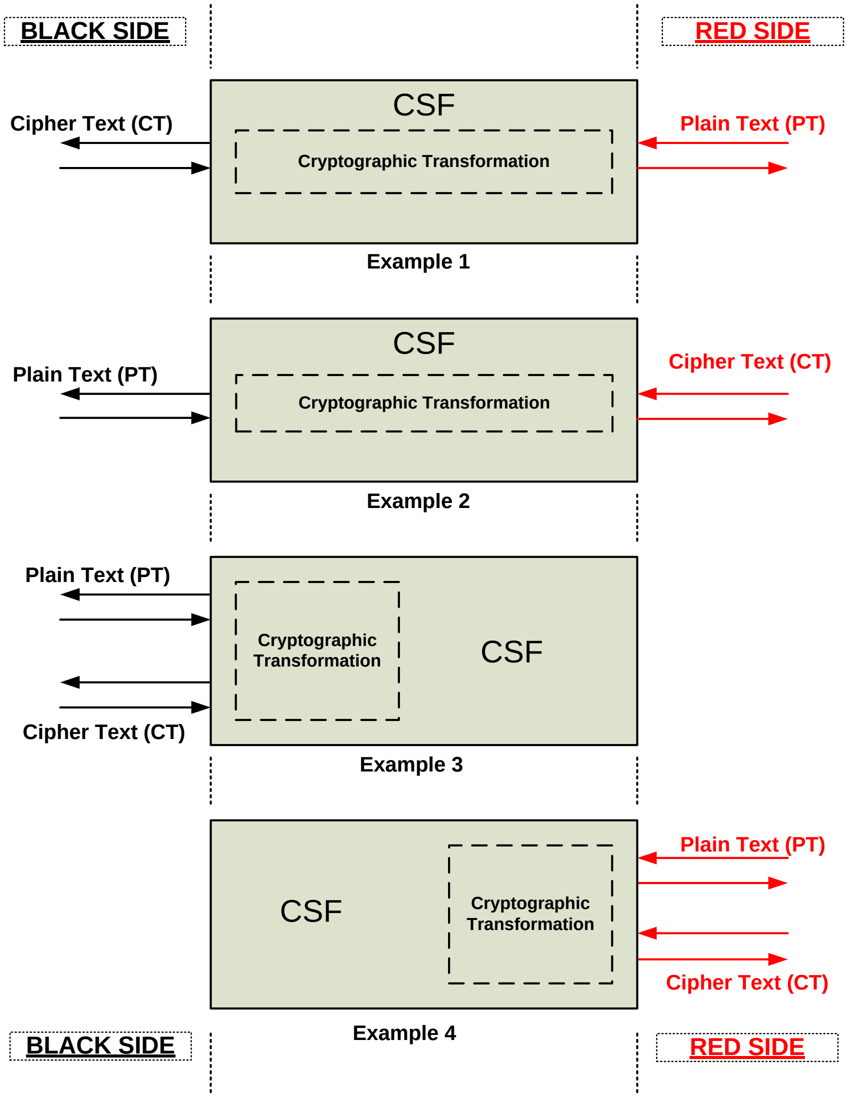


**Figure 3: Cryptographic Channel Configurations**

While we have introduced this topic of channel configuration for INFOSEC functions, it may also apply to TRANSEC channels as well as channels configured for authentication, integrity checks and other purposes. However these later channels typically exist only on either the RED or the BLACK side. Ultimately the Waveform Security Policy will delineate what is and what is not permissible from a configuration perspective for any given waveform.

### *3.3.1 IP Based Ad Hoc Networking (IPBAHN) Waveform*

Ad hoc networking waveforms are emerging to be a highly useful application in the tactical military, commercial and public safety sectors because they allow networked operations to occur without the need for any (or at least minimal) infrastructure, complex or otherwise. The goal is for the SDRs in the network to provide an infrastructure capability which allows its resources to be utilized in support of the users of this network. Such networks may employ Cognitive Radio behaviors as part of establishing and maintaining network formation as well as provide support for other radio functions such a situational awareness and dynamic spectrum utilization. The following sections define the relevant security needs and related characteristics for this hypothetical waveform.

#### 3.3.1.1 IPBAHN Waveform - Operational Characteristics

Network operations are assumed to be IP based in order to facilitate and provide interoperable flow of traffic through the ad hoc radio network to rear echelons and the networks in the command and control structure of the national, allied and coalition forces. As such the waveform and the radio platform shall be required to support standard IP based network services and operations including the application of standardized security services to these network operations in accordance with established standards. It is generally assumed that this waveform would be a wideband waveform to support the necessary protocols and network situational awareness although later, in Section 3.3.5, a next generation narrowband waveform version is postulated. It is possible that some of the situational awareness and ad hoc networking functionality may be based on cognitive radio and or dynamic spectrum access (DSA) operations.

#### 3.3.1.2 IPBAHN Waveform - Security Characteristics and Required Security Services

We shall examine each of the various radio security services as applicable to this waveform. As noted above, the waveform must support all standard IP network security operations, including authentication and encryption services such as IPSEC V4 and V6 as well as any required audit and logging services. The following sections address the specifics of each security service class.

##### 3.3.1.2.1 IPBAHN Waveform - Access Control Services

Access control related services involve identifying an entity requesting access to a device, function or service via a log-in or similar process and being granted access in accordance with pre-defined privileges (as in role based access control methods). As indicated in the table below for this waveform, this is believed only to be applicable to Network related Operating Policy downloads and distribution, as well as related configuration data distribution (e.g. routing updates). This functionality must be supported only to the extent that such functions are defined in accordance with established Internet (RFC) standards. Applicable access control lists are assumed to be available from the waveform application configuration data and if necessary the access control list data is provided to the CSF for its use via an appropriate platform API. Access control lists should include information concerning the role of each entity on the list. Specific properties regarding roles are a platform design concern and are not construed to be a part of the API. Thus we may assume that the security services will be able to determine from the defined role whether or not the entity is allowed access to the requested information, service or platform resource.

It is assumed that Access Control services for any human directly interacting with the SDRD via a control panel or remotely via any waveform will be relegated to a platform defined API. This will also apply to any access control service related to waveform software downloads or updates. Policy downloads and updates are relevant since QoS and other network operations can be managed by policies. Similarly Routing Updates and other network related operating parameters will need to be managed in real time and distributed using standardized protocols.

| **Access Control Services (Identification and Authorization) for:** | |
|---|---|
| HMI SDRD Interface interactions | Platform API |
| Software Downloads/Updates | Platform API |
| Policy Downloads & Updates | Waveform API |
| Configuration Data downloads/Updates | Waveform API |
| Remote access/use of platform resources | Platform API |

#### 3.3.1.2.2 IPBAHN Waveform - Authentication and Non-repudiation Services

Authentication and Non-repudiation services involve methods to unambiguously verify the identity of an entity (device or user), authenticate that identity and any information provided by the entity and to record, when necessary, data related to the activity so that the event and/or data cannot be repudiated by the entity. Services in this class are to be provided as identified in the table below and defined here-in.

Identification and/or mutual authentication is required between any entity joining the network and any entity which is already a part of the network. This is aimed at preventing either a legitimate Device or the Network from being impersonated. In addition these services will be supported to the extent required by established Internet (RFC) standards. The authenticated identify can then be used by the Access Control Service to determine whether or not the entity is to be granted access to the platform for the services is has requested.

Because of the multinational nature of this waveform, the issue of potentially multiple root certification authorities (CAs) must be considered. In one approach, the radio devices might be loaded with root certificates from each national authority. While this may be cumbersome and creates distribution and other security issues, it is none-the-less a valid technical solution. The other approach that might be considered would be for each involved nation to sign and distribute to their respective national forces copies of the root certificates of the other national authorities signed by their own respective CA. In this way the other nations' certification authorities appear to be intermediate level "national" certification authorities within a given nation's network. This latter structure also allows such "intermediates" to have their certificates revoked within any given national network should that be necessary.

For this waveform, this service will consider the needs of utilizing the information contained in Compromised Key Lists (CKLs) and Certificate Revocation Lists (CRLs) in accordance with established Internet (RFC) standards. However the means or method of maintaining and updating these lists are beyond the scope of this document. For this reason we shall assume that installing or updating or otherwise managing CKL and CRL data is a platform responsibility.

As discussed earlier, this analysis will consider examples where the authentication services are provided in one instance by the waveform application using information (keys, certificates etc.) obtained from the CSF and in another instance where all authentication functions are provided by the CSF and supported by the waveform. In this way either method can be supported by the API Any Authentication services of users or the sources of software (content providers) are relegated to platform API's.

| **Authentication and Non-repudiation Services for:** | |
|---|---|
| Users | Platform API |
| User Devices | Waveform API |
| Network Devices | Waveform API |
| Software content providers | Platform API |
| Network Operators | Waveform API |
| Service Providers | Waveform API |

#### 3.3.1.2.3 IPBAHN Waveform - Information Integrity Services:

Information Integrity services include verifying the integrity of received data when so requested or when required by established protocols. This function may also be used to ascertain the integrity of any information stored within the radio by applying and verifying digital signatures. This includes resident software code, firmware code and data elements used by the system. Likewise when such information is transmitted between network elements it is critical that the integrity of the information be verified.

For this waveform, Information Integrity shall be supported as indicated in the table below to the extent required by established Internet (RFC) standards. As with the previous service, the API shall support the integrity service being provided by either the waveform application or the CSF. All Integrity requirements relating to how data or software is stored and retrieved are assumed to be relegated to platform specific requirements.

| **Information Integrity Services for:** | |
|---|---|
| Platform resident user data | Platform API |
| Waveform related resident radio & network configuration data | Waveform API |
| Platform resident software and firmware | Platform API |
| Any waveform specific related downloadable data or software | Waveform API |
| Over the Air Control and configuration commands | Waveform API |

#### 3.3.1.2.4 IPBAHN Waveform - Information Security (INFOSEC), Bypass and Confidentiality Services

INFOSEC services can provide encryption and decryption services for User communications as well as Network Control communications and platform resident data and software. For this waveform these services shall be provided as summarized in the table and described below. The protection level needed for the User communication (i.e. in the information domain) and for the Network Control (i.e. in the transport domain) may be different. The Radio Security services API shall allow for a protection (encryption) layer for each of those with different setups in terms of keys, algorithms, etc.

Encryption and decryption services must be supported for all user communications and required ad hoc network control and management functions. This includes the ability to support multiple algorithms or cryptographic unit emulations, each employing one or more COMSEC Keys as might be used in support of National, Regional and/or Coalition force communications. For this waveform we shall assume that all confidentiality services are provided by the CSF.

Additional encryption/decryption services may apply to files, tokens or other data elements. These encryption operations could employ either symmetric or asymmetric encryption/ decryption operations and could apply to network related data received in network control or network management traffic.

Control and header bypass functions shall be supported to the extent required by the explicit and specific waveform security and bypass policies and the related Radio Platform Security Policies. For the other functions listed in the table, this service must be able to provide these services in accordance with established Internet (RFC) Standards, including those relevant to SSL, TLS and IPSEC V4 and V6. INFOSEC functions for software downloads and for storage of the three data types listed are assumed not to be part of the waveform operations and are thus relegated to platform defined APIs based upon individual platform requirements.
Bypass operations, which are directly related and considered part of the INFOSEC services, are as indicated.

| **Information Security (INFOSEC) Bypass and Confidentiality Services for:** | |
|---|---|
| User communications | Waveform API |
| Network Control communications | Waveform API |
| Device Uploads to networks (e.g., Log data, configuration data) | Waveform API |
| Policy (security, regulatory, etc.) downloads | Waveform API |
| Configuration Data downloads | Waveform API |
| Software Downloads | Platform API |

| **Information Security (INFOSEC) Bypass and Confidentiality Services for:** | |
|---|---|
| User data Storage | Platform API |
| Configuration Data Storage | Platform API |
| Key Material Storage | Platform API |
| Control Bypass | Waveform API |
| Header Information Bypass | Waveform API |
| Plain Text Audio Bypass | Not applicable |

### 3.3.1.2.5 IPBAHN Waveform - Transmission Security (TRANSEC)

For this document we shall assume that there are two basic forms of TRANSEC services that might apply to this waveform. In one form, the waveform application provides data to the CSF and the CSF manipulates and transforms the data according to a defined TRANSEC process and then returns the transformed data for further waveform processing.

In the other form, the waveform requests the CSF to provide either a random number or the TRANSEC Key based generation of a stream of data (known as keystream) to the waveform which the waveform then applies to the outgoing data and/or uses to perform frequency hopping or other spread spectrum techniques. Such a keystream may be used also for use as cover of waveform related control data or a separate keystream using either the same or a different key may be requested for cover application purposes. Thus the API must be able to support either combined or functionally separate interfaces for these purposes.

It is presumed that this waveform would never directly perform TRANSEC keystream generation functions and as such would never request the CSF to provide a copy of a TRANSEC key.

For the IPBAHN waveform we shall assume that whichever method is used that the TRANSEC operations will be periodic because the operations of such a waveform are typically time interval/slot based. We shall also assume that TRANSEC cover will be applied to all control information used to setup and maintain the network that does not required INFOSEC. In addition it is assumed that cover will be applied to all IP packet fields except for the data which will be encrypted as part of the encryption process.

| **Transmission Security (TRANSEC) Services for:** | |
|---|---|
| Spread spectrum applications | Waveform API |
| Frequency hopping applications | Waveform API |

| **Transmission Security (TRANSEC) Services for:** | |
|---|---|
| Cover for waveform control information | Waveform API |
| Cover for waveform data | Waveform API |

### 3.3.1.2.6 IPBAHN Waveform - Key and Credential Management Services

Key and Credential Management services as provided for this waveform are summarized in the table below. To that end, the CSF is presumed to provide storage and integrity protections services for all key material and all forms of electronic credential data. The CSF also would manage and maintain the information until it has been erased, zeroized or superseded by designated newer key material. It is assumed that all key material will be identified via standardized key tags and that one or more common standards are shared by the waveform and the platform for means of identifying and referencing any specific key used by the waveform. It is assumed that any platform which accepts a key without a standardized tag will provide the means to create such a tag when the key material is loaded or installed onto the platform. The means and manner of providing confidentiality to any of this information is a matter left to platform design and shall not be not subject to specification via any of the defined RSS API's.

The nature of an IPBAHN waveform presumes the potential for simultaneous multiple cryptographic contexts using different keys for each. Some of these keys may be preplaced, while others depending upon circumstances might be pair-wise unique generated by means of a given cryptographic process and parameter exchange. Therefore it is important that the API provide the means to support multiple keys in use simultaneously for a given waveform instantiation. This includes the ability to ascertain which key is to be used for a given encryption/decryption context.

Digital certificates for network users/devices can be received via standard protocols and used for a variety of other security services such as authentication, integrity checking etc. Consequently it is essential that the API support the ability of a waveform to pass in certificates for temporary or long term storage and for retrieving them should the waveform requires them in support of another waveform operation.

It is assumed that zeroization of channel specific key's or digital certificates is a waveform API function but general zeroization operations are a platform API function.

The API should also allow, to the extent supported by the waveform security policy, the discovery of what key material is available for the waveform to use for a given instantiation.

Finally we assume that a waveform like this has the ability to support over-the-air rekey operations. However unlike legacy rekey operations, for an IPBAHN like waveform, rekey could involve the distribution of new digital certificates and the establishment of new private and public key pairs for the radio's use on the IPBAHN waveform. It might also involve the secure negotiation of private session keys using standard network protocols.

Alternatively the waveform may be cognizant of receipt of a bulk encrypted file of keys which needs to be decrypted and retained within the CSF rather than being delivered to the RED baseband processor. This is somewhat equivalent to the legacy OTAT operation in which keys were transferred between fill devices using the radio with an internal or external crypto to encrypt the keys during the over-the-air operation.

The API shall support the ability for the waveform to identify keys by defined identifiers which may be platform specific or which may correspond to legacy methods such as "key position/slot ID" references derived from the multi-position key select rotary switch on legacy crypto devices such as the KY-57 and the KYV-5. Any such "key position/slot ID" used by a waveform shall be considered specific to that waveform instantiation and the associated keys used by that instantiation. As such the simultaneous use of numerically identical "key position/slot" references shall be permitted by other waveforms but the associations to specific keys are unique to each such instantiation.

The API shall support the ability for the waveform to identify credentials by defined identifiers which may be specific to a given type of credential. For credentials such as digital certificates contents within the X.509 "Distinguished Name" field shall be capable of being used in addition to any platform specific reference scheme.

| **Key and Credential Management Services for:** | |
|---|---|
| User's National shared and private keys | Waveform API |
| User PKI certificates and related private/shared keys | Waveform API |
| User's Regional and/or Coalition shared keys | Waveform API |
| PINs, Passwords, Biometric access and other electronic credential data | Waveform API |
| Device certificates and private/shared keys | Waveform API |
| Root & intermediate Certification Authority Certificates | Waveform API |
| Over the Air Zeroize (Channel specific) | Waveform API |
| Over the Air Rekey | Waveform API |
| Over the Air key Transfer | Waveform API |

#### 3.3.1.2.7 IPBAHN Waveform - Platform Resource Security Management Services

To the extent applicable to this waveform class, all configuration, management and access to Platform Resource Security Management Services are relegated to the Platform API.

| Platform Resource Security Management Services for: | |
|---|---|
| Memory Management Security Enforcement | Platform API |
| RPOE Software Configuration Management & Version Control | Platform API |
| Radio Platform Application (RPA) Software Configuration Management & Version Control | Platform API |

#### 3.3.1.2.8 IPBAHN Waveform - Logging, Auditing and Security Alarm Services

Logging, auditing and security alarm services shall be considered a part of the waveform API to the extent that such services are required by established internet (RFC) standards. Consideration shall be given to the needs of logging events related to cognitive radio and/or DSA operations. However, it shall be possible via the API for an authorized and authenticated remote entity to request a copy of waveform related log events. This shall include usage logs, Security Event logs, Non-repudiation logs, Cognitive/DSA Operations, Security Related Alarm services and Audit log preparation. Configuration, management and access to any other logging, audit or alarm services are a matter left to platform design.

| Logging, Auditing and Security Alarm Services for: | |
|---|---|
| Usage logs | Waveform API |
| Security Event logs | Waveform API |
| Cognitive/DSA Operations logs | Waveform API |
| Non-repudiation logs | Waveform API |
| Security Related Alarm services | Waveform API |
| Audit log preparation | Waveform API |

#### 3.3.1.2.9 IPBAHN Waveform Policy Enforcement and Management Security Services

The API shall support the ability to permit the waveform to download, store (within the CSF) and retrieve policies which the waveform or other platform application uses to enforce policies involving network management, network security, Quality of Service (QOS) and others required by the waveform application.

| Policy Enforcement and Management Security Services for: | |
|---|---|
| The Platform security policy | Platform API |
| Waveform/application security policies | Waveform API |
| SDRD Behavioral control (cognitive/ learning radio) | Waveform API |
| Regulatory Policies | Platform API |
| Other downloadable policies (e.g., Network Management, Network Security etc.) | Waveform API |

#### 3.3.1.3 IPBAHN - Other Relevant Characteristics

None identified at this time.

#### 3.3.1.4 IPBAHN Waveform - Applicable API Use Case Operations

Based on the security service requirements outlined in Section 3.3.1.2 the API use case waveform operations indicated as being applicable to this waveform are identified in Table 4. Details of these operations are described in Section 4.2

**Table 4: IPBAHN Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | Waveform Applicability |
|---|---|---|
| WF 01 | Setup (configure)/teardown waveform Control Channels | Yes |
| WF 02 | Update Waveform Policy | Yes |
| WF 03 | OTAR/OTAT (Waveform specific) | Yes |
| WF 04 | OTAZ (Channel specific keys/Certs) | Yes |
| WF 05 | Extract/Forward Audit Log | Yes |
| WF 06 | Setup (configure)/teardown Waveform Encryption/ Decryption Channels | Yes |
| WF 07 | Algorithm Selection | Yes |
| WF 08 | Key Selection | Yes |
| WF 09 | Reserved | - |
| WF 10 | Key Negotiation / Session Establishment | Yes |

**Table 4: IPBAHN Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | Waveform Applicability |
|---|---|---|
| WF 11 | Encrypt / Decrypt User Traffic | Yes |
| WF 12 | Setup (configure)/teardown Waveform TRANSEC Channels | Yes |
| WF 13 | Perform TRANSEC Operations | Yes |
| WF 14 | Provide TRANSEC Keystream | Yes |
| WF 15 | Provide/Generate Random Number | Yes |
| WF 16 | Provide TRANSEC Key | No |
| WF 17 | Setup (configure)/teardown Waveform Bypass Channels | Yes |
| WF 18 | Plain Audio Text Bypass | No |
| WF 19 | Control Bypass | Yes |
| WF 20 | Header/In channel Bypass | Yes |
| WF 21 | Setup (configure)/teardown Waveform Authentication/ Integrity Channels | Yes |
| WF 22 | Authenticate Remote Device / Application | Yes |
| WF 23 | Authenticate Remote User (with/without physical token) | No |
| WF 24 | Authenticate Local Device/ Application | Yes |
| WF 25 | Authenticate file/token/data/certificate | Yes |
| WF 26 | Integrity Check file/token/data/certificate | Yes |
| WF 27 | Provide Digital Signature for file/token/data | Yes |
| WF 28 | Provide Hash for file/token/data | Yes |
| WF 29 | Verify Hash for file/token/data | Yes |
| WF 30 | Retrieve Certificate (s) | Yes |
| WF 31 | Accept/pass in Certificate | Yes |
| WF 32 | WF 32 Encrypt/Decrypt File/Token/Data | Yes |

### *3.3.2 TDMA SATCOM Waveform*

Satellite communications employing Time-Division Multiple Access (TDMA) technology has existed for several decades in both commercial and military applications and is likely to continue in the future because of the beyond line of sight (BLOS) capability they provide in the tactical environment. Current systems are predominately manually configured and controlled, but new systems could provide improved and more automated configuration control and management. In this section we shall consider the security needs of current and next generation systems.

#### 3.3.2.1 TDMA SATCOM Waveform - Operational Characteristics

Current systems support 5 kHz & 25 kHz channel assignments for both voice and data applications and utilize a variety of cryptographic protocols and algorithms. Future systems may offer additional bandwidth options with newer cryptographic protocols, some of which may supersede those currently being used. A TRANSEC service in the form of order-wire message encryption/decryption is required for the current systems. At the tactical user terminal these messages are typically initiated and displayed at the radio Human-Machine Interface. This form of manual configuration was necessitated because in the initial deployment of these early terminals, the radios and the cryptographic units were separate physical devices, and the cryptographic units were designed to be used with a multiplicity of radios. Current generation Satellite radios now function with embedded cryptographic solutions. This allows for the future application of automated configuration control of the satellite channel and terminals. In that transition the order-wire channel could evolve from a hybrid order-wire and control channel to a future fully automated control channel.

#### 3.3.2.2 TDMA SATCOM Waveform - Security Characteristics and Required Security Services

The API shall support the security services for the TDMA SATCOM Waveform to the extent specified in the following sections.

##### 3.3.2.2.1 TDMA SATCOM Waveform - Access Control Services

There are no identified Access Control Services that are applicable to the current TDMA SATCOM Waveform RSS API. For future versions with automated configuration of the communications channel over the air, some access control services may be required.

| **Access Control Services (Identification and Authorization) for:** | |
|---|---|
| HMI SDRD Interface interactions | Platform API |
| Software Downloads/Updates | Platform API |
| Policy Downloads & Updates | Platform API |
| Configuration Data downloads/Updates | Platform/Future Waveform API |
| Remote access/use of platform resources | Not Applicable/Future Waveform API |

#### 3.3.2.2.2 TDMA SATCOM Waveform - Authentication and Non-repudiation Services

This waveform does not require any specific Authentication or Non-repudiation services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform to the extent applicable are relegated to the Platform API.

For a future generation of this waveform, configuration of the communications channel may occur via the order-wire. In such eventuality, Identification, Authentication and Non-repudiation services will be necessary. In addition, should the user possess a terminal device, the potential exists for the user to request access to a channel and provide configuration requirements. In this instance additional RSS services as identified in the table below shall be required.

| **Authentication and Non-repudiation Services for:** | |
|---|---|
| Users | Not Applicable/Future Waveform API |
| User Devices | Not Applicable/Future Waveform API |
| Network Devices | Not Applicable/Future Waveform API |
| Software content providers | Not Applicable |
| Network Operators | Not Applicable/Future Waveform API |
| Service Providers | Not Applicable |

#### 3.3.2.2.3 TDMA SATCOM Waveform - Information Integrity Services:

This waveform does not require any specific Information Integrity services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform to the extent applicable are relegated to the Platform API.

While there is a limited over the air control and configuration capability all of the required functionality remains within the waveform. Any integrity services required on the user, radio and network data as well as any waveform related software/firmware is the responsibility of the platform and is defined by platform specific requirements. However for future versions of this waveform class which may support user and remote configuration of the channel, integrity services will be essential as indicated in the table below.

| **Information Integrity Services for:** | |
|---|---|
| Platform resident user data | Platform API |
| Waveform related resident radio & network configuration data | Platform API |
| Platform resident software and firmware | Platform API |

| Information Integrity Services for: | |
|---|---|
| Any waveform specific related downloadable data or software | Platform/Future Waveform API |
| Over the Air Control and configuration commands | Not Applicable/Future Waveform API |

#### 3.3.2.2.4 TDMA SATCOM Waveform - Information Security (INFOSEC) Bypass and Confidentiality Services

For this waveform INFOSEC services in the form of traffic encryption and separate encryption (TRANSEC cover) for orderwire functions are needed and the remaining services, to the extent applicable, are relegated to a Platform API. The waveform currently does not include any of the listed download functions within its capability, but future versions could require additional services as indicated.

| Information Security (INFOSEC) Bypass and Confidentiality Services for: | |
|---|---|
| User communications | Waveform API |
| Network Control communications | Not Applicable/Future Waveform API |
| Device Uploads to networks (e.g., Log data, configuration data) | Not Applicable/Future Waveform API |
| Policy (security, regulatory, etc.) downloads | Not Applicable/Future Waveform API |
| Configuration Data downloads | Platform API /Future Waveform API |
| Software Downloads | Platform API |
| User data Storage | Platform API |
| Configuration Data Storage | Platform API |
| Key Material Storage | Platform API |
| Control Bypass | Waveform API |
| Header Information Bypass | Not applicable |
| Plain Text Audio Bypass | Not applicable |

#### 3.3.2.2.5 TDMA SATCOM Waveform - Transmission Security (TRANSEC) Services

The TDMA SATCOM Waveform requires the ability to send and receive encrypted text based orderwire information. This encryption is a form of TRANSEC cover. Future versions may use the orderwire to automatically configure the communications channel.

| **Transmission Security (TRANSEC) Services for:** | |
|---|---|
| Spread spectrum applications | Not Applicable |
| Frequency hopping applications | Not Applicable |
| Cover for waveform control/orderwire information | Waveform API |
| Cover for waveform data | Not Application |

#### 3.3.2.2.6 TDMA SATCOM Waveform - Key and Credential Management Services

The IRSS API shall support the ability for the TDMA SATCOM waveform to select keys to be used for orderwire and traffic encryption/decryption. Some legacy cryptographic units provide capabilities for OTAR and perhaps even OTAT, but in these instances the waveforms are not aware that those operations are occurring as the functionality resides totally within the bounds of the cryptographic components which have been configured by an operator using the platform's HMI/controls. Thus any API functionality for current waveforms remains a platform API function.

The API shall support the ability for the waveform to identify keys by defined identifiers which may be platform specific or which may correspond to legacy methods such as "key position/slot ID" references. Current TDMA SATCOM waveforms do not utilize digital credentials, but future versions will likely require this ability. Any usage of PINs, passwords, biometric data and other forms of electronic credentials would be strictly relegated to platform functionality and are not applicable to the waveform. The API shall be capable of supporting those functions defined in the table below identified as Waveform API (regardless of whether it is a future capability or required for current operations.

| **Key and Credential Management Services for:** | |
|---|---|
| User's National shared and private keys | Waveform API |
| User PKI certificates and related private/shared keys | Not Applicable/Future Waveform API |
| User's Regional and/or Coalition shared keys | Waveform API |
| PINs, Passwords, Biometric access and other electronic credential data | Platform/Future Waveform API |
| Device certificates and private/shared keys | Not Applicable/Future Waveform API |

| Key and Credential Management Services for: | |
|---|---|
| Root & intermediate Certification Authority Certificates | Not Applicable/Future Waveform API |
| Over the Air Zeroize (OTAZ) | Not Applicable/Future Waveform API |
| Over the Air Rekey (OTAR) | Platform/Future Waveform API |
| Over the Air key Transfer (OTAT) | Platform/Future Waveform API |

### 3.3.2.2.7 TDMA SATCOM Waveform - Platform Resource Security Management Services

To the extent applicable to this waveform class, all configuration, management and access to Platform Resource Security Management Services are relegated to the Platform API.

| Platform Resource Security Management Services: | |
|---|---|
| Memory Management Security Enforcement | Platform API |
| RPOE Software Configuration Management & Version Control | Platform API |
| RPA Software Configuration Management & Version Control | Platform API |

### 3.3.2.2.8 TDMA SATCOM Waveform - Logging, Auditing and Security Alarm Services

To the extent applicable to this waveform class, configuration, management and access to Logging, Auditing and Security Alarm Services are relegated to a platform API.

| Logging, Auditing and Security Alarm Services: | |
|---|---|
| Usage logs | Platform API |
| Security Event logs | Platform API |
| Cognitive/DSA Operations logs | Not Applicable |
| Non-repudiation logs | Platform API |
| Security Related Alarm services | Platform API |
| Audit log preparation | Platform API |

#### 3.3.2.2.9 TDMA SATCOM Waveform - Policy Enforcement and Management Security Services

This waveform class does not require any specific Policy Enforcement and Management Services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform class, to the extent applicable, are relegated to the Platform API.

For future variants of the TDMA SATCOM Waveform class the API shall support the ability to download and implement policies relating to Network Management and Network Security.

| Policy Enforcement and Management Security Services for: | |
|---|---|
| The Platform security policy | Platform API |
| Waveform/application security policies | Platform API |
| SDRD Behavioral control (cognitive/learning radio ) | Not Applicable |
| Regulatory Policies | Platform API |
| Other downloadable policies (e.g., Network Management, Network Security | Not Applicable/ Future Waveform API |

### 3.3.2.3 TDMA SATCOM Waveform - Other Relevant Characteristics

None identified at this time.

### 3.3.2.4 TDMA SATCOM Waveform - Applicable API Use Case Operations

Based on the security service requirements outlined in Section 3.3.2.2 the API use case waveform operations indicated as being applicable to this waveform are identified in Table 5. Details of these operations are described in Section 4.2.

**Table 5: TDMA SATCOM Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | TDMA SATCOM Waveform Applicability | |
|---|---|---|---|
| | | Current | Future |
| WF 01 | Setup (configure)/teardown waveform Control Channels | Yes | Yes |
| WF 02 | Update Waveform Policy | No | Yes |
| WF 03 | OTAR/OTAT (Waveform specific) | No | Yes |

**Table 5: TDMA SATCOM Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | TDMA SATCOM Waveform Applicability | |
|---|---|---|---|
| | | Current | Future |
| WF 04 | OTAZ (Channel specific keys/Certs) | No | Yes |
| WF 05 | Extract/Forward Audit Log | No | No |
| WF 06 | Setup (configure)/teardown Waveform Encryption/ Decryption Channels | Yes | Yes |
| WF 07 | Algorithm Selection | Yes | Yes |
| WF 08 | Key Selection | Yes | Yes |
| WF 09 | Reserved | - | - |
| WF 10 | Key Negotiation / Session Establishment | No | Yes |
| WF 11 | Encrypt / Decrypt User Traffic | Yes | Yes |
| WF 12 | Setup (configure)/teardown Waveform TRANSEC Channels | Yes | Yes |
| WF 13 | Perform TRANSEC Operations | Yes | Yes |
| WF 14 | Provide TRANSEC Keystream | No | Yes |
| WF 15 | Provide/Generate Random Number | No | Yes |
| WF 16 | Provide TRANSEC Key | No | No |
| WF 17 | Setup (configure)/teardown Waveform Bypass Channels | Yes | Yes |
| WF 18 | Plain Audio Text Bypass | No | No |
| WF 19 | Control Bypass | Yes | Yes |
| WF 20 | Header/In channel Bypass | No | Yes |
| WF 21 | Setup (configure)/teardown Waveform Authentication/ Integrity Channels | No | Yes |
| WF 22 | Authenticate Remote Device / Application | No | Yes |
| WF 23 | Authenticate Remote User (with/without physical token) | No | No |
| WF 24 | Authenticate Local Device/ Application | No | Yes |

**Table 5: TDMA SATCOM Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | TDMA SATCOM Waveform Applicability | |
|---|---|---|---|
| | | Current | Future |
| WF 25 | Authenticate file/token/data/certificate | No | Yes |
| WF 26 | Integrity Check file/token/data/certificate | No | Yes |
| WF 27 | Provide Digital Signature for file/token/data | No | Yes |
| WF 28 | Provide Hash for file/token/data | No | Yes |
| WF 29 | Verify Hash for file/token/data | No | Yes |
| WF 30 | Retrieve Certificate (s) | No | Yes |
| WF 31 | Accept/pass in Certificate | No | Yes |
| WF 32 | WF 32 Encrypt/Decrypt File/Token/Data | No | Yes |

### *3.3.3 UHF TACSAT Waveform*

UHF Tactical Satellite (TACSAT) communications have been a mainstay of beyond line-of-sight tactical communications to the US Navy and Air Force since the 1970s and to the US Army since the early 1980's and have been subject to continuous improvements and upgrades over the last 4 decades leading to the newest system currently being introduced and prepared for operational status which is identified as the Mobile User Objective System (MUOS).

#### 3.3.3.1 UHF TACSAT Waveform - Operational Characteristics

The military UHF Tactical Satellite networks typically need to support several simultaneous missions. Mission may be distributed in different geographical areas and UHF TACSAT networks are defined based on typical large-scale deployment scenarios for land and maritime missions. These networks currently operate on both 25kHz and 5 kHz channel bandwidths and support both voice and data operations on separate or individual channels.

In a land-deployed UHF SATCOM context, the TACSAT networks are commonly associated to UHF man-portable radios (also known as man packs), which are primarily used in a mobile tactical and vehicular environment.

In the deployed communications context, UHF SATCOM users will be operating in highly mobile and netted (all-informed) networked environments, involving many users per net.

Also included in this waveform class is the new Mobile User Objective System which supports both legacy UHF TACSAT operation as well as the new mobile user functions. Bandwidths from 64 kHz and lower for legacy TACSAT users are available. The following description of the MUOS System was extracted from a US Navy Website:[7]

> “Mobile User Objective System (MUOS) is a narrowband Military Satellite Communications (MILSATCOM) system that supports a worldwide, multi-Service population of mobile and fixed-site terminal users in the Ultra High Frequency (UHF) band, providing increased communications capabilities to smaller terminals while still supporting interoperability to legacy terminals.
>
> **Features:**
> MUOS adapts a commercial third generation Wideband Code Division Multiple Access (WCDMA) cellular phone network architecture and combines it with geosynchronous satellites (in place of cell towers) to provide a new and more capable UHF MILSATCOM system. The constellation of four operational satellites and ground network control will provide greater than 10 times the system capacity of the current UHF Follow-On (UFO) constellation.
>
> MUOS includes the satellite constellation, a ground control and network management system, and a new waveform for user terminals. The space portion is comprised of a constellation of four geosynchronous satellites, plus one on-orbit spare. The ground system includes the transport, network management, satellite control, and associated infrastructure to both fly the satellites and manage the user’s communications. MUOS and these newer terminals are designed to support users that require greater mobility, higher data rates, and improved operation availability. The new waveform is termed the MUOS Common Air Interface (CAI), a Software Communications Architecture compliant modulations technique for the Joint Tactical Radio System (JTRS) terminals. The MUOS CAI waveform will be available to the Services for porting to JTRS terminals in late 2008. The first MUOS satellite is scheduled to provide an On-Orbit Capability in March 2010. MUOS achieves Full Operational Capability in 2014.
>
> **Background:**
> The flow of information between users when MUOS is operational will be much different than today’s systems. Users will communicate with the satellite via UHF WCDMA links and the satellites will relay this to one of four ground sites located in Hawaii, Norfolk, Sicily, and Australia via a Ka-band feederlink. These ground sites are interconnected to switching and network management facilities located in Hawaii and Virginia. These facilities identify the destination of the communications and route the information to the appropriate ground site for Ka-band uplink to the satellite and UHF WCDMA downlink to the correct users.
>
> The network management will feature a government controlled, priority-based resource management capability that will be adaptable and responsive to changing operational communication requirements. Additionally, MUOS will provide access to

[7] https://acquisition.navy.mil/rda/media/files/programs/muos

> select Defense Information System Network services, a voice and data capability that has not been available to UHF MILSATCOM users on prior systems. For satellite telemetry, tracking and command, MUOS will use the existing control system operated by the Naval Satellite Operations Center at Pt. Mugu, California with the Air Force Satellite Control Network as a back-up.
>
> When MUOS is fielded it will serve a mixed terminal population. Some users will have terminals only able to support the legacy waveforms while other users will have newer terminal able to support the MUOS CAI. In anticipation of this, each MUOS satellite carries a legacy payload similar to that flown on UFO-11. These legacy payloads will continue to support legacy terminals, allowing for a more gradual transition to the MUOS WCDMA waveform."

Because it represents a new military waveform, there is insufficient information available about MUOS to be able to identify any specific security functions that might be needed beyond those already identified for other waveforms. Until such time as an authorized release of public information about this waveform is made, this document cannot address any other specific security needs related to MUOS.

#### 3.3.3.2 UHF TACSAT Waveform - Security Characteristics and Required Security Services

From a security point of view, UHF nets can operate at highly classified levels, depending on the associated mission and the classification of the keying material loaded in the manpack radio's integrated COMSEC device, or in the external COMSEC device attached to the UHF modem.

Individual channels will require the capability to employ Voice and Data Operations with different cryptographic algorithms and cryptographic equipment protocols.

##### 3.3.3.2.1 UHF TACSAT Waveform - Access Control Services

This waveform does not require any specific Access Control services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform are relegated to the Platform API.

| **Access Control Services (Identification and Authorization) for:** | |
|---|---|
| HMI SDRD Interface interactions | Platform API |
| Software Downloads/Updates | Platform API |
| Policy Downloads & Updates | Not Applicable |
| Configuration Data downloads/Updates | Platform API |
| Remote access/use of platform resources | Not Applicable |

##### 3.3.3.2.2 UHF TACSAT Waveform, Authentication and Non-repudiation Services

This waveform does not require any specific Authentication or Non-repudiation services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform to the extent applicable are relegated to the Platform API.

| **Authentication and Non-repudiation Services for:** | |
|---|---|
| Users | Platform API |
| User Devices | Platform API |
| Network Devices | Not applicable |
| Software content providers | Not applicable |
| Network Operators | Not applicable |
| Service Providers | Not applicable |

#### 3.3.3.2.3 UHF TACSAT Waveform - Information Integrity Services:

This waveform does not require any specific Information Integrity services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform to the extent applicable are relegated to the Platform API.

| **Information Integrity Services for:** | |
|---|---|
| Platform resident user data | Platform API |
| Waveform related resident radio & network configuration data | Platform API |
| Platform resident software and firmware | Platform API |
| Any waveform specific related downloadable data or software | Platform API |
| Over the Air Control and configuration commands | Not applicable |

#### 3.3.3.2.4 UHF TACSAT Waveform - Information Security (INFOSEC) Bypass and Confidentiality Services

This waveform only requires INFOSEC Services in support of user communications and plain text audio bypass. No other specific INFOSEC services are needed in support of waveform operations. Thus to the extent applicable to this waveform class, all configuration, management and access to all remaining services in regard to this waveform are relegated to the Platform API.

| Information Security (INFOSEC) Bypass and Confidentiality Services for: | |
|---|---|
| User communications | Waveform API |
| Network Control communications | Not Applicable |
| Device Uploads to networks (e.g., Log data, configuration data) | Not Applicable |
| Policy (security, regulatory, etc.) downloads | Platform API |
| Configuration Data downloads | Platform API |
| Software Downloads | Platform API |
| User data Storage | Platform API |
| Configuration Data Storage | Platform API |
| Key Material Storage | Platform API |
| Control Bypass | Not Applicable |
| Header Information Bypass | Not Applicable |
| Plain Text Audio Bypass | Waveform API |

#### 3.3.3.2.5 UHF TACSAT Waveform - Transmission Security (TRANSEC)

This waveform class does not require any specific TRANSEC services in support of waveform operations. Thus for this waveform all TRANSEC services are not applicable.

| Transmission Security (TRANSEC) Services for: | |
|---|---|
| Spread spectrum applications | Not Applicable |
| Frequency hopping applications | Not Applicable |
| Cover for waveform control information | Not Applicable |
| Cover for waveform data | Not Applicable |

#### 3.3.3.2.6 UHF TACSAT Waveform - Key and Credential Management Services

The IRSS API shall support the ability for the UHF TACSAT waveform to select keys to be used for traffic encryption/decryption. Some legacy cryptographic units provide capabilities for OTAR and perhaps even OTAT, but in these instances the waveforms are not aware that those operations are occurring as the functionality resides totally within the bounds of the cryptographic components which have been configured by an operator using the platform's HMI/controls. Thus any API functionality for current waveforms remains a platform API function.

This waveform class does not require any other specific Key and Credential Management services in support of waveform operations. Any usage of PINs, passwords, biometric data and other forms of electronic credentials would be strictly relegated to platform functionality and are not applicable to the waveform. To the extent applicable to this waveform class, all other configuration, management and access to key management Services are relegated to the Platform API.

| **Key and Credential Management Services for:** | |
|---|---|
| National user's shared and private keys | Waveform API |
| User PKI certificates and related private/shared keys | Not Applicable |
| User's Regional and/or Coalition shared keys | Waveform API |
| PINs, Passwords, Biometric access and other electronic credential data | Platform API |
| Device certificates and private/shared keys | Not Applicable |
| Root & intermediate Certification Authority Certificates | Not Applicable |
| Over the Air Zeroize | Not Applicable |
| Over the Air Rekey | Platform API |
| Over the Air key Transfer | Platform API |

#### 3.3.3.2.7 UHF TACSAT Waveform - Platform Resource Security Management Services

To the extent applicable to this waveform class, all configuration, management and access to Platform Resource Security Management Services are relegated to the Platform API.

| **Platform Resource Security Management Services for:** | |
|---|---|
| Memory Management Security Enforcement | Platform API |

| **Platform Resource Security Management Services for:** | |
|---|---|
| RPOE Software Configuration Management & Version Control | Platform API |
| RPA Software Configuration Management & Version Control | Platform API |

### 3.3.3.2.8 UHF TACSAT Waveform - Logging, Auditing and Security Alarm Services

To the extent applicable to this waveform class, all configuration, management and access to Logging, Auditing and Security Alarm Services are relegated to the Platform API.

| **Logging, Auditing and Security Alarm Services for:** | |
|---|---|
| Usage logs | Platform API |
| Security Event logs | Platform API |
| Cognitive/DSA Operations logs | Not Applicable |
| Non-repudiation logs | Not Applicable |
| Security Related Alarm services | Platform API |
| Audit log preparation | Platform API |

### 3.3.3.2.9 UHF TACSAT Waveform - Policy Enforcement and Management Security Services

To the extent applicable to this waveform class, all configuration, management and access to Policy Enforcement and Management Services are relegated to the Platform API.

| **Policy Enforcement and Management Security Services for:** | |
|---|---|
| The Platform security policy | Platform API |
| Waveform/application security policies | Platform API |
| SDRD Behavioral control (cognitive/learning radio) | Not Applicable |
| Regulatory Policies | Platform API |
| Other downloadable policies (e.g., Network Management, Network Security | Not Applicable |

### 3.3.3.3 UHF TACSAT Waveform - Other Relevant Characteristics

None identified at this time.

### 3.3.3.4 UHF TACSAT Waveform – Applicable API Use Case Operations

Based on the security service requirements outlined in Section 3.3.3.2, the API use case waveform operations indicated as being applicable to this waveform are identified in Table 6. Details of these operations are described in Section 4.2

**Table 6: UHF TACSAT Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | Legacy TACSAT Waveform Applicability |
|---|---|---|
| WF 01 | Setup (configure)/teardown waveform Control Channels | Yes |
| WF 02 | Update Waveform Policy | No |
| WF 03 | OTAR/OTAT (Waveform specific) | No |
| WF 04 | OTAZ (Channel specific keys/Certs) | No |
| WF 05 | Extract/Forward Audit Log | No |
| WF 06 | Setup (configure)/teardown Waveform Encryption/ Decryption Channels | Yes |
| WF 07 | Algorithm Selection | Yes |
| WF 08 | Key Selection | Yes |
| WF 09 | Reserved | - |
| WF 10 | Key Negotiation / Session Establishment | No |
| WF 11 | Encrypt / Decrypt User Traffic | Yes |
| WF 12 | Setup(configure)/teardown Waveform TRANSEC Channels | No |
| WF 13 | Perform TRANSEC Operations | No |
| WF 14 | Provide TRANSEC Keystream | No |
| WF 15 | Provide/Generate Random Number | No |
| WF 16 | Provide TRANSEC Key | No |
| WF 17 | Setup(configure)/teardown Waveform Bypass Channels | Yes |

**Table 6: UHF TACSAT Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | Legacy TACSAT Waveform Applicability |
|---|---|---|
| WF 18 | Plain Audio Text Bypass | Yes |
| WF 19 | Control Bypass | No |
| WF 20 | Header/In channel Bypass | No |
| WF 21 | Setup (configure)/teardown Waveform Authentication/ Integrity Channels | No |
| WF 22 | Authenticate Remote Device / Application | No |
| WF 23 | Authenticate Remote User (with/without physical token) | No |
| WF 24 | Authenticate Local Device/ Application | No |
| WF 25 | Authenticate file/token/data/certificate | No |
| WF 26 | Integrity Check file/token/data/certificate | No |
| WF 27 | Provide Digital Signature for file/token/data | No |
| WF 28 | Provide Hash for file/token/data | No |
| WF 29 | Verify Hash for file/token/data | No |
| WF 30 | Retrieve Certificate (s) | No |
| WF 31 | Accept/pass in Certificate | No |
| WF 32 | WF 32 Encrypt/Decrypt File/Token/Data | No |

### *3.3.4 HF 2G/3G ALE Waveform*

High Frequency (HF) radios are still an important component of tactical BLOS communications. In modern tactical HF radios channel selection has been moved from an almost “black arts” operator based craft to one which uses radios that automate the channel establishment using second and third generation Automatic Link Establishment (2G/3G HF ALE) protocols. These waveforms are detailed in US DOD military standards such as MIL-STD-188-110 and MIL-STD-188-141 as well as NATO STANAGS 4538 and 4539. The most recent standardization efforts define a family of wideband (for HF) physical layer waveforms having bandwidths in 3kHz increments (e.g., 3, 6, 9, etc.) up to 24 kHz bandwidth.

#### 3.3.4.1 HF 2G/3G ALE Waveform - Operational Characteristics

Modern HF tactical radios support of variety of data modulations and rates as well as secure digital voice and data operation. As a consequence the cryptographic capabilities cover a broad span of cryptographic equipment protocols and algorithms as well as TRANSEC operations including Frequency Hopping and cover (link protection) for ALE control information.
In some cases with these waveforms the ALE functionality is independent of the underlying data bearing waveform and thus, when enabled, must always be monitoring the received HF channel for ALE related signals which may appear during idle periods or even when other traffic is being received..

#### 3.3.4.2 HF 2G/3G ALE Waveform - Security Characteristics and Required Security Services

The specific functional services needed by the HF 2G/3G ALE waveform are identified in the remainder of this section.

##### 3.3.4.2.1 HF 2G/3G ALE Waveform - Access Control Services

Current HF waveforms do not directly require or support any access services. Thus, these services, to the extent needed to support this waveform's operations are relegated to the platform API.

| **Access Control Services (Identification and Authorization) for:** | |
|---|---|
| HMI SDRD Interface interactions | Platform API |
| Software Downloads/Updates | Platform API |
| Policy Downloads & Updates | Platform API |
| Configuration Data downloads/Updates | Platform API |
| Remote access/use of platform resources | Not applicable |

##### 3.3.4.2.2 HF 2G/3G ALE Waveform - Authentication and Non-repudiation Services

To the extent applicable to this waveform class, all configuration, management and access to Authentication or Non-repudiation Services are relegated to the Platform API.

This waveform does not require any specific services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform to the extent applicable are relegated to the Platform API.

| **Authentication and Non-repudiation Services for:** | |
|---|---|
| Users | Platform API |
| User Devices | Platform API |

| Authentication and Non-repudiation Services for: | |
|---|---|
| Network Devices | Not applicable |
| Software content providers | Not applicable |
| Network Operators | Not applicable |
| Service Providers | Not applicable |

#### 3.3.4.2.3 HF 2G/3G ALE Waveform - Information Integrity Services:

To the extent applicable to this waveform class, all configuration management and access to Information Integrity Services are relegated to the Platform API.

| Information Integrity Services for: | |
|---|---|
| Platform resident user data | Platform API |
| Waveform related resident radio & network configuration data | Platform API |
| Platform resident software and firmware | Platform API |
| Any waveform specific related downloadable data or software | Not applicable |
| Over the Air Control and configuration commands | Not applicable |

#### 3.3.4.2.4 HF 2G/3G ALE Waveform - Information Security (INFOSEC) Bypass and Confidentiality Services

HF waveforms provide diverse operations and support different modes of voice and data communications employing a variety of cryptographic protocols and algorithms. In addition, legacy waveform support of cryptographic bypass for plain text audio communications is required. Other services to the extent applicable are relegated to a platform API.

| Information Security (INFOSEC) Bypass and Confidentiality Services for: | |
|---|---|
| User communications | Waveform API |
| Network Control communications | Not applicable |
| Device Uploads to networks (e.g., Log data, configuration data) | Not applicable |
| Policy (security, regulatory, etc.) downloads | Platform API |

| **Information Security (INFOSEC) Bypass and Confidentiality Services for:** | |
|---|---|
| Configuration Data downloads | Platform API |
| Software Downloads | Platform API |
| User data Storage | Platform API |
| Configuration Data Storage | Platform API |
| Key Material Storage | Platform API |
| Control Bypass | Waveform API |
| Header Information Bypass | Waveform API |
| Plain Text Audio Bypass | Waveform API |

##### 3.3.4.2.5 HF 2G/3G ALE Waveform - Transmission Security (TRANSEC)

When operating in modes using ALE, there is the potential that the information exchanged in ALE protocols will be protected by a form of TRANSEC cover referred to as “Link Protection”, a basic form of which is defined by the current military standard for ALE (MIL-STD-188-141B). The standard permits different levels of link protection. Depending upon platform security requirements, the Link protection information may be generated and applied by the waveform or the keystream used for the link protection could be generated by the CSF and applied by the waveform. The IRSS waveform API shall support both options.

In addition, HF tactical radios also provide a frequency hopping capability. The capabilities defined for other waveforms in this document should be adequate to support HF waveform frequency hopping and other TRANSEC operations.

| **Transmission Security (TRANSEC) Services for:** | |
|---|---|
| Spread spectrum applications | Waveform API |
| Frequency hopping applications | Waveform API |
| Cover for waveform control (ALE) information | Waveform API |
| Cover for waveform data | Not Applicable |

##### 3.3.4.2.6 HF 2G/3G ALE Waveform - Key and Credential Management Services

The IRSS API shall support the ability for the HF 2G/3G ALE waveform to select keys to be used for traffic encryption/decryption and for TRANSEC operations include ALE link protection functions. Some legacy cryptographic units provide capabilities for OTAR and perhaps even OTAT, but in these instances the waveforms are not aware that those operations are occurring as the functionality resides totally within the bounds of the cryptographic components which have been configured which have been configured by an operator using the platform's HMI/controls. Thus any API OTAR or OTAT functionality for current waveforms remains a platform API function.

Any usage of PINs, passwords, biometric data and other forms of electronic credentials would be strictly relegated to platform functionality and are not applicable to the waveform.

This waveform class does not require any other specific Key and Credential Management services in support of waveform operations.

The remaining services, to the extent applicable to this waveform class, are assumed to be a platform API and not a waveform API.

| **Key and Credential Management Services for:** | |
|---|---|
| User's National shared and private keys | Waveform API |
| User PKI certificates and related private/shared keys | Not Applicable |
| Regional and/or Coalition shared keys | Waveform API |
| PINs, Passwords, Biometric access and other electronic credential data | Platform API |
| Device certificates and private/shared keys | Not Applicable |
| Root & intermediate Certification Authority Certificates | Not Applicable |
| Over the Air Zeroize | Not Applicable |
| Over the Air Rekey | Platform API |
| Over the Air key Transfer | Platform API |

#### 3.3.4.2.7 HF 2G/3G ALE Waveform - Platform Resource Security Management Services

To the extent applicable to this waveform class, all configuration, management and access to Platform Resource Security Management Services are relegated to the Platform API.

| **Platform Resource Security Management Services for:** | |
|---|---|
| Memory Management Security Enforcement | Platform API |

| Platform Resource Security Management Services for: | |
|---|---|
| RPOE Software Configuration Management & Version Control | Platform API |
| RPA Software Configuration Management & Version Control | Platform API |

### 3.3.4.2.8 HF 2G/3G Waveform Logging, Auditing and Security Alarm Services

To the extent applicable to this waveform class, configuration, management and access to Logging, Auditing and Security Alarm Services are relegated to a platform API.

| Logging, Auditing and Security Alarm Services for: | |
|---|---|
| Usage logs | Platform API |
| Security Event logs | Platform API |
| Cognitive/DSA Operations logs | Not Applicable |
| Non-repudiation logs | Platform API |
| Security Related Alarm services | Platform API |
| Audit log preparation | Platform API |

### 3.3.4.2.9 HF 2G/3G Waveform Policy Enforcement and Management Security Services

To the extent applicable to this waveform class, all configuration, management and access to Policy Enforcement and Management Services are relegated to the Platform API.

| Policy Enforcement and Management Security Services for: | |
|---|---|
| The Platform security policy | Platform API |
| Waveform/application security policies | Platform API |
| SDRD Behavioral control (cognitive/learning radio ) | Not Applicable |
| Regulatory Policies | Platform API |
| Other downloadable policies (e.g., Network Management, Network Security | Not Applicable |

### 3.3.4.3 HF 2G/3G Waveform Other Relevant Characteristics

During waveform operations when the ALE functions have been activated, there is the possibility that the ALE function will detect an incoming ALE request from another radio. ALE settings will determine whether or not the ongoing link traffic will be interrupted to permit the radio to respond to the ALE request. To respond, the waveform would have to temporarily cease any cryptographic operations that may be occurring and later resume these operations when the ALE exchange is finished. This function will necessitate the ability of the waveform to cause a cessation and later resumption of the cryptographic operations without tearing down any cryptographic channels.

#### 3.3.4.4 HF 2G/3G Waveform - Required API Use Case Waveform Operations

Based on the security service requirements outlined in Section 3.3.4.2, the API use case waveform operations indicated as being applicable to this waveform are identified in Table 7. Details of these operations are described in Section 4.2

**Table 7: HF 2G/3G Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | Waveform Applicability |
|---|---|---|
| WF 01 | Setup (configure)/teardown waveform Control Channels | Yes |
| WF 02 | Update Waveform Policy | No |
| WF 03 | OTAR/OTAT (Waveform specific) | Yes |
| WF 04 | OTAZ (Channel specific keys/Certs) | No |
| WF 05 | Extract/Forward Audit Log | No |
| WF 06 | Setup (configure)/teardown Waveform Encryption/ Decryption Channels | Yes |
| WF 07 | Algorithm Selection | Yes |
| WF 08 | Key Selection | Yes |
| WF 09 | Reserved | - |
| WF 10 | Key Negotiation / Session Establishment | No |
| WF 11 | Encrypt / Decrypt User Traffic | Yes |
| WF 12 | Setup (configure)/teardown Waveform TRANSEC Channels | Yes |
| WF 13 | Perform TRANSEC Operations | Yes |
| WF 14 | Provide TRANSEC Keystream | Yes |
| WF 15 | Provide/Generate Random Number | Yes |

### Table 7: HF 2G/3G Waveform - Applicable API Use Case Operations

| ID | API Use Case Waveform Operation | Waveform Applicability |
|---|---|---|
| WF 16 | Provide TRANSEC Key | No |
| WF 17 | Setup (configure)/teardown Waveform Bypass Channels | Yes |
| WF 18 | Plain Audio Text Bypass | Yes |
| WF 19 | Control Bypass | Yes |
| WF 20 | Header/In channel Bypass | No |
| WF 21 | Setup (configure)/teardown Waveform Authentication/ Integrity Channels | No |
| WF 22 | Authenticate Remote Device / Application | No |
| WF 23 | Authenticate Remote User (with/without physical token) | No |
| WF 24 | Authenticate Local Device/ Application | No |
| WF 25 | Authenticate file/token/data/certificate | No |
| WF 26 | Integrity Check file/token/data/certificate | No |
| WF 27 | Provide Digital Signature for file/token/data | No |
| WF 28 | Provide Hash for file/token/data | No |
| WF 29 | Verify Hash for file/token/data | No |
| WF 30 | Retrieve Certificate (s) | No |
| WF 31 | Accept/pass in Certificate | No |
| WF 32 | WF 32 Encrypt/Decrypt File/Token/Data | No |

### *3.3.5 VHF/UHF LOS Waveform*

This class of waveforms includes simple two-way VHF or UHF line of sight waveforms used for tactical Ground to Ground and Air Ground Air as well as air-air communications. Security measures include voice and data encryption as well as ECCM techniques, for example measures such as frequency hopping. Current examples of this class include standard include the VULOS, SINCGARS and HAVEQUICK waveforms which typically operate on 25 kHz channels. Current operations ongoing in Central Asia involve multinational coalition forces. Operations such as this demonstrate the critical need for interoperable communications. All too often interoperability is achieved by an exchange of radios at different levels of command in order for the deployed forces to be able to communicate with each other. Future coalition networks will need greater interoperability and the ability to communicate amongst themselves on shared communication channels. The potential exists for these 25 kHz channel radio waveforms to evolve in order to facilitate coalition force operations. For these reason this section will consider possible additional capabilities for consideration as to how the API could support such future features.

An effective alliance force structure is based on force contributions from both allied (e.g. NATO) and non-allied nations leading to multinational force structures operating cooperatively down to ever lower levels of command, e.g. company level. The principle communications mechanism to support command and control at lower levels is combat radio mainly operating in the military VHF/UHF frequency bands. As we have observed, interoperability between nations currently is very limited and then mostly unsecure. To enhance operational effectiveness an API set supporting both secure voice and data has to be defined. The main area of operation of such a waveform is used for ground to ground, ground to air and ground to sea (littoral) operation.

In operations such as these radios from different participating nations' forces need to communicate with each other on short notice and without special preparation of the radio on site. As an example, NATO-Nation A and Non-NATO nation B as well as organization C (perhaps a local cooperating authority) have to communicate in theatre. This can be realized without any local interaction with their equipment, such as additional key filling, etc., by developing new waveforms whose signaling protocols support the security features necessary to ensure the security of the joint operations.

The principal flow of events can be outlined as follows:

1. The participating radios join the Deployed CoI groups.
2. Individual radios are authenticated as they join
3. The session keys for confidentiality protection are negotiated between designated units and distributed to the group participants using asymmetric key technology.
4. Secured channels are set up.
5. All terminals can participate in the group communication.

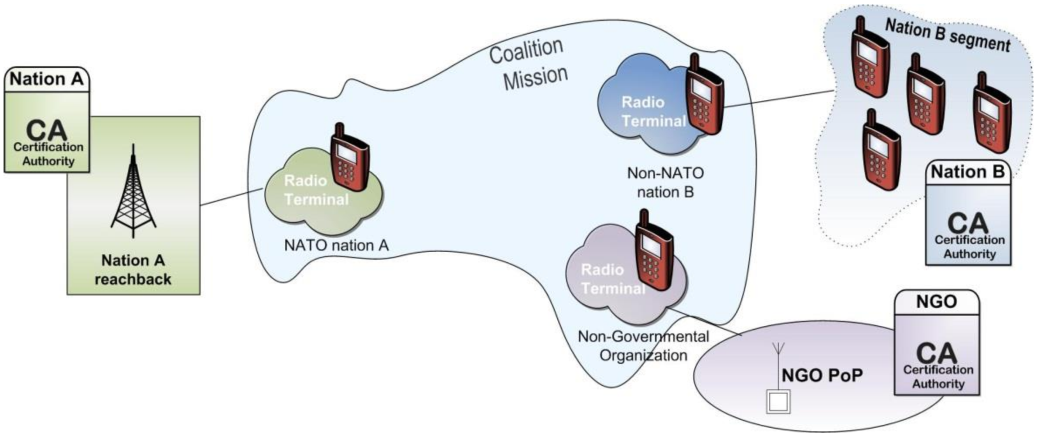


**Figure 4: Dynamic formation of Community of Interests**

This of course assumes that a common interoperable waveform is present in all coalition force radios. In order for such a waveform to be ported to diverse radio platforms, a common set of API's, especially for Radio Security Services is essential.

Note: in a deployed coalition operation, several Communities-of-Interest may co-exist with a need for passing encrypted user traffic in national or other negotiated keys, but without the need for private encryption of the network control traffic. Consequently common independent levels of protection at the network layer could be used while for user traffic a combination of national, allied and common coalition forces keys could be employed.

However, since such Dynamic Group Key Establishment and distribution methods have not yet been developed for military use, pre-placed keys for each CoI group will likely be necessary in the interim. To facilitate both current and future operations a common cryptographic key tag structure and format would facilitate the distribution of keys amongst the coalition force participants an aiding in misidentification or misuse of key material.

#### 3.3.5.1 VHF/UHF LOS Waveform - Operational Characteristics

This class of waveforms include simple waveforms such standard clear voice over VHF FM and UHF AM channels, as well as waveforms providing both INFOSEC and TRANSEC functions such as the SINCGARS, and HAVEQUICK I/II waveforms. Also considered are the needs of next generation waveforms to meet the emerging requirements derived from operations involving allied and coalition forces as highlighted in the preceding section.

#### 3.3.5.2 VHF/UHF LOS Waveform - Security Characteristics and Required Security Services

The protection requirements for the application data, telemetry, network access and control layers may be different. So separation of protection of the Transport Domain and the Information Domain should be supported in tactical environments. It is possible that separate protection between the different sub layers within the transportation domain may be needed. Figure 5 provides a notional view of the separation between transport domain and information domain as well as different sub layers of the Transport Domain.

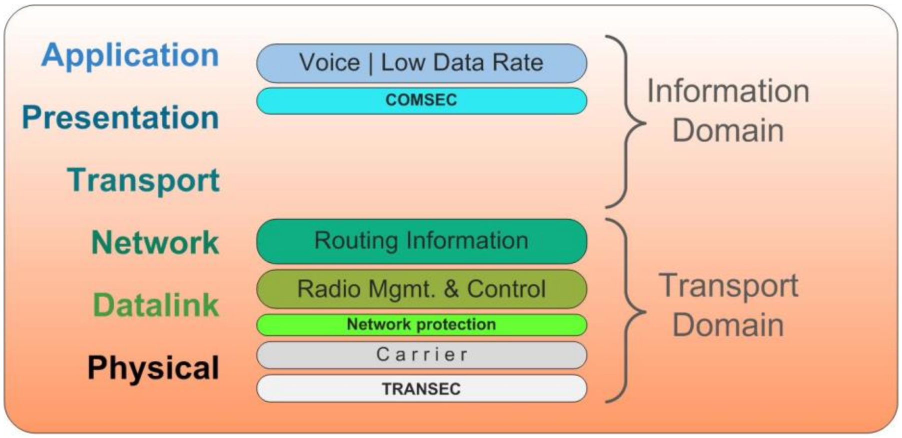


**Figure 5: Potential layers of (confidentiality) protection**

A logical high level architecture of such radio could be as shown in Figure 6. Again it may worth highlighting that there can be up to three layers of protection, denoted in this figure as TRANSEC, LINKSEC, and COMSEC. We see a similar form in the HF ALE 2G/3G waveform. Some forms of TRANSEC need to be integral parts of the waveform (e.g. frequency hopping, spread spectrum, etc.) while COMSEC is quite independent from the carrier. Between the two layers there may be routing, network and/or radio control information to be protected. These all may be at the same or different levels of classification, but regardless they could all be independent operations each using their specified algorithms and keys.

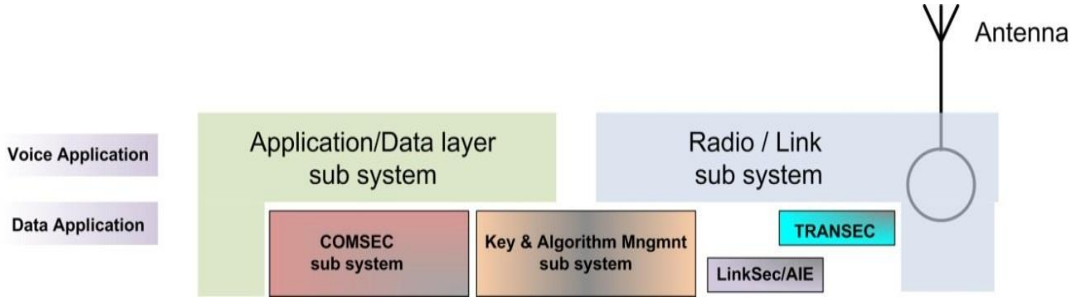


**Figure 6: High level overview on the security components in a combat radio**

### 3.3.5.2.1 VHF/UHF LOS Waveform - Access Control Services

In today’s conventional VHF/UHF LOS radio networks access control functions are local to the radio if indeed such a function even exists. Radio controls are inherent to the radio front panel in ground radios and to a cockpit interface in tactical fixed/rotary wing aircraft. As such formal access control mechanisms are rare and in many respects are undesired since user/operators lives are in jeopardy in combat operations. Future operations are speculative, and it is possible that some of the functions in the table below might one day apply to radios using this class of waveform. It is expected that any such functions will be similar to those already in use by those radios which already support such operations. Consequently for this class of radio waveform the presumption is that any operations listed in the table would be relegated to a radio platform API.

| Access Control Services (Identification and Authorization) for: | |
|---|---|
| HMI SDRD Interface interactions | Platform API |
| Software Downloads/Updates | Platform API |
| Policy Downloads & Updates | Platform API |
| Configuration Data downloads/Updates | Platform API |
| Remote access/use of platform resources | Platform API |

#### 3.3.5.2.2 VHF/UHF LOS Waveform - Authentication and Non-repudiation Services

Authentication and non-repudiation services involve methods to unambiguously identify an entity (device or user) via their credentials, authenticate that identity and any information provided by the entity and, when necessary, to record in a security log data relevant to the activity so that the event and/or data cannot be repudiated by the entity. Additionally positive identification and mutual authentication is required between any entity joining the network and any entity which is already a part of the network. This is aimed at preventing either a legitimate device or the network from being impersonated by adversarial forces and allowing the network to be compromised as a result.

In typical VHF/UHF combat radios using these waveforms there are no formal methods or protocols by which identification or authentication occurs. The presumption is that if the radio has the correct keys and hopsets, then it is a legitimate device (although its user may not be). User identification is typically performed by speaker recognition. Emerging and future radio systems are likely to have the capabilities to support formal (e.g. PKI based) methods of authentication and user identification..

Notwithstanding these possibilities, specifics of these types of operations might be considered speculative. Thus, this waveform does not require any specific Authentication or Non-repudiation services in support of waveform operations. Thus configuration, management and access to all such services in regard to this waveform to the extent applicable are relegated to the Platform API. Future versions of this waveform will likely require services as indicated in the table below.

| Authentication and Non-repudiation Services for: | |
|---|---|
| Users | Platform API |
| User Devices | Platform/Future Waveform API |
| Network Devices | Not Applicable/Future Waveform API |

| Authentication and Non-repudiation Services for: | |
|---|---|
| Software content providers | Platform API |
| Network Operators | Not Applicable/Future Waveform API |
| Service Providers | Not Applicable/Future Waveform API |

#### 3.3.5.2.3 VHF/UHF LOS Waveform - Information Integrity Services

To the extent that future applications of these waveforms employ network or radio control then information integrity is likely to be employed. It is believed that any of these operations will be similar or identical to those in use for other waveforms which do support the need for these services.

| Information Integrity Services for: | |
|---|---|
| Platform resident user data | Platform API |
| Waveform related resident radio & network configuration data | Platform API |
| Platform resident software and firmware | Platform API |
| Any waveform specific related downloadable data or software | Platform API |
| Over the Air Control and configuration commands | Not Applicable/Future Waveform API |

#### 3.3.5.2.4 VHF/UHF LOS Waveform - Information Security (INFOSEC) Bypass and Confidentiality Services

INFOSEC services can provide encryption and decryption services for User communications as well as Network Control communications, as well as for platform resident data and software. For this waveform these services will be provided as summarized in the table and described below. The protection levels needed for the User communication (i.e. in the information domain) and for the Network Control (i.e. in the transport domain) are likely to be different. The IRSS API Security Services shall allow for a protection (encryption) layer for each of those with different setups in terms of keys, algorithms, modes etc.

Encryption and decryption services must be supported for all user communications and any required network control and management functions. In the information domain, this includes the ability to support multiple algorithms or cryptographic unit emulations each employing one or more COMSEC Keys as might be used in support of National, Regional and/or Coalition force communications. The control and routing information of the transport domain may be used on a netted (all-informed) protection scheme among all partners or certain classes of information may need separate protection. For this kind of information the sharing of transport related data among all CoIs is less critical than for the content itself.

If future 25kHz tactical networks are going to support shared usage radio channels on which national, NATO (or similar alliances) and non-allied coalition forces can be simultaneously communicating amongst themselves as well as to their allied/coalition partners, then a means for a radio to identify which key to use to decrypt received signals and a schema to select the correct encryption key for transmission will be essential.

Proper decryption key selection is perhaps the simplest to solve since the cryptographic protocol could embed information in the encrypted transmission that could identify the class of key to use and high speed cryptographic hardware could quickly cycle through a selection of keys to find the proper key.

However, selecting the correct key for transmission must be done in such a way that a user does not inadvertently broadcast sensitive national information to a coalition or allied partner. This may be particularly challenging since the user may not have direct access to a control panel and the radio handset may be the only device readily available. Any such method would have to be failsafe in operation and is could be platform specific. Certainly a new handset, headset device could be developed but that might require a significant modification to the standardized headset connectors and interface.

| **Information Security (INFOSEC) Bypass and Confidentiality Services for:** | |
|---|---|
| User communications | Waveform API |
| Network Control communications | Not Applicable/Future Waveform API |
| Device Uploads to networks (e.g., Log data, configuration data) | Not Applicable/Future Waveform API |
| Policy (security, regulatory, etc.) downloads | Platform/Future Waveform API |
| Configuration Data downloads | Platform/Future Waveform API |
| Software Downloads | Platform API |
| User data Storage | Platform API |
| Configuration Data Storage | Platform API |
| Key Material Storage | Platform API |
| Control Bypass | Waveform API |
| Header Information Bypass | Waveform API |

| Information Security (INFOSEC) Bypass and Confidentiality Services for: | |
|---|---|
| Plain Text Audio Bypass | Waveform API |

### 3.3.5.2.5 VHF/UHF LOS Waveform - Transmission Security (TRANSEC)

The availability of the physical carrier is paramount for the users' (e.g. soldiers') situational awareness. For instance, solid anti-jamming protection needs to be present. This is a feature of existing waveforms such as SINCGARS and HAVEQUICK and it is likely to be relevant to future 25 kHz channel tactical waveforms as well.

| Transmission Security (TRANSEC) Services for: | |
|---|---|
| Spread spectrum applications | Waveform API |
| Frequency hopping applications | Waveform API |
| Cover for waveform control information | Not Applicable/Future Waveform API |
| Cover for waveform data | Not Applicable/Future Waveform API |

### 3.3.5.2.6 VHF/UHF LOS Waveform - Key and Credential Management Services

The IRSS API shall support the ability for the VHF/UHF LOS waveform to select keys to be used for traffic encryption/decryption as well as TRANSEC operations. Some legacy cryptographic units provide capabilities for OTAR and perhaps even OTAT, but in these instances the waveforms are not aware that those operations are occurring as the functionality resides totally within the bounds of the cryptographic components which have been configured by an operator using the platform’s HMI/controls. Thus any OTAR/OTAT API functionality for current waveforms remains a platform API function.

Any usage of PINs, passwords, biometric data and other forms of electronic credentials would be strictly relegated to platform functionality and are not applicable to the waveform. This waveform class does not require any other specific Key and Credential Management services in support of waveform operations.

Future waveforms are likely to include many of these other functions but the operations may still be relegated completely to the CSF and embedded into the cryptographic equipment emulation protocols but the current API set should consider the nature of API operations should the waveform become involved. As noted earlier a common key tag structure and format could facilitate distribution and interoperability in coalition and allied force operations.

| Key and Credential Management Services for: | |
|---|---|
| User's National shared and private keys | Waveform API |
| User PKI certificates and related private/shared keys | Not Applicable/Future Waveform API |
| Regional and/or Coalition shared keys | Waveform API |
| PINs, Passwords, Biometric access and other electronic credential data | Platform API |
| Device certificates and private/shared keys | Not Applicable/Future Waveform API |
| Root & intermediate Certification Authority Certificates | Not Applicable/Future Platform API |
| Over the Air Zeroize | Not Applicable/Future Waveform API |
| Over the Air Rekey | Platform/Future Waveform API |
| Over the Air key Transfer | Platform /Future Waveform API |

#### 3.3.5.2.7 VHF/UHF LOS Waveform - Platform Resource Security Management Services

To the extent applicable to this waveform class, all configuration, management and access to Platform Resource Security Management Services are relegated to the Platform API.

| Platform Resource Security Management Services for: | |
|---|---|
| Memory Management Security Enforcement | Platform API |
| RPOE Software Configuration Management & Version Control | Platform API |
| RPA Software Configuration Management & Version Control | Platform API |

#### 3.3.5.2.8 VHF/UHF LOS Waveform - Logging, Auditing and Security Alarm Services

To the extent applicable to this waveform class, configuration, management and access to Logging, Auditing and Security Alarm Services are relegated to a platform API. Future waveform examples could employ the API facilities postulated for the IPBAHN waveform.

| Logging, Auditing and Security Alarm Services | |
|---|---|
| Usage logs | Platform API |
| Security Event logs | Platform API |
| Cognitive/DSA Operations logs | Not Applicable |
| Non-repudiation logs | Platform API |
| Security Related Alarm services | Platform API |
| Audit log preparation | Platform API |

#### 3.3.5.2.9 VHF/UHF LOS Waveform - Policy Enforcement and Management Security Services

To the extent applicable to this waveform class, all configuration, management and access to Policy Enforcement and Management Services are relegated to the Platform API.

Future generations of this waveform class may be required to be cognizant of security and other network related policies.

| Policy Enforcement and Management Security Services for: | |
|---|---|
| The Platform security policy | Platform API |
| Waveform/application security policies | Platform/Future Waveform API |
| SDRD Behavioral control (cognitive/learning radio ) | Not Applicable |
| Regulatory Policies | Platform API |
| Other downloadable policies (e.g., Network Management, Network Security) | Not Applicable/Future Waveform API |

### 3.3.5.3 VHF/UHF LOS Waveform - Other Relevant Characteristics

None identified.

### 3.3.5.4 VHF/UHF LOS Waveform - Required API Use Case Waveform Operations

Based on the security service requirements outlined in Section 3.3.5.2 the API use case waveform operations indicated as being applicable to this waveform are identified in Table 8. Details of these operations are described in Section 4.2

**Table 8: VHF/UHF LOS Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | VHF/UHF Waveform Applicability | |
|---|---|---|---|
| | | Current Generation | Future Coalition |
| WF 01 | Setup (configure)/teardown waveform Control Channels | Yes | Yes |
| WF 02 | Update Waveform Policy | No | No |
| WF 03 | OTAR/OTAT (Waveform specific) | Yes | Yes |
| WF 04 | OTAZ (Channel specific keys/Certs) | No | Yes |
| WF 05 | Extract/Forward Audit Log | No | No |
| WF 06 | Setup (configure)/teardown Waveform Encryption/ Decryption Channels | Yes | Yes |
| WF 07 | Algorithm Selection | Yes | Yes |
| WF 08 | Key Selection | Yes | Yes |
| WF 09 | Reserved | - | - |
| WF 10 | Key Negotiation / Session Establishment | No | Yes |
| WF 11 | Encrypt / Decrypt User Traffic | Yes | Yes |
| WF 12 | Setup (configure)/teardown Waveform TRANSEC Channels | Yes | Yes |
| WF 13 | Perform TRANSEC Operations | Yes | Yes |
| WF 14 | Provide TRANSEC Keystream | Yes | Yes |
| WF 15 | Provide/Generate Random Number | Yes | Yes |
| WF 16 | Provide TRANSEC Key | Yes | Yes |
| WF 17 | Setup (configure)/teardown Waveform Bypass Channels | Yes | Yes |
| WF 18 | Plain Audio Text Bypass | Yes | Yes |
| WF 19 | Control Bypass | Yes | Yes |
| WF 20 | Header/In channel Bypass | No | Yes |

**Table 8: VHF/UHF LOS Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | VHF/UHF Waveform Applicability | |
|---|---|---|---|
| | | Current Generation | Future Coalition |
| WF 21 | Setup (configure)/teardown Waveform Authentication/ Integrity Channels | No | Yes |
| WF 22 | Authenticate Remote Device / Application | No | Yes |
| WF 23 | Authenticate Remote User (with/without physical token) | No | Yes |
| WF 24 | Authenticate Local Device/ Application | No | No |
| WF 25 | Authenticate file/token/data/certificate | No | No |
| WF 26 | Integrity Check file/token/data/certificate | No | No |
| WF 27 | Provide Digital Signature for file/token/data | No | Yes |
| WF 28 | Provide Hash for file/token/data | No | Yes |
| WF 29 | Verify Hash for file/token/data | No | Yes |
| WF 30 | Retrieve Certificate (s) | No | Yes |
| WF 31 | Accept/pass in Certificate | No | Yes |
| WF 32 | WF 32 Encrypt/Decrypt File/Token/Data | No | Yes |

## 3.4 Public Safety Waveforms

There are two internationally recognized and standardized waveforms serving the public safety community around the globe. These are the P25 waveform developed by the Telecommunications Industry Association (TIA) in the USA (see ref. (TIA, 2012) and related specifications), and the Tetra waveform developed in the European Community (see (TETRA + Critical Communications Association)) Proprietary non-standardized waveforms are not considered in this document.

### *3.4.1 P25 Waveform*

Thus far the waveforms we have been discussing either rely on either sparse or non-existent infrastructure other than satellites. This is not the case for public safety communications systems. For these systems, in addition to handheld and vehicular radios, there are fixed and mobile infrastructure elements (Relay stations, base stations, and fixed locations like 911 centers, and other communication facilities as well as end users) which provide access to fixed facilities as well as to fixed and mobile control/management elements.

#### 3.4.1.1 P25 Waveform - Operational Characteristics

The P25 system provides the public safety community the ability for secure and non-secure voice and data communications. The system operates on 12.5 kHz communication channels.

As this report is being prepared, the Public Safety Community is developing the standards for services which will be provided for use in the recently allocated Long Term Evolution (LTE) band in the USA. When completed these may involve additional security services or different application of current P25 security services

#### 3.4.1.2 P25 Waveform - Security Characteristics and Required Security Services

Figure 7 illustrates the P25 reference model. In the context of this document, the P25 Subscriber Unit (SU) corresponds to the SDRD, and the $U_m$ and $U_{m2}$ reference points carry the P25 waveform. As a general rule, the bolded elements (Consoles, Subscriber Units, Key Fill Devices, and Key Management Facilities) are thought of as belonging to a user organization, while the non-bolded elements are owned by an operator (which may or may not be in the same organization as the users, but are certainly not part of the same security domain).

Project 25 key management is performed via a Key Management Facility (KMF) and employs either manual keying (i.e. through a key fill device), or Over-The-Air-Rekeying through point-to-point IP packet exchange over the P25 waveform.

Figure 8 illustrates the protocols stacks for Project 25 security. As illustrated, Project 25 voice is end-to-end encrypted and relayed through the RFSS by the P25 waveform. Optionally, the subscriber unit may be authenticated to the RFSS and vice versa through "link layer authentication" protocols which may be thought of as part of or above the P25 waveform itself.

Keys may be distributed either via OTAR or manually. In either case key security is provided between the key management facility and the SU. A second layer of security is optionally provided for OTAR, but is not present for manually loaded keys.

##### 3.4.1.2.1 P25 Waveform - Access Control Services

Project 25 does not standardize man-machine interfaces, software management, policy management, or configuration data (with the exception of security key management), and has no mechanisms for remote use of the radio platform. Therefore, Access Control Services as defined herein are all considered to be part of the Platform API.

| Access Control Services (Identification and Authorization) for: | |
|---|---|
| HMI SDRD Interface interactions | Platform API |
| Software Downloads/Updates | Platform API |
| Policy Downloads & Updates | Platform API |

| Access Control Services (Identification and Authorization) for: | |
|---|---|
| Configuration Data downloads/Updates | Platform API |
| Remote access/use of platform resources | Not Applicable |

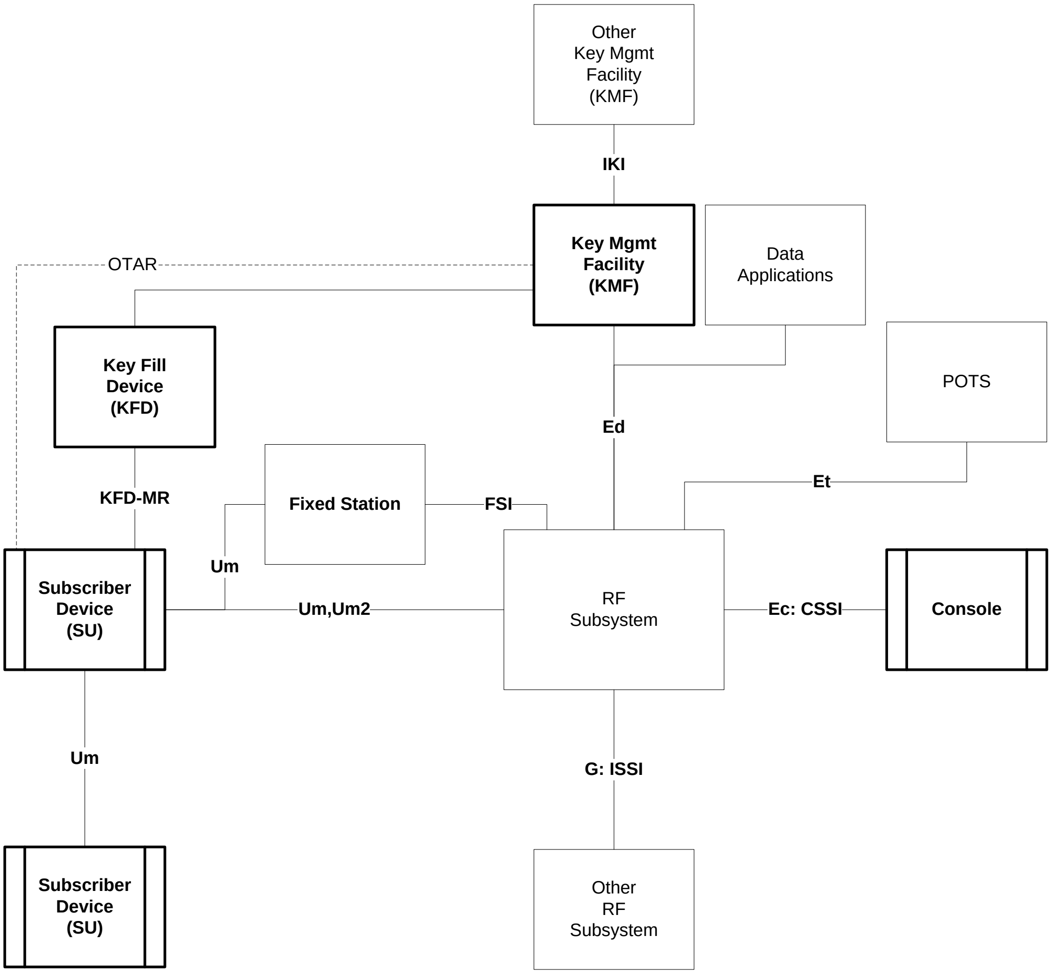


**Figure 7: Project 25 Reference Model**

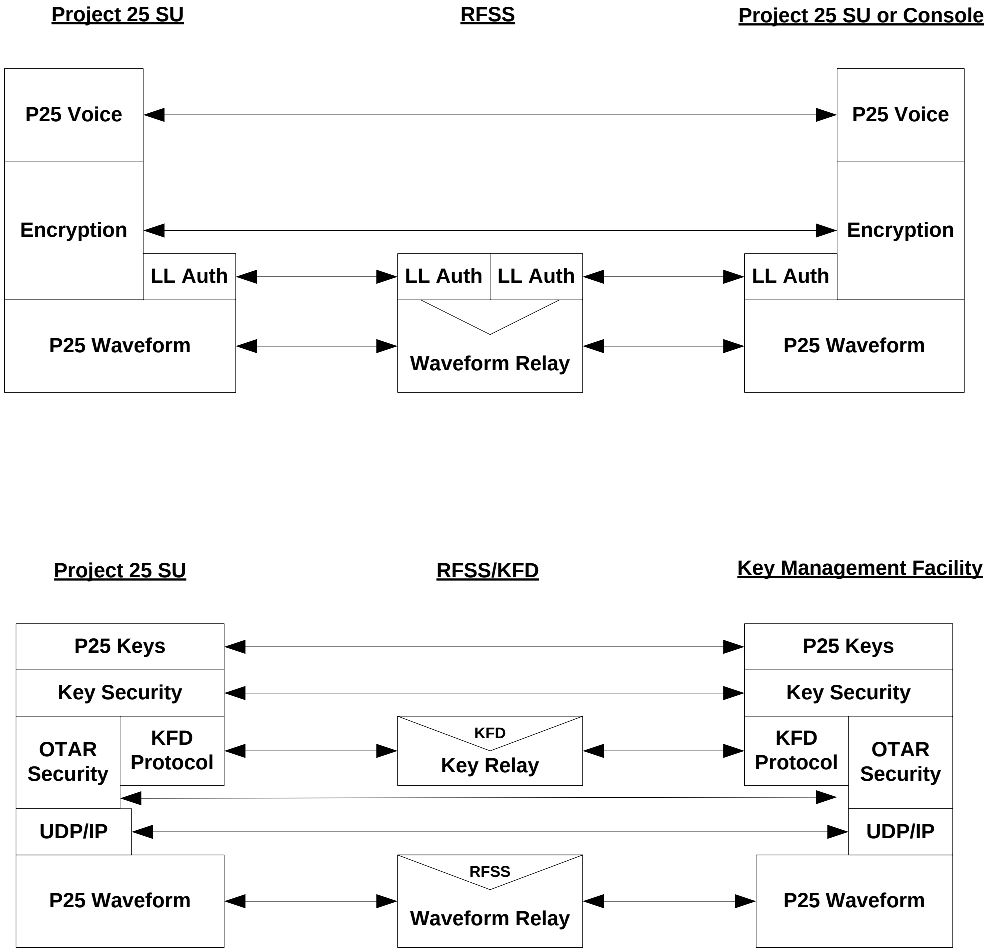


**Figure 8: Project 25 Protocol Stacks**

### 3.4.1.2.2 P25 Waveform - Identification, Authentication and Non-repudiation Services

The Project 25 waveform specifies a mutual authentication technique by which a subscriber unit (SDRD) may be authenticated to the infrastructure and vice versa. Thus authentication of User Devices and Network Operators (i.e. "the infrastructure") is part of the Waveform API and employs a non-PKI based authentication mechanism which requires the use of a pseudorandom (PN) number which could either be generated by the CSF or by a suitable algorithm in the waveform. For purposes of this specification we shall assume the CSF is the source of the PN number. P25 uses the higher order Secure Hash Algorithms (SHA), such as SHA256.

Users, Network Devices, Software Content Providers, and Service Providers have no identity per se in P25, and the related services are either not applicable or relegated to a Platform API.

The P25 waveform does not require any Non-repudiation services.

| Authentication and Non-repudiation Services for: | |
|---|---|
| Users | Platform API |
| User Devices | Waveform API |
| Network Devices | Not Applicable |
| Software content providers | Not Applicable |
| Network Operators | Not Applicable |
| Service Providers | Not Applicable |

#### 3.4.1.2.3 P25 Waveform - Information Integrity Services

The Project 25 suite of standards is mute with regard to information integrity. Thus all information integrity services, to the extent they are applicable to a specific platform implementation, are relegated to a Platform API.

| Information Integrity Services for: | |
|---|---|
| Platform resident user data | Platform API |
| Waveform related resident radio & network configuration data | Platform API |
| Platform resident software and firmware | Platform API |
| Any waveform specific related downloadable data or software | Platform API |
| Over the Air Control and configuration commands | Platform API |

#### 3.4.1.2.4 P25 Waveform - Information Security (INFOSEC) Bypass and Confidentiality Services

Project 25 specifies end-to-end encryption for voice, therefore INFOSEC for user communications are part of the Waveform API. In addition, specific implementations may require the use of the bypass services. All other INFOSEC services, to the extent supported by a particular device instance, are related to the Platform API.

| Information Security (INFOSEC) Bypass and Confidentiality Services for: | |
|---|---|
| User communications | Waveform API |
| Network Control communications | Platform API |
| Device Uploads to networks (e.g., Log data, configuration data) | Platform API |
| Policy (security, regulatory, etc.) downloads | Platform API |
| Configuration Data downloads | Platform API |
| Software Downloads | Platform API |
| User data Storage | Platform API |
| Configuration Data Storage | Platform API |
| Key Material Storage | Platform API |
| Control Bypass | Waveform API |
| Header Information Bypass | Waveform API |
| Plain Text Audio Bypass | Waveform API |

#### 3.4.1.2.5 P25 Waveform - Transmission Security (TRANSEC)

Project 25 does not define any service for Transmission Security. Therefore, all TRANSEC services are Not Applicable.

| Transmission Security (TRANSEC) Services for: | |
|---|---|
| Spread spectrum applications | Not Applicable |
| Frequency hopping applications | Not Applicable |
| Cover for waveform control information | Not Applicable |
| Cover for waveform data | Not Applicable |

#### 3.4.1.2.6 P25 Waveform - Key and Credential Management Services

P25 Key management is based on the use of pre-placed keys, although the waveform does support an OTAR function as well as an over the air zeroize (OTAZ) which will be summarized below. When joint operations with other organizations are required multiple keys can be stored and have their usage associated with specific talk groups.

P25 currently does not utilize any public/private asymmetric key functionality and thus does not require any digital certificates or related materials. This may change as P25 operations migrate to the national public safety network being planned for the LTE band. Any such future usage by P25 is likely to be addressed by current waveforms already addressed in preceding sections.

Any usage of PINs, passwords, biometric data and other forms of electronic credentials would be strictly relegated to platform functionality and are not applicable to the waveform.

Over the Air key management functions are supported by the P25 system and are managed by a Key Management Facility using a Key Management Message (KMM) structure, supporting rekeying and other functions,. The KMM's are sent over the air using IP packets. These packets, when containing key material, are doubly encrypted. One layer, which is the inner layer encrypts the key material in a Unique Key Encryption Key (UKEK. The key material may be comprised of individual keys or sets of keys. The outer layer of encryption encrypts both the key management message and the inner layer as well. Hence the key material is doubly encrypted when sent over the air.

The outer layer of encryption uses a specialized key which also serves to authenticate the source of a KMM.  For the purposes of this document it shall be assumed that the P25 Waveform will configure a BLACK SIDE to BLACK side decryption channel for purposes of decrypting/authenticating the KMMs. Not all KMM's would necessarily be passed into the CSF Once authenticated the KMM message would then be passed into the CSF where the key material would be decrypted and placed into storage. This assumes that the CSF will be able to interpret the P25 KMM suite of messages, including the command to change over from one keyset to another keyset, as well as the various zeroization commands.

The Zeroize KMM's allow zeroization of individual keys, keysets or all keys.

| **Key and Credential Management Services:** | |
|---|---|
| User's National/organizational shared and private keys | Waveform API |
| User PKI certificates and related private/shared keys | Not Applicable |
| Regional and/or Coalition shared keys | Waveform API |
| PINs, Passwords, Biometric access and other electronic credential data | Platform API |
| Device certificates and private/shared keys | Not Applicable |
| Root & intermediate Certification Authority Certificates | Not Applicable |

| **Key and Credential Management Services:** | |
|---|---|
| Over the Air Zeroize (OTAZ) | Waveform API |
| Over the Air Rekey (OTAR) | Waveform API |
| Over the Air key Transfer (OTAT) | Waveform API |

#### 3.4.1.2.7 P25 Waveform - Platform Resource Security Management Services

Project 25 does not specify platform security management services, so to the extent applicable to a device, all configuration, management and access to Platform Resource Security Management Services are relegated to the Platform API.

| **Platform Resource Security Management Services:** | |
|---|---|
| Memory Management Security Enforcement | Platform API |
| RPOE Software Configuration Management & Version Control | Platform API |
| RPA Software Configuration Management & Version Control | Platform API |

#### 3.4.1.2.8 P25 Waveform - Logging, Auditing and Security Alarm Services

Project 25 does not specify Logging, Auditing or Security Alarm services, so to the extent applicable to a device, these services are relegated to a platform API.

| **Logging, Auditing and Security Alarm Services** | |
|---|---|
| Usage logs | Platform API |
| Security Event logs | Platform API |
| Cognitive/DSA Operations logs | Not Applicable |
| Non-repudiation logs | Not Applicable |
| Security Related Alarm services | Platform API |
| Security Related Alarm services | Platform API |

#### 3.4.1.2.9 P25 Waveform - Policy Enforcement and Management Security Services

Project 25 does not standardize Policy Enforcement and Management Services, so to the extent they are applicable a device, such services are relegated to the Platform API.

| **Policy Enforcement and Management Security Services for:** | |
|---|---|
| The Platform security policy | Platform API |
| Waveform/application security policies | Not applicable |
| SDRD Behavioral control (cognitive/learning radio ) | Not Applicable |
| Regulatory Policies | Platform API |
| Other downloadable policies (e.g., Network Management, Network Security | Not Applicable |

### 3.4.1.3 P25 Waveform - Other Relevant Characteristics

None identified

### 3.4.1.4 P25 Waveform - Required API Use Case Waveform Operations

Based on the security service requirements outlined in Section 3.4.1.2, the API use case waveform operations indicated as being applicable to this waveform are identified in Table 9. Details of these operations are described in Section 4.2

**Table 9: P25 Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | P25 Waveform Applicability |
|---|---|---|
| WF 01 | Setup (configure)/teardown waveform Control Channels | Yes |
| WF 02 | Update Waveform Policy | No |
| WF 03 | OTAR/OTAT (Waveform specific) | Yes |
| WF 04 | OTAZ (Channel specific keys/Certs) | Yes |
| WF 05 | Extract/Forward Audit Log | No |
| WF 06 | Setup (configure)/teardown Waveform Encryption/ Decryption Channels | Yes |
| WF 07 | Algorithm Selection | Yes |
| WF 08 | Key Selection | Yes |

Table 9: P25 Waveform - Applicable API Use Case Operations

| ID | API Use Case Waveform Operation | P25 Waveform Applicability |
|---|---|---|
| WF 09 | Reserved | - |
| WF 10 | Key Negotiation / Session Establishment | No |
| WF 11 | Encrypt / Decrypt User Traffic | Yes |
| WF 12 | Setup(configure)/teardown Waveform TRANSEC Channels | No |
| WF 13 | Perform TRANSEC Operations | No |
| WF 14 | Provide TRANSEC Keystream | No |
| WF 15 | Provide/Generate Random Number | Yes |
| WF 16 | Provide TRANSEC Key | No |
| WF 17 | Setup(configure)/teardown Waveform Bypass Channels | Yes |
| WF 18 | Plain Audio Text Bypass | Yes |
| WF 19 | Control Bypass | Yes |
| WF 20 | Header/In channel Bypass | Yes |
| WF 21 | Setup (configure)/teardown Waveform Authentication/ Integrity Channels | Yes |
| WF 22 | Authenticate Remote Device / Application | Yes |
| WF 23 | Authenticate Remote User (with/without physical token) | No |
| WF 24 | Authenticate Local Device/ Application | No |
| WF 25 | Authenticate file/token/data/certificate | Yes |
| WF 26 | Integrity Check file/token/data/certificate | No |
| WF 27 | Provide Digital Signature for file/token/data | No |
| WF 28 | Provide Hash for file/token/data | Yes |
| WF 29 | Verify Hash for file/token/data | Yes |
| WF 30 | Retrieve Certificate (s) | No |

**Table 9: P25 Waveform - Applicable API Use Case Operations**

| ID | API Use Case Waveform Operation | P25 Waveform Applicability |
|---|---|---|
| WF 31 | Accept/pass in Certificate | No |
| WF 32 | WF 32 Encrypt/Decrypt File/Token/Data | No |

### *3.4.2 TETRA (Future Work Group Objective)*

Any organization desiring to contribute information concerning security service needs of the Tetra System may submit information to the Wireless Innovation Forum International Security Services API Work Group. Until such time as a contribution is made, no specific requirements will be considered for inclusion in future editions of this document or those documents addressing the IRSS API.

## 3.5 Commercial SATCOM Waveforms (Future Work Group Objective)

Any organization desiring to contribute information concerning security service needs of commercial satellite services such as INMARSAT, Iridium etc., may submit information to the Wireless Innovation Forum International Security Services API Work Group. Until such time as a contribution is made, no specific requirements will be considered for inclusion in future editions of this document or those documents addressing the IRSS API.

## 3.6 Commercial Terrestrial Waveforms (Future Work Group Objective)

Any organization desiring to contribute information concerning security service needs of commercial Terrestrial communications services such as GSM, CDMA, WCDMA, and other 2G, 2.5G, 3G and 4G services etc., may submit information to the Wireless Innovation Forum International Security Services API Work Group. Until such time as a contribution is made no specific requirements will be considered for inclusion in future editions of this document or those documents addressing the IRSS API.

# 4 API Use Case Operations Usage Overview

The following lists comprise an overview of API operations for the Use Cases to be drafted in the future. Use Cases shall consider the impact of different Security Architecture and platform Channel configuration needs. For example, a platform may consist of a single radio channel or multiple radio channels. In either case the radio platform may possess one or more user/operator interfaces, each operating at different security levels. Thus a single user interface may need to support different waveform applications if there are waveform specific software components that must operate on the plain text side of Cryptographic operations and the user side of the Crypto interface must support traffic for multiple radio channels. The user interfaces may also be operating at different security levels ranging from a single level of security, to multiple single levels of security, to Multiple Independent Levels of Security or to Multi-Level Security. This requires the platform as well as the Radio Security Service API's to be able to associate specific encrypted data streams with specific user channels as well as the different security levels that may exist within a user channel.

The operations listed in the next two sections are low level operations which when strung together in a specific sequence with the appropriate data parameters will provide the means to provide a specific Waveform or platform security service function as called out in Section 3. The Security service API must provide the capability to support equivalent operations.

This section thus documents examples of how an API set could be constructed to meet the Waveform needs identified and defined in Section 3. However, the API need not provide a 1:1 correspondence for the listed operations so long as the API meets the security service needs of the Waveform and/or platform and is capable of providing the functionality required by the waveforms and platform. As will be seen there is substantially more detail in Section 4.2 than in 4.1 as the waveform API was the focus of our analysis and the analysis contributed substantially to the development of the waveform/application IRSS API requirements contained in Section 5.

## 4.1 Platform Use Case API Operations

Identified sets of Platform API Operations for application to use case examples are listed below and are described in the sections following the table. It is understood that, at this time, the IRSS API will defer any work on defining a standard set of platform API's.

These sets of Platform API Operations shall not be construed to define a specific set of API operations for implementation by the International Tactical Radio Security Services API (IRSS API), nor is this listing claimed to be a complete listing of the service classes that may be required by a radio platform. They are instead defined simply for the convenience of identifying the general nature of the operations needed by the platform. The IRSS API may define any combination or set of API operations, which may contain either fewer or a greater number of API sets which provide the equivalent functional capabilities associated with the total set of functional operations defined here-in.

The listed set of Radio Platform API Operations do not include the capability to create any ”channels” such as those defined by the waveform API operations in WF 01, WF 06, etc. This is because such channels are presumed to be created and in existence as part of the Radio Platform Operating Environment instantiation/boot process. Security design requirements will typically dictate that these interfaces will not be available to any waveform or other application that is not a part of the RPOE in support of Least Privilege Principle (LPP) and process separation security requirements.

Many of the API operation sets listed below involve human-machine interfaces and the resultant effects of some operations could render the radio platform inoperable. While this might not be true for all operations listed, there is the potential that a subset of these where the CSF must be directly involved with ascertaining and validating the identity of the user/operator as defined by the platform security policy and related design requirements. This may include verifying that such operations fall within those to which the user/operator is authorized to perform these set of API operations and are addressed by the PF-23 operations set.

It is presumed that all of these operations are carried out via a system interface between the radio's HMI of the radio control subsystem to the CSF. Any usage of PINs, passwords, biometric data and other forms of electronic credentials shall be strictly relegated to platform functionality and to platform API's.

**Table 10: Platform Use Case API Operations Summary**

| ID | Platform Use Case API Operation |
|---|---|
| PF 01 | Install/Uninstall/Manage cryptographic algorithms |
| PF-02 | Update/Load/Fill/Manage Keys |
| PF 03 | Zeroize Key (s) (Includes Zeroize All) |
| PF 04 | Install/Manage/Replace Trust Anchors |
| PF 05 | Zeroize Trust Anchor(s) |
| PF 06 | Load/Fill/Manage Certificate(s) |
| PF 07 | Zeroize Certificate(s) |
| PF 08 | Load/Fill/Manage User/Device/Entity Credentials |
| PF 09 | Zeroize Credentials |
| PF 10 | Install/Uninstall Manage waveform/application/platform resident software |
| PF 11 | Install/Uninstall/Manage waveform/application/platform resident software Update |
| PF 12 | Install /Update/ Uninstall/Manage waveform/application/platform Security Policy/Policies |
| PF 13 | Platform Operating Environment boot (Includes all Radio Security Services) |

**Table 10: Platform Use Case API Operations Summary**

| ID | Platform Use Case API Operation |
|---|---|
| PF 14 | Instantiate/De-instantiate Waveform/Application Software |
| PF 15 | Start /Stop Waveform |
| PF 16 | OTAZ Platform |
| PF 17 | OTAR Platform |
| PF 18 | Install, Retrieve and Update Compromised Key Lists (CKLs) and Certificate Revocation Lists (CRLs) |
| PF 19 | Install/Update Platform Operating Parameters |
| PF 20 | Install/Update Channel Operating Parameters |
| PF 21 | Setup/teardown Platform Encryption/Decryption Channels |
| PF 22 | Encrypt/Decrypt User Data/Platform Data/Files/applications |
| PF 23 | Request CSF Authenticate User/Device/Entity and Authorize Operations |
| PF 24 | User Authentication (with/without physical token) |
| PF 25 | Local or Remote Device/ Entity Authentication |
| PF 26 | Manage Security Faults/Alarms |
| PF 27 | Report/Manage Auditable event/alarm condition |
| PF 28 | Manage/Review/Extract Audit Log(s) |
| PF 29 | Platform Memory Resource Management enforcement/enablement |

### *4.1.1 PF 01 - Install/Uninstall/Manage cryptographic algorithms*

This platform set of API operations provide the ability of the platform users or operators to install , uninstall and otherwise manage cryptographic algorithms used by the platform in support of waveform or other platform cryptographic operations such as local file encryption as an example. Management operations might include updating algorithms to the latest software version or regressing to a prior version of the algorithm and defining which versions are stored on the platform in an archive should one exist.

### *4.1.2 PF 02 - Update/Load/Fill/Manage Keys*

This platform set of API operations allow responsible individuals to load, fill or update cryptographic keys used by the Waveforms and other platforms.

The keys may be loaded by a designated fill port in which case this API would define the set of API operations that would allow the responsible individual to successfully load keys either individually or in bulk. When such keys do not have standardized tags this or another designated platform API operation would support the passing of relevant parameters between the “fill” operator and the CSF that will allow a suitable key tag to be created and bound to the key. This subset of API Operation should also allow any key tag field containing incomplete or erroneous data to be edited and corrected by authorized individuals.

This set of API operations shall also support the ability to load one or more keys via other designated platform interfaces. In such instances the platform will have one or more defined methods and interfaces by which keys may be loaded. For example it may be possible to transfer an encrypted set of keys to a specified IP address which is associated with a designated platform port or function. This subset of API Operations would thus allow these keys to be loaded into the CSF and placed under local key management. In such instances it can be assumed that all such keys have associated key tags which can be used to identify the key and its usage and includes any operations necessary for the users to manage these keys other than for local key Zeroize operations. This includes initiating defined cryptographic key updates, key transfers, Over the air Rekey operations or over the air transfer operations as they fall within the operational capabilities of the radio platform.

### *4.1.3 PF 03 - Zeroize Key(s)*

This subset of platform API operations are those which define the means by which an authorized individual can cause one or more cryptographic keys stored and used by the platform for waveform or platform cryptographic operations to be Zeroized. This does not include any physical means employed (e.g. Zeroize controls) by the platform to Zeroize keys, but rather only those operations which are initiated by an operator or user via the API. Such Zeroize operations might involve one or more keys, including all of a type for 1) a designated waveform type, 2) all keys (& related parameters) on the platform (Zeroize all), and 3) all keys whose expiration date has been passed and have been preserved in an archive or other designated groups of keys as defined by the platform requirements.

### *4.1.4 PF 04 - Install/Manage/Replace Trust Anchor(s)*

This subset of API operations provides the means to install, manage and/or replace the initial trust anchor (e.g. root certificates and associate private keys) and any associated trust anchors (e.g coalition root certificates) used by the platform. The initial installation may occur in a manufacturing environment or in a designated depot repair facility. Replacements are needed when certificates expire. Management of these might involve identifying or tagging a certificate with a flag that denotes the private key may be compromised or that a certificate has been revoked.

### *4.1.5 PF 05 - Zeroize Trust Anchor*

This subset of API operations provides the means to Zeroize one or more designated Trust Anchors. Generally a Zeroize All as in 4.1.3 above would eradicate all sensitive material including the Trust Anchors so a separate Zeroize all trust anchors may not be needed but the API could support such in any event.

### *4.1.6 PF 06 - Load/Fill/Manage Certificate(s)*

Certificates and other forms of digital credentials are generally associated with local users, and devices. Devices may be both within (e.g., internal router function) or external to the platform. Each such certificate/credential loaded into the platform typically requires a designated use, and a user or device identifier association. These designations may go beyond the designated name in the certificate since the name does not necessarily define a specific platform or network use/role (but could). This kind of association is needed when role based access control mechanisms are employed to authorize operations done either locally or remotely on the radio platform. This API subset therefore shall support the identification of the roles and associations necessary to perform such security functions when required by the radio platform specification.

### *4.1.7 PF 07 - Zeroize Certificate(s)*

This subset of API operations provides the means to Zeroize either an individual or a subset of certificates and credentials held by the platform. For those certificates which the CSF also maintains the private key, the associated Private key shall also be Zeroized concurrently with the certificate to which it applies.

Generally a “Zeroize all” as provided in 4.1.3 above or a hardware initiated control would eradicate all sensitive material including the certificates and other forms of digital credentials so a separate Zeroize all certificates/credentials may not be needed but the API could support a Zeroize all certificates in any event.

### *4.1.8 PF-08 Load/Fill/Manage User/Device/Entity Credentials*

This subset of API operations is the equivalent of the operations defined above in section 4.1.2 except that they apply to certificates and other forms of digital credentials such as ergonometric data (finger prints, retinal images) or other information relating to user or device identification.
Certificates and other forms of digital credentials are generally associated with local users, and devices. Devices may be both within (e.g., internal router function) or external to the platform. Each such certificate/credential loaded into the platform typically requires a designated use, and a user or device identifier association. These designations may go beyond the designated name in the certificate since the name does not necessarily define a specific platform or network use/role (but could). This kind of role/function association is needed when role based access control mechanisms are employed to authorize operations done either locally or remotely on the Radio Platform. This API subset therefore shall support the identification of the roles and associations necessary to perform such security functions when required by the Radio Platform specification.

### *4.1.9 PF 09 - Zeroize Credentials*

This subset of API operations provides the means to Zeroize either an individual entity's credential set or a designated subset of credentials held by the platform.

As noted previously a "Zeroize all" as in 4.1.3 above would eradicate all sensitive material including the certificates and other forms of digital credentials so a separate Zeroize certificates/credentials may not be needed but the API could support a Zeroize all certificates in any event if deemed useful.

### *4.1.10 PF 10 - Install/Uninstall/Manage waveform/application/platform resident software*

Platform operations involving installing, uninstalling and managing software of any form are not specifically security services. However, the processes involved generally do include the application of security services. Any given software package may have to be totally or partially decrypted before it can be installed and it may be necessary to store the software or portions thereof in encrypted form while it is retained inactive in platform memory. Other likely operations on installing software are likely to include integrity checks as well as authentication of the source of the software code and potentially authentication and authorization of the software distributing agent in that role.

While conceivably the platform could use the same API as the Waveform used for similar operations, the application of LPP and process separation security design principles would generally necessitate separate and distinct platform interfaces (CORBA ports) for these platform operations.

The manner in which the software is delivered to the platform may also affect the way the security services are applied and whether additional verifications are needed. For example, a platform may have a security policy design requirement that software can only be installed from a specific physical port on the platform. Thus the platform would need a security service function that would enforce or otherwise ensure that the specific requirement is met.

### *4.1.11 PF 11 - Install/Uninstall/Manage waveform/application/platform resident software Update*

This group of platform operations is essentially identical to those in 4.1.10, with the possible exception that version configuration management control rules could be enforced by the CSF rather than some other functions on the radio platform. To allow such a possibility a platform API should support the requisite functionality. This should also include any operations which involved rollback to a prior version.

### *4.1.12 PF 12 - Install /Update/ Uninstall/Manage waveform/application/platform Policy/Policies*

This set of API operations assumes that there are separate, downloadable security, regulatory, cognitive/behavioral, or other policy types that apply to waveforms, specific applications (e.g. IP routers or firewalls) or other platform based security functions. These policies may be enforced by the CSF or other suitably protected/safeguarded function, and similar to the software installation discussed in 4.1.10 above regarding the interfaces over which the policy is received and loaded may be subject to specific security policy requirements in addition to other services such as decryption, integrity checking and authentication of the policy and it source and delivery/distribution agent.

### *4.1.13 PF 13 - Platform Operating Environment boot (Includes all Radio Security Services)*

This set of API operations could involve numerous interactions with the CSF depending upon platform design and platform security policy specific requirements. For example, this might involve file/software decryption, authentication and integrity verification services or even secure file management services for the Radio Platform operating environment software as well as for the CSF software itself.

Because of the nature of the boot operation, the use of APIs such as those used by waveforms are not yet in place until the boot process is substantially complete. Thus the APIs for the boot operations are of necessity different and as such may not be able to be standardized as they will likely be platform hardware and software design dependent and subject to specific platform security policy design requirements.

### *4.1.14 PF 14 - Instantiate/De-instantiate Waveform/Application Software*

The Waveform operations sets defined in 4.2 include those necessary for the waveform/application to assemble and activate all security related services and mechanisms needed by the waveform/application as well as to perform an orderly shutdown of the waveform operations. However, a similar set of API operations might be necessary for the operating environment software to employ when instantiating other applications which may not have the ability to create their own ports for the security services that they may require.

This need may be met with a duplicate set of API operations such as those used by the waveforms however, the process separation security principle would require that a designated port be used for these operations that is only available to the software responsible for launching/tearing down designated waveforms/applications.

### *4.1.15 PF 15 - Start/Stop Waveform*

This operation set supports the human-machine interface whereby authorized individuals can cause a Waveform to initiate, cease or resume normal waveform operations. This may be the result of the need to alter operating parameters, initiate radio silence or by some other operational need. Since the CSF is a separate component of the platform, independent of the Waveform, it should also be informed of the change in status and security specific requirements could necessitate CSF enforcement of the operation.

Some Waveforms (e.g. 2G/3G HF ALE) may need to have a similar capability as a part of normal waveform operations, but notwithstanding such a need it is recommended that separate API’s be used to permit LPP enforcement.

### *4.1.16 PF 16 – OTAZ Platform*

The manner and methods by which an Over-The-Air-Zeroization of all platform security sensitive data (keys, certificates, credentials, and perhaps waveform configuration data, platform operating data, etc.) will be determined by platform specific security policy and other operational requirements. As such it is believe that this cannot be subject to a standardized API. Furthermore, a local Zeroize All function is often hardware activated and is implemented such that it does not involve any operational software or APIs.

### *4.1.17 PF 17 - OTAR Platform*

Platform specific security and operational requirements will ultimately determine the manner and methods by which an Over-The-Air-Rekey of platform security data (keys, certificates, credentials, and security specific operating data) will be accomplished. As such it is believed that these operations cannot be subject to a full set of standardized APIs. There may be a significant portion of these operations or of parameter related there-to which can be standardized.

### *4.1.18 PF 18– Install, Retrieve and Update Compromised Key Lists (CKLs) and Certificate Revocation Lists (CRLs)*

While the manner of requesting and distributing these lists may not be standardized, a set of platform API operations will be necessary to pass these lists into the CSF so that they can be integrity checked, authenticated and then stored within the CSF for use during other authentication operations to the extent that such lists are required to be supported by a platform security policy.

These operations are being designated as a platform API since 1) the network overhead associated with requesting and retrieving these lists during IP based radio network operations may be too high to support in tactical radio networks, 2) the radio platform does not yet have the IP based radio network in an operational state and these lists are being distributed prior to operations, or 3) the IP protocols used do not support distribution of these lists via the network but might allow updates.

If a Radio Platform does include CKLs and CRLs, then these lists should be automatically used to validate any certificate being used for authentication purposes. Should the certificate or its private key be included in the listing then the authentication operation should be reported as a failure.

### *4.1.19 PF 19 - Install/Update Platform Operating Parameters*

This set of API operations involves those needed for CSF support of either individual or bulk data installation/updates of radio platform operating parameters/configuration data.

For individual data entries via the human-machine interface this may be totally accommodated by those defined in section 4.1.24 except when such parameters are maintained by and stored within the CSF, in which case these would be covered by this set of API operations.

Another set of API operations relating to this are the bulk installation or update of a portion or all of the platform configuration data, including those included in section 4.1.20 which follows. These data are likely to be passed as bulk files and the files will typically have to be decrypted, integrity checked, authenticated as to the originator and possibly to the distributor being authorized to create/distribute these data. Other forms of security related checks, such as time stamps or other forms of version control can be applied to ensure that invalid or obsolete data is not accepted by the radio platform.

### *4.1.20 PF 20 - Install/Update Channel Operating Parameters*

These types of radio operating parameters are a subset of those defined in the preceding section. They are identified separately since a radio platform may, while on a deployed mission, be required to instantiate a different Waveform than originally planned as part of the mission. These data may be distributed as bulk data files or manually entered via the HMI and may be accompanied by the need to install a new Waveform and fill associated key materials as defined in the preceding sections dealing with those operations.

This set of API operations may fall entirely within the set of platform operations defined in the preceding section but are separately identified to ensure that a critical aspect of these operations is not overlooked and inadvertently not considered.

### *4.1.21 PF 21 - Setup/teardown Platform Encryption/Decryption Channels*

This set of API operations deals with those necessary to support the Radio Platform establishing those cryptographic channels necessary to support platform related encryption and decryption operations. It is recognized that these channels could be established by default during start-up/boot operations or separately established in a manner similar to waveform encryption/decryption and only for the time frame that the channels are needed.

While the set of API operations may be similar or identical to that used by waveforms, LPP and the process separation security principals dictate that these APIs be distinct and separate from those used by the waveforms.

### *4.1.22 PF 22 - Encrypt/Decrypt User Data/Platform Data/Files/applications*

This set of API operations relates to the Radio Platform use of the cryptographic channels established by the preceding set of platform operations.

While the set of API operations may be similar or identical to that used by waveforms, LPP and the process separation security principals dictate that these APIs be distinct and separate from those used by the waveforms.

### *4.1.23 PF-23 Request CSF Authenticate User/Device/Entity and Authorize Operations*

This set of API operations provides the platform with an API that supports the ability of the CSF to directly interact with the users, operators, devices, both internal and external, as well as any entity that interacts with the platform via interfaces which do not support user and/or networked traffic. This may include the platform HMI or external computer terminals providing radio control or management services, fill devices etc., in order for the CSF to verify the individuals/entities identity and to allow the platform to ascertain and verify that the operation being requested by that entity falls within those permitted by the entity via techniques such as role based access control, authorizations lists or other techniques consistent with the platform security policy.

The identification process might involve direct communication and interaction between the CSF and the entity via a trusted or encrypted path, including interaction with credential forms such as user identifier tokens, smart cards, and biometric devices such as fingerprint scanners or retinal scanners to ensure that the data hasn't been altered during the input/retrieval process.

The need for any of the above will be a result of platform specific requirements consistent with the platform security policy. LPP and process separation security principles dictate that this API be distinct and separate from those used by the Waveforms or other applications, especially since trusted paths may be involved.

### *4.1.24 PF 24 - User Authentication (with/without physical token)*

This set of API operations includes those needed to perform general user authentication where the CSF may not actually be directly involved in the authentication process as described in the preceding section. In this instance some other platform function is responsible for performing the authentication. In such an instance, for example, the process may request random data from the CSF for use as a "token" to be signed by a user security process and returned for authentication. The actual authentication may be performed by that process or by design might rely on the CSF to simply authenticate the signature applied to the token. Regardless which process actually authenticates the signature, the overall control of the authentication operations is the external process.

While the set of API operations may be similar or identical to that used by Waveforms, LPP and the process separation security principals dictate that these APIs be distinct and separate from those used by the Waveforms

### *4.1.25 PF 25 - Local or Remote Device/ Entity Authentication*

This set of API operations includes those needed to perform general authentication of a local or remote "device" or other entity where the CSF is not actually directly involved in the authentication process as described earlier in 4.1.23.

In this instance the actual authentication may be performed by another platform process. In such an instance, for example, the process may request random data from the CSF for use as a "token" to be signed by a user security process and returned for authentication. The actual authentication may be performed by that process, or by design might rely on the CSF to simply authenticate the signature applied to the token. Regardless of which process actually authenticates the signature, the overall control of the authentication operations is the external process.

Each of these choices requires a different set of API operations to be supported by the API. The set of API operations for these functions should permit the combination or choice of either option (external process and/or CSF) to be supported.

While the set of API operations may be similar or identical to that used by Waveforms, LPP and the process separation security principals dictate that these APIs be distinct and separate from those used by the Waveforms.

### *4.1.26 PF 26 - Manage Security Faults/Alarms*

The design and implementation of specific security related faults and alarm conditions will likely very specific to a given Radio Platform design. In many instances these alarm conditions are detected and reported by dedicated hardware. Notwithstanding the unique platform aspects of these functions, the CSF is typically required to be notified of all such security faults so that the Radio

Platform Security Policy governing radio operations under security fault conditions can be enforced by the CSF. Since external processes may not have any knowledge of the specifics of the security alarm policy, this set of API operations must provide the means for processes external to the CSF to report relevant faults. Depending upon platform security requirements this may necessitate either a separate API set for security alarms or it may allow the use of the auditable event API operations set as defined in the next section, or some combination of the two.

### *4.1.27 PF-27 Report/Manage Auditable event/alarm condition*

This set of API operations must provide the capability for any process responsible for monitoring events which may be auditable, to report the occurrence of an event and any relevant associated data. This relevant data may differ from one type of event to another. For a process event condition (e.g., a timeout) it might include a reference to the event and identification of the reporting process, while for an HMI related event, it would include identification of the user, the users role, the specific operation and details of that operation. Depending upon whether or not the CSF has independent access to a time-of-day etc., then the data might include time and date information.

In some systems, there may be a need to manage the auditable event list. This might involve a class of event which can be enabled or disabled based on some policy statement or by human entry via the HMI.

Enforcement of this latter aspect for security reasons could be allocated to the CSF, thus the Radio Platform API set should support managing such events.

### *4.1.28 PF 28 - Manage/Review/Extract Audit Log(s)*

This set of Security related platform API operations involve those needed to support the management, review and extraction of the contents or portion thereof related to the audit log.

### *4.1.29 PF-29 - Platform Memory Resource Management enforcement/enablement*

The set of platform API operations provide the capability for the RPOE components and other applications to utilize the Radio Platform’s Memory Resource Management facilities to the extent that such facilities exist and are accessible to these software components.

### *4.1.30 PF-30 Software/Firmware Management*

Platform management of software and firmware resources are typically an HMI initiated activity related to installation and updating, including version control and removal of waveform and platform software and firmware to include Radio Platform Operating Environment components, waveforms and other installed applications as well as Cryptographic subsystem software/firmware components. Version control may include rollback or version skipping restrictions or controls.

### *4.1.31 PF-31 Logging, Auditing and Security Alarm Services*

Processes related to logging , auditing and alarm services other than the actual logging activities and the alarm monitoring services are generally focused on the Radio Platform’s HMI since it is through the HMI that users can obtain information about the contents of the audit logs and alarm conditions that have been detected. These HMI based operations allow authorized individuals to access details of the alarms and logs to include specialized searches using date and time ranges along with filter parameters so the search can focus on entries of specific types or those related to a specific individuals or some combination there-of. Other HMI activities would provide the capability to off load the logs or portions thereof either to an external device or to send the information as an encrypted file to a specified destination/addressee through one of the radio networks. These latter operations could also possibly be configured so that the log was transmitted when specified conditions exists. The specifics for any given radio platform will be determined by the Radio Platform's functional requirements and the RPSP.

## 4.2 Waveform Operations

The following sections provide a list of identified waveform API use case operations for application to the API use case analysis along with a complete summary of the application to each waveform based on the information presented in Section 3 of this document. Their listing as a waveform API operation does not necessarily preclude any of these from also being a platform operation. However, because of LPP and process separation security requirements, the middleware (e.g. CORBA) ports used for waveform operations shall be separate and distinct from those used for Platform operations. Furthermore the use of any specific operation by any given Waveform shall be subject to the Waveform's security policy.

Each of these operations is further defined following the table.

**Table 11 Waveform Applicable API Use Case Operations Summary**

| ID | API Use Case Waveform Operation | Waveform Applicability | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPBAHN | TDMA SATCOM | | UHF TACSAT | HF 2G/3G ALE | VHF/UHF | | P25 |
| | | | Legacy | Future | | | Legacy | Coalition | |
| WF 01 | Setup (configure)/teardown waveform Control Channels | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| WF 02 | Update Waveform Policy | Yes | No | Yes | No | No | No | No | No |
| WF 03 | OTAR/OTAT (Waveform specific) | Yes | No | Yes | No | Yes | Yes | Yes | Yes |
| WF 04 | OTAZ (Channel specific keys/Certs) | Yes | No | Yes | No | No | No | Yes | Yes |
| WF 05 | Extract/Forward Audit Log | Yes | No | No | No | No | No | No | No |
| WF 06 | Setup (configure)/teardown Waveform Encryption/ Decryption Channels | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| WF 07 | Change Algorithm Selection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| WF 08 | Change Key Selection | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| WF 09 | Reserved for Future Use | - | - | - | - | - | - | - | - |
| WF 10 | Key Negotiation / Session Establishment | Yes | No | Yes | No | No | No | Yes | No |
| WF 11 | Encrypt / Decrypt User Traffic | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| WF 12 | Setup (configure)/teardown Waveform TRANSEC Channels | Yes | Yes | Yes | No | Yes | Yes | Yes | No |
| WF 13 | Perform TRANSEC Operations | Yes | Yes | Yes | No | Yes | Yes | Yes | No |
| WF 14 | Provide TRANSEC Keystream | Yes | No | Yes | No | Yes | Yes | Yes | No |
| WF 15 | Provide/Generate Random/PN Number | Yes | No | Yes | No | Yes | Yes | Yes | Yes |
| WF 16 | Provide TRANSEC Key | No | No | No | No | No | Yes | Yes | No |
| WF 17 | Setup (configure)/teardown Waveform Bypass Channels | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| WF 18 | Plain Audio Text Bypass | No | No | No | Yes | Yes | Yes | Yes | Yes |

**Table 11 Waveform Applicable API Use Case Operations Summary**

| ID | API Use Case Waveform Operation | Waveform Applicability | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPBAHN | TDMA SATCOM | | UHF TACSAT | HF 2G/3G ALE | VHF/UHF | | P25 |
| | | | Legacy | Future | | | Legacy | Coalition | |
| WF 19 | Control Bypass | Yes | Yes | Yes | No | Yes | Yes | Yes | Yes |
| WF 20 | Header/In channel Bypass | Yes | No | Yes | No | No | No | Yes | Yes |
| WF 21 | Setup (configure)/teardown Waveform Authentication/ Integrity Channels | Yes | No | Yes | No | No | No | Yes | Yes |
| WF 22 | Authenticate Remote Device / Application | Yes | No | Yes | No | No | No | Yes | Yes |
| WF 23 | Authenticate Local/ Remote User (with/without physical token) | No | No | No | No | No | No | Yes | No |
| WF 24 | Authenticate Local Device/ Application | Yes | No | Yes | No | No | No | No | No |
| WF 25 | Authenticate file/token/data/certificate | Yes | No | Yes | No | No | No | No | Yes |
| WF 26 | Integrity Check file/token/data/certificate | Yes | No | Yes | No | No | No | No | No |
| WF 27 | Provide Digital Signature for file/token/data | Yes | No | Yes | No | No | No | Yes | No |
| WF 28 | Provide Hash for file/token/data | Yes | No | Yes | No | No | No | Yes | Yes |
| WF 29 | Verify Hash for file/token/data | Yes | No | Yes | No | No | No | Yes | Yes |
| WF 30 | Retrieve Certificate(s) | Yes | No | Yes | No | No | No | Yes | No |
| WF 31 | Accept/pass in Certificate(s) | Yes | No | Yes | No | No | No | Yes | No |
| WF 32 | Encrypt/Decrypt File/Token/Data | Yes | No | Yes | No | No | No | Yes | No |

### *4.2.1 WF 01 - Setup (configure)/teardown waveform Control Channels*

This set of API operations provides the Waveform a capability to establish and configure a Control Channel which the Waveform can then use to communicate specifics regarding other waveform API operations to the CSF.

It is permitted for this operation to be able to support the establishment of both RED & BLACK side Control Channels, either as separate operations, one from each side, or with a composite request from either side.

The channels thus established would be used to pass selected API operations requests to the CSF. This Control Channel could be used to support the Waveform reporting waveform specific auditable events for the radio platform’s audit log unless the Waveform reports these events to another radio service (e.g. Core Framework logging service) which then passes the auditable events as in PF-25. All such waveform reporting should be in accordance with the Waveform and/or Radio Platform Security Policy.

Under no circumstances shall this channel ever be used to pass sensitive/classified data either to or from the CSF, nor would it be used to support any type of bypass operation.

This set of API operations also includes those necessary to tear down the Control Channels when the Waveform is de-instantiated or otherwise terminated.

It is assumed that this API operations set would only be used during waveform instantiation and de-instantiation.

### *4.2.2 WF 02 - Update Waveform Policy*

This set of API operations will support a Waveform’s need to update one or more policies relevant to that Waveform’s operation.

The operations assume that any new policy received by the Waveform will be passed into the CSF where it will be subjected to a series of waveform specific verifications using other operations defined in this set such as WF-25 (authenticate/integrity check file).

Where and how the policies are stored and enforced is a matter of platform and waveform specific requirements but it is anticipated that the CSF will play a significant role.

The API set should support the ability of the Waveform to identify the policy as to the type (e.g. security, regulatory, cognitive behavior, network, etc.) and a reference to the identity/reference number of the policy which is being updated, superseded or modified.

This set of API operations should use the logical Control Channel configured by WF-01.

### *4.2.3 WF 03 – OTAR/OTAT (Waveform specific)*

For waveforms that support OTAR and/or OTAT, this set of API operations presumes that a Waveform will have awareness that an over-the-air rekey or transfer operation is about to commence. This knowledge may be obtained by the Waveform from an associated waveform protocol, or the operation could be sensed by the CSF as a result of a cryptographic protocol operation or change in cryptographic mode. Alternatively, the process could have been initiated at the local man-machine interface by interactions between the HMI and the CSF as well as the Radio Platform fill port.

There are no known standardized methods regarding how an OTAZ or OTAT is performed. Legacy operations involved the use of fill devices working directly with the Cryptographic equipment.

As noted earlier, it should be assumed for emerging and future Waveforms that the keys may include appropriate and standardized key tags for each key which will be a part of the key material exchanged.

Included in these operations might be a forced, but temporary cessation of user traffic processing and perhaps changes in waveform processing of the received/transmitted key material user traffic.

The process might require the CSF to directly authenticate the source of the key material or alternatively the key material file(s) might be separately and individually authenticated after they have been transferred. There are also many possibilities for how the files would be transferred. It could be initiated by a download by an authenticated and authorized user to a radio platform as a file transfer. Subsequent distribution could be via over the air exchanges between the CSF in each of two radios, or simply sent as a file transfer to a designated and addressable function in a radio’s waveform. These are just some of the possibilities.

The use case analysis should consider the type of operations that will be needed for each of these or other likely scenarios. The operations should be able supporting rekeying a single key or an entire set of keys.

API operations sets supporting these operations when there is waveform cognizance include WF 22 or WF 23 to authenticate and validate access privileges when the Waveform or platform security required direct authentication of the source, while individual key data sets received via the Waveform could be authenticated using WF 25.

Another type of operation that could fall within this set of API operations is initiation of a process involving the negotiation of session keys used to support user traffic or other operations such as key transfer operations. However, when this is the case, then the LPP and process separation principles would require that the protocol for the process should use a designated cryptographic channel configured by the Waveform per WF 06 for that purpose.

The operations for this API set, except as noted above should use the Control Channel configured by WF-01.

### *4.2.4 WF 04 - OTAZ (Channel specific keys/Certs)*

This set of API operations is relevant only to the extent that the Waveform needs to be cognizant that an OTAZ operation is about to occur and is informed of this by a waveform control protocol or message. This may be needed if confirmation of the Zeroization must be provided back to the originator of the command. In this case the command would likely have to be fully authenticated and verified for authenticity and the originator of the command identified and verified regarding authorization to initiate such an operation. Such authentication and authorization may employ processes such as WF 22 or WF 23. If the OTAZ operation is inherent to the cryptographic protocols then it is assumed that the OTAZ operation is relegated to a platform operation since the waveform need not be aware.

All interactions between the waveform and the CSF regarding these operations should utilize the Control Channel configured by WF-01.

### *4.2.5 WF 05 - Extract/Forward Audit Log*

This set of API operations are those that would allow an waveform to receive a command addressed to the specific radio platform that requests that all or some portion of the radio platform audit log be extracted, offline encrypted, digitally signed using the requesting entities device certificates public key, and returned via the waveform to the requesting source.

The Waveform’s extraction request for the log should permit the identification of a date ranges, either specific (from this date to another date) or more general (the last day, week, month), and whether or not that portion of the log may be deleted/overwritten.

The Waveform’s extraction request may optionally permit identification of specific types of events or designated event subsets (e.g. alarms).

The API set shall also permit the Waveform to specify a key and/or a digital certificate and its associated private key to be used for securing the content of the log and for creating a digital signature for the result log file.

The API set shall optionally allow the Waveform to specify the hash and/or signature algorithms in the event that more than one must be supported in accordance with the waveform’s or the radio platform’s security policy.

All such requests shall be in accordance with the Waveform and/or platform security policies.
When the request has been received and authorization verified, the responsible process shall prepare the log which will then be forwarded by the CSF using this API set of operations.

The Forward of an audit log to a Waveform could also optionally be initiated using the radio platform HMI and the CSF would then forward the log to the waveform after it has been prepared. Any such interactions between the Radio Platform HMI and the CSF fall within the Radio Platform’s API set.

All interactions between the Waveform and the CSF regarding these operations should utilize the Control Channel configured by WF-01 or alternatively may use another channel configured specifically for an operation such as this.

### *4.2.6 WF 06 - Setup (configure)/teardown Waveform Encryption/ Decryption Channels*

This set of API operations will permit the waveform/application to set-up and configure one or more encryption or decryption channels for the waveforms use.

The API shall support the establishment of channels for traffic encryption and, when permitted by the Waveform Security Policy, an additional but separate channel for file/data/token encryption/decryption.

For any channel established using this set of API operations, the API will provide the Waveform the capability to specify the cryptographic equipment protocol (e.g. KY-57, KG-84) or equivalent, the cryptographic algorithm and mode (when applicable) and the associated keys to be used.

The keys may be pre-placed or negotiated via an IKE or similar process and associated with the waveform channel being set-up and configured.

For file/token/data encryption the API shall support the option to specify the use a private or public key associated with a specified digital certificate for encryption and or decryption and whether the use of the key applies to the encryption process, the decryption process or both.

This API operations set will permit the definition/specification for the direction of the encryption or decryption operation and support RED to BLACK, RED-RED, BLACK-BLACK and BLACK to RED encryption or decryption and be able to pair-wise link encryption and decryption channels for both the cipher text and plain text operations. This is especially important when a CSF channel must support multiple encryption/decryption contexts.

Encryption and decryption channels should never be used for bypass operations, except optionally for packetized data headers who contents must be bypassed.

This set of API operations also includes those actions necessary to tear down the channels when the waveform is de-instantiated or otherwise terminated.

This set of API operations shall occur via the Control Channel created and configured by the waveform API operations defined by WF-01.

### *4.2.7 WF 07 – Change Algorithm Selection*

This API operation will permit a waveform to effect a change in the cryptographic equipment protocol, the cryptographic algorithm and/or mode and the cryptographic key for a previously established encryption/decryption channel.

The API may provide this capability as a separate operation via the Control Channel established WF-01 or it could be a variant of the operations in the INFOSEC channel created byWF-06.

### *4.2.8 WF 08 – Change Key Selection*

This API operation will permit a waveform to change the cryptographic key being used for a previously established encryption/decryption or TRANSEC Channel.

The API may provide this capability as a separate operation using the Control Channel created by WF-01 or it could be a variant of the operations in WF-06 for encryption/decryption channels or for WF-12 regarding TRANSEC channels. If the WF-01 Control Channel is used then the request would have to be able to identify the appropriate channel INFOSEC/TRANSEC to which the request applies.

### *4.2.9 WF 09 – Reserved*

Section reserved for future use.

### *4.2.10 WF 10 - Key Negotiation / Session Establishment*

This API operation set will provide the Waveform the capability to request the CSF to perform a key-negotiation or session key establishment as required by IP based networks. This includes Internet Key Exchange (IKE and IKEv2) and national systems such as the US High Assurance Internet Protocol Encryptor (HAIPE).

The request for this set of API operations should occur via the Control Channel created and configured by the waveform API operations defined by WF-01, while the requested key negotiation/session establishment shall occur via a Cryptographic Channel created and configured by the waveform API operations defined by WF-06.

### *4.2.11 WF 11 - Encrypt / Decrypt User Traffic*

This set of API operations is used by the waveform to pass traffic for decryption or encryption into a previously established channel. Encrypted or decrypted traffic could then be pushed out to the corresponding associated decryption/encryption channel after being transformed by the cryptographic operation.

This set of API operations shall occur via the Encryption/Decryption channel created and configured by the waveform API operations defined by WF-06.

### *4.2.12 WF 12 – Setup (configure)/teardown Waveform TRANSEC Channels*

The set of API operations provides the Waveform the capability to configure a channel that will be used for TRANSEC operations.

For any channel established using this set of API operations, the API shall provide the Waveform the capability to specify the Crypto Equipment Protocol or equivalent, the cryptographic algorithm and mode (when applicable) and the associated keys.

1. These API operations will support establishing TRANSEC channels that support CSF keystream generation for the Waveform’s use and application to the TRANSEC operations required by the waveform.

   a. When configured for this purpose, this set of API operations shall consider supporting the waveform specifying parameters such as the length of each data block of keystream provided, the frequency and/or application bit rate that the CSF should be prepared to support or any other data that may be relevant to the waveform's TRANSEC operations.

2. These API operations will support establishing TRANSEC channels that provide for encryption and decryption of waveform control information.

   a. When configured for this purpose the API set shall permit specifying whether the plain text side of these channels is located on the BLACK or RED side of the CSF unless defined by specific waveform and/or platform security policy requirements. It is assumed that the cipher text side is always on the BLACK side.
   b. Notwithstanding that these may be BLACK to BLACK operations the API should enforce that separate CORBA ports are used by the waveform for the plain text and cipher text interfaces. Thus the Waveform shall also be able to pair-wise link encryption and decryption channels for both the cipher text and plain text operations.

3. These API operations will support establishing TRANSEC channels that support TRANSEC Key extraction for application and use by the waveform. In the instance the waveform is responsible for performing all TRANSEC operations and this channel will be used to extract the key from the CSF as well as for requesting and obtaining random numbers for the Waveform's use.

The creation of any of the above TRANSEC channel types shall be in accordance with the waveform and/or platform security policy.

This set of API operations shall include those necessary to tear down the channels when the waveform is de-instantiated or otherwise terminated.

This set of API operations which establishes these channels shall occur via the Control Channel created and configured by the waveform API operations defined by WF-01.

### *4.2.13 WF 13 - Perform TRANSEC Operations*

The set of API operations correspond to a request from the Waveform for the CSF to encrypt or decrypt waveform control or orderwire information using the a channel created and configured per WF 12-2 and pushing the information to the corresponding cipher text and plain text output ports.

### *4.2.14 WF 14 - Provide TRANSEC Keystream*

This set of API operations is used by the Waveform to request the CSF provide the required and previously defined block of TRANSEC keystream and by the CSF to provide the keystream data to the waveform. These operations occur on the previously configured TRANSEC channel created and configured by WF 12-1.

### *4.2.15 WF 15 - Provide/Generate Random Number*

This set of API operations is used by the Waveform to request the CSF to generate and provide a random number of "n" bits in length for and by the CSF to provide the requested random number data to the Waveform. These operations occur on a TRANSEC channel created and configured by WF 12-3.

### *4.2.16 WF 16 - Provide TRANSEC Key*

This set of API operations is used by the Waveform to request the CSF to provide a specified TRANSEC key for and by the CSF to provide the requested key data to the Waveform. These operations occur on the previously configured TRANSEC channel defined by WF 12-3.

### *4.2.17 WF 17 – Setup (configure)/teardown Waveform Bypass Channels*

The set of waveform API operations provides the capability for the waveform to set-up and configure whatever bypass channels are permitted by the Waveform’s security policy and are required for proper waveform operation. These can be as follows:

1. A plain text audio bypass as required by some legacy tactical waveforms. Even though configured for bypass, the bypass feature is enabled by the CSF only when specific conditions are met. Those conditions, as well as the specific method by which this bypass is accomplished are determined by both waveform and platform specific design and security requirements.
2. A control bypass that allows a waveform specific set of control commands and associated parameters which are permitted to pass between waveform software components located on the respective RED and BLACK sides of the radio channel, subject to CSF scrutiny. This channel is a separate logical channel with its own CORBA port identifier.
3. A logical channel (associated with a specified cryptographic channel) through the CSF which allows specified packet header fields and associated parameters which are to be extracted from the data stream and re-inserted after the cryptographic transformation (i.e. encryption or decryption) has been applied to the data fields, subject to CSF bypass scrutiny. These channels do not share the same CORBA port ids with the cipher text decryption and plain text encryption traffic channels configured by the Waveform, but are specifically associated with them on a 1:1 basis. As a separate operation this API feature can be used to define a specific configuration of this bypass should such be required by a waveform.

NOTE: The WInnForum recommends against a general “plain text “data” bypass” channel as there is significant potential for exploitation. Only waveforms running on platforms with certified MLS channels would even have the capability to ensure that the unclassified data has not been contaminated. Furthermore, passing of plain text data over the air allows hostile intelligence forces the potential ability to conduct traffic flow and other forms of analysis. If plain text data does need to be transmitted then an unclassified traffic channel can be configured on a radio and used for that purpose. However, it is common to encrypt such unclassified data for transmission over radio channels to deny hostile forces any intelligence opportunity.

This set of API operations also includes those necessary to tear down the bypass channels when the waveform is de-instantiated or otherwise terminated.

This set of API operations shall occur via the Control Channel created and configured by the waveform API operations defined by WF-01.

### *4.2.18 WF 18 - Plain Audio Text Bypass*

This set of API operations when configured and enabled may be used to pass:

1. The demodulated plain text audio from the BLACK Side of the radio channel to the RED side of the radio channel, bypassing the decryption cryptographic transform, and delivering the information to the user's audio channel, and
2. Accepting user plain text audio from the RED side of the radio channel to the BLACK side of the radio so that it can be modulated for transmission over the air without encryption or digitization.

As noted in WF-17, the specific means by which such a channel which has been configured for plain text audio bypass can be enabled for operation in either the receive or transmit direction is subject to waveform and platform specific requirements.

### *4.2.19 WF 19 - Control Bypass*

This set of API operations allows a waveform to pass specified control information from the BLACK side of the radio channel to the RED side of the radio channel and vice versa. This set of API operations are confined to a designated and properly configured control bypass channel establish per WF 17 -2 which does not share any CORBA port with any user traffic or other information. The CSF is responsible for ensuring that only specified control information passes through this channel in either direction.

### *4.2.20 WF 20 – Header or In-channel Bypass*

This set of API operations requires a Waveform to deliver the header data which is to be bypassed for any given packet, whether from RED to BLACK or BLACK to RED, to be delivered to a separate bypass port/channel for this purpose which has been established and configured per WF 17-3. Two general methods could be used to accomplish header bypass.

1. When the extraction operation is performed by an RSS component, the header data which is to be bypassed for any given packet, whether from RED to BLACK or BLACK to RED, is passed to a designate interface with the CSF that has been established and configured for this purpose. With this method, it will be a matter left to the platform designers and those responsible for porting the Waveform to the platform to ensure the synchronization is achieved between the data packets passing through the separate encrypt/decrypt channels and their associated header information.
2. A variant of the preceding operation would be to have the waveform extract the packet header data and pass it in over separate CORBA ports configured for that purpose. It would then be the Waveform's responsibility to ensure synchronization which may be very difficult to accomplish reliably.

An alternative method would be to make the CSF cognizant of which specific header information is allowed to be bypassed and which is not, including any applicable restrictions. This could be part of a waveform security policy or as basic design criteria. The CSF could then extract that header information from the outgoing PT or incoming CT streams and re-insert the information after the message packet has been decrypted / encrypted. In this latter case, a specific channel for header bypass would not be required. When the extraction operation is performed by the CSF, the

RSS components simply pass in the data packets, including headers, to the CSF in accordance with platform design and security policy requirements. It will then be the responsibility of the CSF to ensure that the packet header is bypassed as required.

It is recommended that the API set of operations support both options in order to allow the radio platforms security policy to govern over which alternative should be implemented.

#### *4.2.21 WF 21 - Setup (configure)/teardown Waveform Authentication/Integrity Channels*

This set of API operations allows the Waveform to establish one or more channels to the CSF that will support a wide variety of authentication and/or integrity checking operations, including enabling or invoking non-repudiation services to be performed by the CSF when required by the waveform security policy.

These operations include:

1. Establishing a logical channel that will allow the CSF to interact with and authenticate local or remote entities (e.g. devices and/or applications other than users). (See WF 22, and WF 24))
2. Establishing a channel that will allow the CSF to interact with and authenticate local or remote users who optionally may or may not be provided with a physical token (e.g. smart card) to be used in the authentication process. (See WF 23)
3. Establishing a Channel that will allow the Waveform to pass in files and/or other data entities such as certificates and tokens to be authenticated and/or integrity checked by the CSF. (See WF 25 and WF 26)
4. Establishing a Channel that will allow the Waveform to pass in a file and/or other data entities such as tokens for hash calculations or for digital signature to be applied by the CSF. When a digital signature is performed it will utilize a specified certificate’s private key which the Waveform is authorized to either use, or request its use in accordance with waveform or platform security policy and/or waveform or platform configuration data. (See WF 27, WF 28, WF 29 )
5. Establishing a Channel that will allow the Waveform to either pass in or retrieve a digital certificate and the associated private key. The CSF shall ensure the Waveform is authorized access to the identified certificate in accordance with waveform or platform security policy and/or waveform or platform configuration data.(See WF 30 and WF 31)

These channels may be established on the RED, BLACK or both RED and BLACK sides of the CSF as needed by the Waveform and as permitted by the waveform security policy.

This set of API operations shall occur via the Control Channel created and configured by the waveform API operations defined by WF 01.

#### *4.2.22 WF 22 - Authenticate Remote Device/Application*

This set of API operations provides the Waveform with the ability to request the CSF to authenticate a designated remote device or application entity as to their identity.

This set of API operation shall optionally allow the waveform/application to identify the hash and/or signature algorithms used for the authentication/integrity/signature processes when there is more than one possible choice.

The Waveform may optionally request that the CSF also verify that the entity is authorized access to perform whatever operation/action initiated the authentication request, and to identify the operation for which access is being requested.

When entity access authorization verification is requested as part of the authentication, this API set shall provide the Waveform the ability to identify the entity and the specific waveform configuration data to be used when ascertaining whether or not the entity is authorized to perform the operation/action.

This API set shall include the ability to enable or invoke non-repudiation logging services to be performed by the CSF when required by the waveform security policy.

The authentication processes for these operations may use certificates which have been pre-stored in the CSF or which has been received by the Waveform and passed into the CSF (IAW WF 31). Whether or not the CSF retains a waveform provided certificate may be a waveform or Radio Platform Security Policy parameter.

The CSF shall provide the Waveform with the results of this request when the authentication process has been completed.

The API design may provide the related configuration operations outlined above either as a separate operation via the Control Channel established per WF-01 or they may be incorporated as operations within the channel established by WF 21-1. The actual authentication request, CSF responses and results as well as the authentication process between the CSF and the Remote Device/Application shall occur over the channel established per WF 21-1.

### *4.2.23 WF 23 - Authenticate Local/Remote User (with/without physical token)*

This set of API operations provides the waveform with the ability to request the CSF to authenticate a local or a remote user entity to the claimed identity. The authentication request shall include the capability to indicate whether or not a user token will be involved.

This set of API operation shall optionally allow the waveform/application to identify the hash and/or signature algorithms used for the authentication processes when there is more than one possible choice.

The waveform may optionally request that the CSF also verify that the user is authorized access to perform whatever operation/action initiated the authentication request and to identify the operation for which access is being requested.

When entity access authorization verification is requested as part of the authentication, this API set shall provide the waveform the ability to identify the entity and the specific waveform configuration data to be used when ascertaining whether or not the entity is authorized to perform the operation/action.

This API set shall include the ability to enable or invoke non-repudiation logging services to be performed by the CSF.

The authentication processes for these operations may use certificates which have been pre-stored in the CSF or which has been received by the waveform and passed into the CSF. Whether or not the CSF retains a waveform provided certificate may be a waveform or Radio Platform Security Policy parameter.

The CSF shall provide the waveform with the results of this request when the authentication process has been completed.

The API design may provide the related configuration operations outlined above either as a separate operation via the Control Channel established per WF-01 or they may be incorporated as operations within the channel established by WF 21-2. The actual authentication request, CSF responses and results as well as the authentication process between the CSF and the Local/Remote user shall occur over the channel established per WF 21-2.

### *4.2.24 WF 24 – Authenticate Local Device/ Application*

This set of API operations provides the waveform with the ability to request the CSF to authenticate a local device or application entity as to their identity.

This set of API operation shall optionally allow the waveform/application to identify the hash and/or signature algorithms used for the authentication processes when there is more than one possible choice.

The waveform may optionally request that the CSF also verify that the local device or application entity is authorized access to perform whatever operation/action initiated the authentication request and to identify the operation for which access is being requested.

When entity access authorization verification is requested as part of the authentication, this API set shall provide the waveform the ability to identify the entity and the specific waveform configuration data to be used when ascertaining whether or not the entity is authorized to perform the operation/action.

This API set shall include the ability to enable or invoke non-repudiation logging services to be performed by the CSF when required by the waveform security policy.

The authentication processes for these operations may use certificates which have been pre-stored in the CSF or which has been received by the waveform and passed into the CSF. Whether or not the CSF retains a waveform provided certificate may be a waveform or Radio Platform Security Policy parameter.

The CSF shall provide the waveform with the results of this request when the authentication process has been completed.

The API design may provide the related configuration operations outlined above either as a separate operation via the Control Channel established per WF-01 or they may be incorporated as operations within the channel established by WF 21-1. The actual authentication request and CSF responses/results shall occur over the channel established per WF 21-1.

The authentication process between the CSF and the local device/application shall occur over a channel established per WF 21-1 or a pre-designated platform interface in accordance with waveform and /or platform security policy design requirements.

### *4.2.25 WF 25 – Authenticate file/token/data/certificate*

This set of API operations permit requesting waveform/application to have the CSF authenticate the signature for a file or other data entity such as a token or digital certificate.

This set of API operations shall optionally allow the waveform/application to identify the hash and/or signature algorithms used for the authentication/integrity/signature processes when there is more than one possible choice.

This API set shall include the ability to enable or invoke non-repudiation logging services to be performed by the CSF when required by the waveform security policy.

The authentication processes for these operations may use certificates which have been pre-stored in the CSF or which have been received by the waveform and passed into the CSF. Whether or not the CSF retains a waveform provided certificate may be a waveform or Radio Platform Security Policy parameter.

The CSF shall provide the waveform with the results of this request when the authentication process has been completed.

This set of operations also includes the act of the waveform/application transferring the file/token/data to the CSF and the return of the CSF determination whether or not the file, token, certificate or other data was determined to be authentic.

The API design may provide the related configuration operations outlined above either as a separate operation via the Control Channel established per WF-01 or they may be incorporated as operations within the logical Channel established by WF 21-3. The actual authentication request and the passing of the information to be authenticated shall occur via the logical Channel created, and configured by the waveform API operations established per WF 21-3.

### *4.2.26 WF 26 - Integrity Check file/token/data/certificate*

This set of API operations provides the requesting waveform/application with the ability to have the CSF perform an Integrity check on a file, or other data entity such as a token or digital certificate.

This set of API operation shall optionally allow the waveform/application to identify the hash or other type of algorithm to be used for the integrity check process when there is more than one possible choice.

This operation includes the act of the waveform/application transferring the file/token/data to the CSF and, after performing the requested check, the CSF shall return the pass/fail results to the waveform/application via the same channel.

This set of API operations shall occur via the logical Channel created and configured by the waveform API operations established per WF 21-3.

### *4.2.27 WF 27 - Provide Digital Signature for file/token/data*

This set of API operations permits the requesting waveform/application to have the CSF create a digital signature for a file, or other data entity such as a token or other data using the public or private key associated with a specified digital certificate which the waveform has authorization to use.

The request shall optionally allow the waveform/application to identify the hash and/or signature algorithm to be used when there is more than one possible choice.

The waveform request shall include the capability to identify a specific certificate and whether or not the associated public or private key is to be used for the signature process.

When a public key is used for the signature, the authentication processes for these operations may use certificates which have been pre-stored in the CSF or which has been received by the waveform and passed into the CSF. Whether or not the CSF retains a waveform provided certificate may be a waveform or Radio Platform Security Policy parameter.

This operation includes the act of the waveform/application transferring the file/token/data to the CSF and the CSF returning the results (The signature or signed file/token/data) to the requesting waveform/application.

This set of API operations shall occur via the Channel created and configured by the waveform API operations established per WF 21-4.

### *4.2.28 WF 28 - Provide Hash for file/token/data*

This set of API operations permits the requesting waveform/application to have the CSF generate a hash of perform an Integrity check for a file, or other data entity such as a token.

This operation includes the acts of the waveform/application transferring the file/token/data to the CSF and the CSF returning the results to the requesting waveform/application.

The request shall optionally allow the waveform/application to identify the hash algorithm to be used when there is more than one possible choice.

This set of API operations shall occur via the Channel created and configured by the waveform API operations established per WF 21-4.

### *4.2.29 WF 29 - Verify Hash for file/token/data*

This set of API operations permits the requesting waveform/application to have the CSF verify the hash code for a file or other data entity, such as a token using a Channel established per WF 21-4, and provide a response to the requestor that the calculated hash is valid or not valid. With this operation the waveform/application could calculate the hash for the file and is requesting the CSF to compare against a known good and protected (by the CSF) value or could allow the CSF to provide the calculation.

This operation includes the act of transferring the file/token/data to the CSF along with the included hash and the return of the CSF verification whether or not the provided hash is correct. The request shall optionally allow the waveform/application to identify the hash algorithm to be used when there is more than one possible choice.

Note: This operation is almost identical with WF 26. Two differences are that 1) in WF 26 the integrity check may not necessarily use a hash algorithm and 2) the results in this operation are simply pass/fail, whereas WF 26 allows for more possibilities.

### *4.2.30 WF 30 - Retrieve Certificate (s)*

This set of operations provides the waveform/application the capability to request that the CSF retrieve and provide a copy of a specified digital certificate which the waveform/application has been authorized to use (See description for WF 21-5).

This set of operations includes the request containing the identification of the specific certificate(s) and private//public key(s) needed by the waveform/application and subsequently the CSF response which passes out the requested certificate and key material.

This set of API operations shall occur via the Channel created and configured by the waveform API operations established per WF 21-5.

### *4.2.31 WF 31 - Accept/pass in Certificate*

The set of API operations provides the capability for a waveform/application to pass in a digital certificate associated with another entity in the network in which the platform operates, which will be used by either the CSF or the waveform/application for authentication and integrity checking operations.

This operation assumes that the certificate includes adequate information regarding the Identification of the associated network entity.

It may be assumed that the function(s) and/or the operations that the network entity is authorized to perform may be derived from any “role” included as part of the digital certificate or that the waveform/application configuration data or the platform configuration data includes such information associated with the identity of the certificate’s owner at the time the certificate is passed into the CSF.

This set of API operations shall occur via the Channel created and configured by the waveform API operations established per WF 21-5.

### *4.2.32 WF 32 Encrypt/Decrypt File/Token/Data*

This set of API operations provides the capability for a waveform/application to pass in a file, token or other data set for encryption/decryption by the CSF and have the results passed out via a designated port.

This API shall use the logical channels created by the waveform using the option available in WF 06 for this purpose.

# 5 Requirements in Support of Waveform Security Operations

This section presents the functional requirements for accessing the common services that may be supplied by an International Radio Security Services component in conjunction with the Radio Platform's CSF. A general description and list of functional requirements accompanies each service. The API requirements in the following paragraphs are only intended to address API functional requirements in support of waveform/application portability. As such, there are no requirements which are directed at specifying API requirements for services delegated to the Radio Platform or other components of a network. In some instances there are services which are totally left to the discretion of the Platform API set. In addition, for those services for which waveform API requirements have been specified, they are not intended to constrain or limit in any way the Radio Platform API providing an identical API or similar service for use by non-waveform applications and services. Those are left strictly to the discretion of the radio platform developer. However, adherence to the LPP and process separation principles would require at least a separate middleware (CORBA) port for use by the platform and preferably a separate physical port into the CSF which is not accessible by the Waveform or other non-platform services/applications. The set of requirements which follow are intended only to specify the required functionality and other than indicating applicability of LPP and process separation security principles, the requirements are not intended to require any specific implementation.

The listed radio security services are an abstraction that hide the underlying interfaces between the radio platform and the embedded cryptographic module with the aim to make the waveform API agnostic to the Radio Platform Security Architecture, including the cryptographic module and security services implementations.

Please note that there is no intent that there will be a one-to-one corresponding API for each security service or API set identified in this document with the resultant set of IRSS APIs and their operations, so long as the defined IRSS APIs includes the functional capabilities specified here-in.

As stated in earlier sections there are some security service operations that may be performed within the waveform or by a Centralized Security Function. These choices are a function of the waveform design and its associated requirements as well as the platform security policy. In these instances, the API will need to support additional operations that might otherwise be internal. This is necessitated by the need for the API to be independent and agnostic to the underlying radio security architecture as discussed previously in 3.2. It is also relevant to the implementation of some legacy waveforms.

In the process of developing the API operations sets, the design should first consider the API from the perspective that reflects all designated radio security services that will be provided by the Centralized Security Function (CSF). When this is complete, the analysis shall then consider API needs where the Waveform would perform those designated aspects of the security service as exemplified throughout Chapter 3.

**Example:**

> In some situations the Waveform might need to have an authentication performed. The actual authentication process (or portion thereof) could occur within the Waveform or it might be relegated to a CSF. In the first instance the Waveform would need to retrieve key material, certificates etc. in order to perform the required authentication. It might also need to have any certificates received in the process authenticated down to the root level. Alternatively the Waveform could pass into the CSF whatever material needs to be authenticated and let the CSF perform the required operations. Clearly these two different approaches impose different requirements on the APIs. Any necessary derivation or clarification of the services used shall be clearly shown in the details of an appropriate use case example.

Table 12 is a summary of the International Radio Security Services needs for all of the waveforms as described in Section 3. This table identifies in a high level manner those services which the IRSS Waveform API Set must be capable of supporting as well as those which are fall within the responsibility of the Radio Platform API set.

In the sections which follow the integrity requirements have been combined with the authentication and non-repudiation requirements since all identified Integrity security services is a logical subset of the authentication services.

In addition and in the interest of simplification, the term waveform/application which has been used previously throughout the document has been shortened to simply “waveform” in the requirements which follow. Notwithstanding these requirements apply to any non-waveform application that is not a part of the RPOE applications and services.

**Table 12: Waveform Security Service Needs Summary**

| SERVICE CLASS | SERVICES | WAVEFORM | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPBAHN | TDMA SATCOM | | UHF TACSAT | HF 2G/3G ALE | VHF/UHF | | P25 |
| | | | Current | Future | | | Current | Future | |
| Access Control Services for Identification and Authorization: | Human-SDRD Interface interactions | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Software Downloads/Updates | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Policy Downloads & Updates | Waveform API | Platform API | Platform API | Not applicable | Platform API | Platform API | Platform API | Platform API |
| | Configuration Data downloads/Updates | Waveform API | Platform API | Future Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Remote access/use of platform resources | Platform API | Not Applicable | Future Waveform API | Not applicable | Not applicable | Platform API | Platform API | Platform API |
| Authentication and Non-repudiation Services | Users | Platform API | Not Applicable | Future Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | User Devices | Waveform API | Not Applicable | Future Waveform API | Platform API | Platform API | Platform API | Future Waveform API | Waveform API |
| | Network Devices | Waveform API | Not Applicable | Future Waveform API | Not applicable | Not applicable | Not applicable | Future Waveform API | Not applicable |
| | Software content providers | Platform API | Not Applicable | Not Applicable | Not applicable | Not applicable | Platform API | Platform API | Not applicable |
| | Network Operators | Waveform API | Not Applicable | Future Waveform API | Not applicable | Not applicable | Not applicable | Future Waveform API | Not applicable |
| | Service Providers | Waveform API | Not Applicable | Not Applicable | Not applicable | Not applicable | Not applicable | Future Waveform API | Not applicable |
| Information Integrity Services | All resident user data | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Waveform related resident radio & network configuration data | Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | All resident software and firmware | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Any waveform specific related downloadable data or software | Waveform API | Platform API | Future Waveform API | Platform API | Not applicable | Platform API | Platform API | Platform API |
| | Over the Air Control and configuration commands | Waveform API | Not Applicable | Future Waveform API | Not applicable | Not applicable | Not applicable | Future Waveform API | Platform API |
| | User communications | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API |

Table 12: Waveform Security Service Needs Summary

| SERVICE CLASS | SERVICES | WAVEFORM | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPBAHN | TDMA SATCOM | | UHF TACSAT | HF 2G/3G ALE | VHF/UHF | | P25 |
| | | | Current | Future | | | Current | Future | |
| Information Security (INFOSEC) Bypass and Confidentiality Services | Network Control communications | Waveform API | Not Applicable | Future Waveform API | Not Applicable | Not applicable | Not applicable | Future Waveform API | Platform API |
| | Device Uploads to networks (e.g., Log data, configuration data) | Waveform API | Not Applicable | Future Waveform API | Not Applicable | Not applicable | Not applicable | Future Waveform API | Platform API |
| | Policy (security, regulatory, etc.) downloads | Waveform API | Not Applicable | Future Waveform API | Platform API | Platform API | Platform API | Future Waveform API | Platform API |
| | Configuration Data downloads | Waveform API | Platform API | Future Waveform API | Platform API | Platform API | Platform API | Future Waveform API | Platform API |
| | Software Downloads | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | User data Storage | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Configuration Data Storage | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Key Material Storage | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Control Bypass | Waveform API | Waveform API | Waveform API | Not Applicable | Waveform API | Waveform API | Waveform API | Waveform API |
| | Header Information Bypass | Waveform API | Not applicable | Not applicable | Not Applicable | Waveform API | Waveform API | Waveform API | Waveform API |
| | Plain Text Audio bypass | Not applicable | Not applicable | Not applicable | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API |
| Transmission Security (TRANSEC) Services | Spread spectrum applications | Waveform API | Not Applicable | Not Applicable | Not Applicable | Waveform API | Waveform API | Waveform API | Not Applicable |
| | Frequency hopping applications | Waveform API | Not Applicable | Not Applicable | Not Applicable | Waveform API | Waveform API | Waveform API | Not Applicable |
| | Cover for waveform control information | Waveform API | Waveform API | Waveform API | Not Applicable | Waveform API | Not Applicable | Future Waveform API | Not Applicable |
| | Cover for waveform data | Waveform API | Not Application | Not Application | Not Applicable | Not Applicable | Not Applicable | Future Waveform API | Not Applicable |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Key and Credential Management Services | User's National shared and private keys | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API |

Table 12: Waveform Security Service Needs Summary

| SERVICE CLASS | SERVICES | WAVEFORM | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPBAHN | TDMA SATCOM | | UHF TACSAT | HF 2G/3G ALE | VHF/UHF | | P25 |
| | | | Current | Future | | | Current | Future | |
| | User PKI certificates and related private/shared keys | Waveform API | Not Applicable | Future Waveform API | Not Applicable | Not Applicable | Not Applicable | Future Waveform API | Not Applicable |
| | Regional and/or Coalition shared keys | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API | Waveform API |
| | PINs, Passwords, Biometric access and other electronic credential data | Waveform API | Platform API | Future Waveform API | Platform API | Platform API | Platform API | Platform API | Not Applicable |
| | Device certificates and private/shared keys | Waveform API | Not Applicable | Future Waveform API | Not Applicable | Not Applicable | Not Applicable | Future Waveform API | Not Applicable |
| | Root & intermediate Certification Authority Certificates | Waveform API | Not Applicable | Future Waveform API | Not Applicable | Not Applicable | Not Applicable | Future Waveform API | Not Applicable |
| | Over the Air Zeroize (OTAZ) (Channel specific) | Waveform API | Not Applicable | Future Waveform API | Not Applicable | Not Applicable | Not Applicable | Future Waveform API | Waveform API |
| | Over the Air Rekey (OTAR) | Waveform API | Platform API | Future Waveform API | Platform API | Platform API | Platform API | Future Waveform API | Waveform API |
| | Over the Air key Transfer (OTAT) | Waveform API | Platform API | Future Waveform API | Platform API | Platform API | Platform API | Future Waveform API | Waveform API |
| Platform Resource Security Management Services | Memory Management Enforcement | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | RPOE Software Configuration Management & Version Control | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | RPA Software Configuration Management & Version Control | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| Logging, Auditing and Security Alarm Services | Usage logs | Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Security Event logs | Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Cognitive/DSA Operations logs | Waveform API | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| | Non-repudiation logs | Waveform API | Platform API | Platform API | Not Applicable | Platform API | Platform API | Platform API | Not Applicable |
| | Security Related Alarm services | Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| Logging, Auditing and Security Alarm Services | Audit log preparation | Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |

**Table 12: Waveform Security Service Needs Summary**

| SERVICE CLASS | SERVICES | WAVEFORM | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | IPBAHN | TDMA SATCOM | | UHF TACSAT | HF 2G/3G ALE | VHF/UHF | | P25 |
| | | | Current | Future | | | Current | Future | |
| Policy Enforcement and Management Security Services | The Platform security policy | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Waveform/application security policies | Waveform API | Platform API | Platform API | Platform API | Platform API | Platform API | Future Waveform API | Not Applicable |
| | SDRD Behavioral control (e.g. cognitive/learning radio ) | Waveform API | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable | Not Applicable |
| | Regulatory Policies | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API | Platform API |
| | Other downloadable policies (e.g., Network Management, Network Security | Waveform API | Not Applicable | Future Waveform API | Not Applicable | Not Applicable | Not Applicable | Future Waveform API | Not Applicable |

## 5.1 General Requirements Related to the Waveform IRSS API

The following general requirements shall apply to the extent applicable to the waveform/application, the radio platform or the IRSS API.

5.1-1. As a design goal the International Radio Security Services (IRSS) waveform API shall be agnostic to cryptographic module hardware and software implementations.

5.1-2. As a design goal the IRSS waveform API shall be agnostic to the underlying radio security services implementation.

5.1-3. As a design goal the IRSS waveform API shall be agnostic to the high level security architecture of the Radio Platform.

5.1-4. As a design goal the IRSS API shall be capable of being implemented in any of the four high level security architecture variants described in section 3.2 of this document. These are identified as

a. Multi-level Security,

b. Multiple Independent Levels of Security,

c. Multiple Single Levels of Security, and

d. Single Levels of Security.

Note: The IRSS API designers should all consider the different high level architectural implementations and examined them to determine if there is any influence on RSS API requirements resulting from a given architecture and to ensure that any requirements which emerge are appropriately captured and reflected in the resultant API.

5.1-5. In recognition that future needs of the IRSS API will evolve, the design of the IRSS API shall include, to the extent feasible and practical, provisions for extending API definitions to incorporate these needs.

5.1-6. The IRSS API design shall support enforcement of the Least Privilege Principle.

5.1-7. The IRSS API design shall support the process separation security principles.

5.1-8. The IRSS API shall support IP based standardized network operations and protocols to the extent that these protocols require radio security services.

5.1-9. The IRSS API design shall support standardized security services such as IPSEC V4 and V6, utilized in IP based networks being provided either by the Waveform or by the Platform’s CSF or in some combination of the two.

5.1-10. In order to claim compliance with the WInnForum Waveform API standard, any waveform shall include a documented waveform security policy that is in compliance with the requirements stated here-in.

5.1-11. As a minimum, the Waveform Security Policy shall define the extent to which the waveform supports the RSS API.

5.1-12. The Waveform Security Policy shall define/specify those API operations and their features and capabilities the Waveform requires to support waveform operations

5.1-13. The Waveform Security Policy shall clearly identify those API features and capabilities which are not required by the Waveform.

5.1-14. The Waveform Security Policy shall specify the number (max, min) and types of interface channels (e.g. encryption, decryption, control bypass, TRANSEC etc.) required for the Waveform API.

5.1-15. The Waveform Security Policy shall, for each API permitted operation, indicate whether the operation is a RED side only, a BLACK side only or an operation required from both RED and BLACK processes.

5.1-16. The Waveform Security Policy shall also define those API exception conditions that constitute a security alarm condition with regard to waveform operations.

Note: Waveform security policy elements that are in conflict with Platform Security Policy shall be superseded by Platform Security Policy.

5.1-17. In order for any Radio Platform to be able to claim compliance with the IRSS API, the Radio Platform OE design shall support all of the security policy enforcement measures specified here-in unless specifically superseded by the Radio Platform Security Policy requirements.

5.1-18. The Radio Platform shall ensure that the Waveform shall only be granted the services allowed within the constraints of the waveform security policy, unless further restricted or superseded by the Radio Platform Security Policy.

5.1-19. The Radio Platform shall ensure that the nature and types of operations as well as the number and type of channels needed by a given waveform shall be constrained to those defined by the waveform security policy.

5.1-20. In accordance with the LPP, the radio platform design shall ensure that the IRSS and/or CSF components do not permit any RED or BLACK side operation for a given waveform that is not explicitly allowed by the waveform security policy.

5.1-21. When permitted by the Waveform Security Policy, the IRSS API shall provide the capability for the waveform to configure in entirety or in part, the IRSS API and services required by the waveform during the waveform instantiation process.

5.1-22. When permitted by the Waveform Security Policy, the IRSS API shall be support the establishment of a Control Channel which supports waveform API operations. The capabilities specified for the API operations set define in section 4.2.1 for WF 01 (Setup /configure /teardown waveform Control Channel) shall be used as a guide.

5.1-23. The IRSS API Control Channel created by 5.1-22 shall support the creation of other channels between the Waveform and IRSS components for use in cryptographic, TRANSEC, Bypass as well as Authentication/ Integrity and other identified Operations to the extent permitted by the Waveform Security Policy.

5.1-24. When permitted by the Waveform Security Policy, the IRSS API shall support the ability of a waveform to reconfigure the nature and types of services as well as the cryptographic, TRANSEC, control and bypass channels that have been established to include the ability to:

a. Modify the characteristics of an existing channel

b. Delete an existing channel

c. Create an additional channel

## 5.2 Radio Security Services API Requirements

Functional requirements for the IRSS API are contained in the sections which follow.

### *5.2.1 Access Control, Identification & Authorization Services*

Access control related services involve an entity such as a user, operator, remote management center, router, software or policy distribution point requesting access to a device, function or service via a log-in or other identification and authentication process for purposes such as downloading information that could include configuration data, software and/or policy updates or other such similar processes, and being granted access in accordance with pre-defined privileges or because of an authenticated role as in role based access control.

#### 5.2.1.1 Introduction/Overview

References within this specification to the CSF performing an access control function should not be construed to assign any level of assurance to the access control service since such matters are a matter of Radio Platform Security Policy and design.

Waveform specific information such as Access Control Lists, when employed by the waveform, are assumed to be available as part of the waveform application configuration data or as part of the radio platform configuration data. When required by the Radio Platform Security Policy the access control data, if not already managed by the CSF may be provided to the CSF for its use via an appropriate radio platform API.

Access control lists should include information concerning the role and/or access constraints of each entity on the list. Specific properties regarding roles/access constraints are a platform design concern and are not construed to be a part of the IRSS API.

Thus we may assume that the centralized security services, to the extent necessary, will be able to determine from the defined role and/or access privileges whether or not the entity is allowed access to the requested information or service and the nature of the access being granted (i.e. read, write, change, erase, etc.). It is a matter of radio platform design to ensure the validity of these assumptions.

Within the context of this specification, any access control service used by the Waveform is requested as part of an authentication process and includes identification of the entity being authenticated, references to or copies of the entity’s credentials to be used in the authentication process, and optionally references to data which can be used to validate the entity’s authorization to access or perform some operation involving the waveform and the radio platform.

This includes any access control service related to OTAR, OTAT or OTAZ operations as well as to waveform software downloads or updates, policy downloads and updates, configuration data downloads and updates or requests from remote entities/individuals for access to the platform for remote control or configuration of platform functions. These operations typically also invoke a corresponding set of identification, authentication, integrity checking and, when required, non-repudiation security services. COMSEC functions may also be applicable.

The specific methods to be used are not to be construed as being a part of the IRSS API except so far as the Waveform API set includes appropriate API operations which permit these processes to occur. When these operations are invoked via the waveform API set, it may be assumed that the waveform is capable of invoking the required API’s in the correct sequence and manner necessary to manage the identification and authentication of the entity, and to ensure that the entity is authorized to perform the associated operation(s).

#### 5.2.1.2 Access Control API Requirements

The IRSS Waveform API shall conform to the following requirements regarding Access Control.

5.2.1-1. The Radio Platform, to include the CSF, shall only support waveform Access Control Service requests from waveforms whose associated security policy stipulates this functionality as a necessary component of the waveforms API set, and only to the extent permitted by the waveform’s security policy.

5.2.1-2. The access control service request shall include the capability for the Waveform to identify the entity to which the request applies.

5.2.1-3. The access control service request shall include the capability for the Waveform to identify the specific waveform configuration data to be used when ascertaining whether or not the entity is authorized to perform the operation/action.

5.2.1-4. The access control service request shall include the capability for the Waveform to identify the types of actions/activities to which the request applies. Such activities should consider the following as examples:

a. The IRSS Waveform API shall support waveform requested access control services for local or remote entities supporting download and distribution of waveform related policies. Examples of such policies include but are not necessarily limited to waveform related security policies, routing policies, cognitive radio behavioral policies, Quality of Service policies, and regulatory policies.

Note: The policy download may have been initiated as a "push" operation from a remote entity or at the request of a processing component of the waveform or the platform.

b. The IRSS Waveform API shall support waveform requested access control services from local or remote entities supporting the download and distribution of waveform associated configuration data and related updates.

c. The IRSS API shall support waveform requested access control services from local or remote entities for purposes of configuring or changing the configuration of a radio channel to support waveform operations.

d. The IRSS API shall support waveform requested access control services for devices and/or users initiating OTAR or OTAT operations.

e. The IRSS API shall support waveform requested access control services for devices and/or users initiating waveform specific OTAZ operations.

5.2.1-5. Access control services shall only be employed in conjunction with corresponding identification, authentication and, when so designated, non-repudiation services.

5.2.1-6. Representative Waveform Use Case operations WF 22, WF 23 and WF 24 shall be used as a guide for determining requesting access control services in conjunction with a corresponding Authentication request.

### *5.2.2 Authentication, Integrity and Non-repudiation Services*

Authentication services involve methods to unambiguously verify the identity of an entity. Examples of entities include a device such as a router, another radio, a network server, a specific software/firmware application or process such as service providers, or the identity of a local or remote user. Users may include actual communicators, operators, as well as individuals fulfilling network roles.

In addition, authentication can be applied to any form of digital documents, data files or credentials such as PKE certificates to ensure the validity and integrity of the information contained there-in.

Non-repudiation services, when required as part of an authentication process, provide an indisputable data record directly related to the activity so that the event and/or data cannot be repudiated by the entity that performed the activity. They are also signed by the recording process. The record is typically stored within an audit or similar protected log.

The IRSS Waveform API shall support these types of services as defined here-in.

#### 5.2.2.1 Introduction/Overview

Authentication processes in a modern tactical radio employing IP based operations are integral to the operation of the radio. In some instances these processes may need to be performed within the waveform, while in other instances the process may require the higher assurance level provided by a CSF performing the authentication. The use of Authentication and Non-repudiation Services for any specific function is waveform dependent and should thus be defined by the waveform security policy.

Authentication may employ standards based processes and data such as those defined by today's internet standards, however, other waveform specific non-standardized processes may also exists such as those provided by the P25 public safety waveform. It is therefore important that the IRSS Waveform API provide the capability and flexibility to support both types to the extent that the detailed requirements for these can be defined.

Furthermore, PKI based authentication processes for these operations may use certificates which have been pre-stored in the CSF or alternatively which have been received by the waveform and passed into the CSF. Whether or not the CSF retains such a waveform provided certificate may be a waveform or Radio Platform Security Policy parameter.

Emerging waveforms will provide the capability to support ad-hoc networking among multi-national forces. Identification and/or mutual authentication is required between any entity joining such a network and an entity which is already a part of the network and is aimed at preventing either a legitimate Device or the Network from being impersonated. These emerging and future radio systems are likely to have the capabilities to support formal (e.g. PKI based) methods of authentication and user identification.

Because of the multinational use of these waveforms in a future coalition force, the issue of potentially multiple root certification authorities must be considered. This is necessary because the roots form the trust anchor for authentication processes.

One approach that may be employed would involve each national force signing and distributing to their respective national forces copies of the root certificates of the other national authorities (cross-certification). In this way the other CA's appear to be intermediate level national CA's. This method allows individual nations the control of which other National CA's are to remain valid in their own national radio communications, thus allowing them to revoke their certification authority should it become necessary.

An obvious alternative would be to distribute and install the roots of each nation/organization involved in all radios. In order to support this alternative, the radio platform would either have to automatically select the proper root certificate, authenticate it against all installed roots or have the waveform identify which root should be used. This latter option assumes the waveform can identify which to use based on information exchanged with the other radio platform.

#### 5.2.2.2 Authentication, Integrity and Non-Repudiation API Requirements

The IRSS Waveform API shall conform to the following requirements regarding Authentication, Integrity and Non-Repudiation security services.

5.2.2-1. The Radio Platform, to include the CSF, shall only support waveform requested Authentication and/or Non-repudiation requests from waveforms whose associated security policy stipulates this functionality as a necessary component of the waveforms API set and only to the extent permitted by the waveform's security policy.

**Authentication Channel Creation and Configuration**

5.2.2-2. The IRSS API shall provide the capability for a waveform to create and configure one or more logical channels for use as a means to request authentication, integrity and non-repudiation services to be provided by the CSF for the following purposes.

a. Establishing a logical channel that will allow the CSF to interact with and authenticate local or remote entities (e.g. devices and/or applications) other than users or to retrieve/update CKLs and CRLs.

b. Establishing a logical channel that will allow the CSF to interact with and authenticate local or remote users who optionally may or may not be provided with a physical token (e.g. smart card) to be used in the authentication process.

c. Establishing a logical channel that will allow the Waveform to pass in files and/or other data entities such as certificates and tokens to be authenticated and/or integrity checked by the CSF.

d. Establishing a logical channel that will allow the Waveform to pass in a file and/or other data entities such as tokens for integrity checking, hash calculations or for digital signatures to be applied by the CSF. When a digital signature is performed it will utilize a specified certificate's private key which the Waveform is authorized to either use or request its use in accordance with waveform or platform security policy and/or waveform or platform configuration data.

e. Establishing a logical channel that will allow the Waveform to either pass in or retrieve a digital certificate and the associated private key. The CSF shall ensure the Waveform is authorized access to the identified certificate in accordance with waveform or platform security policy and/or waveform or platform configuration data.

5.2.2-3. When creating a logical channel per 5.2.2-2 the IRSS API shall provide the capability for the Waveform to designate if a channel is to be established on the RED side or the BLACK side of the CSF as permitted by the waveform security policy.

Note: Some waveforms may require distinct and separate channels on both RED and BLACK sides and the request to establish these channels, depending upon waveform security policy, may originate on only one side or on both in accordance with the waveform security policy.

**Digital Certificate Related Operations**

5.2.2-4. The IRSS API shall provide the capability for the Waveform to request that the CSF provide a copy to the Waveform of a specified digital certificate which the waveform has been authorized to use.

5.2.2-5. The request of 5.2.2-4 shall provide the waveform the capability to identify the specific certificate(s) and private/public key(s) needed by the waveform.

5.2.2-6. The CSF shall respond and pass out the requested certificate and key material over the same channel on which the request was received.

5.2.2-7. The IRSS API shall provide the capability for a waveform, using a logical channel created by the operations of 5.2.2-2.e, to pass into the CSF, for storage and future use, a digital certificate associated with another entity with which the waveform / platform operates and which will be used by either the CSF or the waveform for authentication operations.

Notes:

a. Requirements governing the storage and retention of a waveform provided certificate may be a specific Waveform Security Policy, and/or a Radio Platform Security Policy or design parameter.

b. This operation assumes that the certificate includes adequate information regarding the Identification of the associated entity. It further assumes that if the certificate is to be used an access control operation, the function(s) and/or the operations that the entity is authorized to perform may be derived from any “role” included as part of the digital certificate data or that the waveform configuration data or the platform configuration data includes such information associated with the identity of the certificate’s owner at the time the certificate is passed into the CSF.

**Credential Identification**

5.2.2-8. The means of identifying specific credentials for use in the authentication process shall employ standards based reference/naming conventions to the extent feasible.

5.2.2-9. When non-standards based identification methods must be employed it may be assumed that the waveform configuration data files will provide a mapping between the non-standard and the standardized references. Use of a standardized Key tag bound to the credential is the recommended method.

5.2.2-10. When such configuration data is to be used to map standardized references to non-standardized references, the IRSS API shall provide the Waveform the capability to optionally identify the configuration data to be used. The specific parameters and their interpretation is a matter of radio platform design.

**Remote Device/Entity Authentication and Access Control**

5.2.2-11. The IRSS API shall provide the capability for a waveform to request the CSF to authenticate a designated/identified remote device or application entity as to their identity.

5.2.2-12. The authentication service request of 5.2.2-11 shall be subject to the following optional configuration items:

a. The API shall provide the capability for the Waveform optionally to identify the hash and/or signature algorithms used for the authentication/integrity/signature processes when there is more than one possible choice.

b. The API shall provide the capability for the Waveform optionally to request that the CSF also verify that the entity is authorized access to perform whatever operation/action initiated the authentication request and to identify the operation for which access is being requested.

c. When entity access authorization verification is requested as in b above, the API shall provide the Waveform the capability to identify the entity and the specific waveform configuration data to be used when ascertaining whether or not the entity is authorized to perform the operation/action.

d. This API shall provide the capability for the Waveform optionally to enable or invoke non-repudiation logging services to be performed by the CSF when required by the waveform security policy

e. The API shall provide the capability for the Waveform to identify the credentials to be used by the CSF for the authentication. These operations may use certificates which have been pre-stored in the CSF through platform API operations or which has been received by the Waveform and passed into the CSF per 5.2.2-4.

f. It is the intent that the above configuration parameters are to be included in the authentication service request of 5.2.2-11 to permit the authentication channel created by the waveform with 5.2.2-2.a, to be used for multiple authentication operations involving different entities. An alternative would be to set-up and use such a channel for a single such authentication operation. In such an event then the above configuration items could be applied as needed when the channel is created using the API operation specified by 5.2.2-2.a.

**Local or Remote User Authentication and Access Control**

5.2.2-13. The IRSS API shall provide the capability for a waveform to request the CSF to authenticate a designated/identified local or remote user entity to the claimed identity.

5.2.2-14. The authentication service request of 5.2.2-13 shall be subject to the following optional configuration items:

a. The API shall provide the capability for the Waveform optionally to indicate whether or not a user token will be employed as part of the process.

b. The API shall provide the capability for the Waveform optionally to identify the hash and/or signature algorithms used for the authentication/integrity/signature processes when there is more than one possible choice.

c. The API shall provide the capability for the Waveform optionally to request that the CSF also verify that the local or remote user is authorized access to perform whatever operation/action initiated the authentication request and to identify the operation for which access is being requested.

d. When entity access authorization verification is requested as in c above, the API shall provide the Waveform the capability to identify the user and the specific waveform configuration data to be used when ascertaining whether or not the entity is authorized to perform the operation/action.

e. This API shall provide the capability for the Waveform optionally to enable or invoke non-repudiation logging services to be performed by the CSF when required by the waveform security policy.

f. The API shall provide the capability for the Waveform to identify the credentials to be used by the CSF for the authentication. These operations may use certificates which have been pre-stored in the CSF through platform API operations or which has been received by the waveform and passed into the CSF per 5.2.2-4.

g. It is the intent that the above configuration parameters are to be included in the authentication service request of 5.2.2-13 to permit the authentication channel created by the waveform with 5.2.2-2.b to be used for multiple authentication operations involving different entities. An alternative would be to set-up and use such a channel for a single such authentication operation. In such an event then the above configuration items could be applied as needed when the channel is created using the API operation specified by 5.2.2-2.b

**Local Device/Entity Authentication and Access Control**

5.2.2-15. The IRSS API shall provide the capability for a waveform to request the CSF to authenticate a designated/identified a local device or application entity as to their identity.

5.2.2-16. The authentication service request of 5.2.2-15 shall be subject to the following optional configuration items:

a. The API shall provide the capability for the Waveform optionally to identify the hash and/or signature algorithms used for the authentication/integrity/signature processes when there is more than one possible choice.

b. The API shall provide the capability for the Waveform optionally to request that the CSF also verify that the local device/application is authorized access to perform whatever operation/action initiated the authentication request and to identify the operation for which access is being requested.

c. When entity access authorization verification is requested as in b above, the API shall provide the Waveform the capability to identify the entity and the specific waveform configuration data to be used when ascertaining whether or not the entity is authorized to perform the operation/action.

d. This API shall provide the capability for the Waveform optionally to enable or invoke non-repudiation logging services to be performed by the CSF when required by the waveform security policy.

e. The API shall provide the capability for the Waveform to identify the credentials to be used by the CSF for the authentication. These operations may use certificates which have been pre-stored in the CSF through platform API operations or which has been received by the waveform and passed into the CSF per 5.2.2-4.

f. The API shall provide the capability for the Waveform to identify whether the authentication process between the CSF and the local Device/application will occur over a channel established per 5.2.2-2.a or a pre-designated platform interface in accordance with waveform and /or platform security policy design requirements.

g. It is the intent that the above configuration parameters are to be included in the authentication service request of 5.2.2-15 to permit the authentication channel created by the waveform with 5.2.2-2.c to be used for multiple authentication operations involving different entities. An alternative would be to set-up and use such a channel for a single such authentication operation. In such an event then the above configuration items could be applied as needed when the channel is created using the API operation specified by 5.2.2-2.c.

**File/Token/Certificate Authentication**

5.2.2-17. The IRSS API shall provide the capability for a waveform to request the CSF to authenticate the signature for a file, or other data entity such as a token or digital certificate. This operation includes the requesting waveform passing in the item to be authenticated.

5.2.2-18. The authentication service request of 5.2.2-17 shall be subject to the following optional configuration items:

a. The API shall provide the capability for the Waveform optionally to identify the hash and/or signature algorithms used for the authentication/integrity/signature processes when there is more than one possible choice.

b. This API shall provide the capability for the Waveform optionally to enable or invoke non-repudiation logging services to be performed by the CSF when required by the waveform security policy.

c. The API shall provide the capability for the Waveform to identify the credentials to be used by the CSF for the authentication. These operations may use certificates which have been pre-stored in the CSF through platform API operations or which has been received by the waveform and passed into the CSF per 5.2.2-4.

d. It is the intent that the above configuration parameters are to be included in the authentication service request of 5.2.2-17 to permit the authentication channel created by the waveform with 5.2.2-2.d to be used for multiple authentication operations involving different entities. An alternative would be to set-up and use such a channel for a single such authentication operation. In such an event then the above configuration items could be applied as needed when the channel is created using the API operation specified by 5.2.2-2.d.

**<u>File/Token/Certificated Integrity Operations</u>**

5.2.2-19. The IRSS API shall provide the capability for a waveform to request the CSF to provide an integrity based service for a file, or other data entity such as a token or digital certificate as follows.

a. The service request shall specify one of the following possible actions.

i. Verify data entity integrity

ii. Provide hash for data entity

iii. Verify hash for data entity

iv. Provide signature for data entity

b. This operation includes the requesting waveform passing in the item to be authenticated or integrity checked and optionally a hash/integrity check value to be verified by the CSF.

5.2.2-20. The service request of 5.2.2-19 shall be subject to the following optional configuration items:

a. The API shall allow the Waveform optionally to identify the hash and/or signature algorithms used for the authentication/integrity/signature processes when there is more than one possible choice.

b. When a digital signature has been requested per 5.2.2-19.a.iv, the API shall provide the capability for the Waveform optionally to identify a specific certificate and whether or not the associated public or private key associated with the certificate is to be used for the signature process.

c. When a public key is used for the signature, the authentication processes for these operations may use certificates which have been pre-stored in the CSF or which has been received by the Waveform and passed into the CSF per 5.2.2-4.

   Note: Use of a private key implies the certificate has been pre-stored.

d. It is the intent that the above configuration parameters are included in the authentication service request of 5.2.2-19 to permit the authentication channel created by the waveform with 5.2.2-2.d to be used for multiple authentication or integrity related operations involving different entities. An alternative would be to set-up and use such a channel for a single such authentication operation. In such an event then the above configuration items could be applied as needed when the channel is created using the API operation specified by 5.2.2-2.d.

### *5.2.3 Information Integrity Services*

All Waveform API functions regarding integrity services are available using specific API services and options within the authentication services. (See 5.2.2-2.d, 5.2.2-19 and 5.2.2-20 )

### *5.2.4 Information Security (INFOSEC) Bypass and Confidentiality Services including encryption and decryption*

Information Security Services for International Tactical Radios are arguably one of the most important service sets available to the modern tactical environment. These services include the confidentiality services of encryption and decryption of traffic, platform data and software in storage, as well as secure and protected storage of sensitive files and data such as the cryptographic key material. Another critical aspect of information security is the management and control of bypass channels. The IRSS API shall provide the waveforms the capability to use these services as follows.

#### 5.2.4.1 Introduction/Overview

Table 12 includes among all of the identified security services a summary of those needed by contemporary and future waveforms. AS can be seen several of these INFOSEC security services are not applicable to waveform needs and will be addressed by the Radio Platform Security Policy and API design requirements.

As indicated by the analyses described in Section 3, a diverse range of confidentiality services are required to protect user communications, network management and control communications including the distribution of policies, configuration data and other information.

The distribution of software and the protection of data in storage are also required, but only as a function of Radio Platform Security Policy.

The analysis has shown that some waveforms must support multiple simultaneous encryption/decryption operations for traffic and/or the associated network control and management information, requiring the ability to configure multiple channels with potentially different encryption algorithms and keys and the associated complication of establishing and maintaining a proper association between cipher text and plain text traffic streams. The need for a single waveform to have multiple channels operating at different security levels for user and network traffic is also an important factor. In some instances network traffic encryption may be considered a TRANSEC function while in others it may be considered an INFOSEC function. Thus the API needs sufficient flexibility to accommodate either when a Waveform or Radio Platform Security indicates a specific approach.

In addition waveforms such the IP Based Ad Hoc Networking waveform and the future VHF/UHF LOS waveform supporting coalition operations require multiple simultaneous traffic channels using multiple keys which may be a combination of pre-placed and negotiated keys. In the case of negotiated keys the CSF must be able to directly access the traffic channel in order to participate in key negotiation processes such as the Internet Key Exchange protocol.

Furthermore the ability to configure the INFOSEC channels for virtually any combination of RED and BLACK interfaces facilitates the portability of the Waveform to any of the various system security architectures discussed in 3.2.

Another aspect of re-configurability emerges from HF 2/3G ALE waveforms with the need to switch between voice and data operations and varying air interfaces depending upon what the channel usage may be at any given time. With the kind of waveform the ability to rapidly switch between different cryptographic equipment protocols or modes within a given protocol is essential. Additionally, the HF waveform needs the ability to cease/suspend traffic encryption/decryption operations when ALE operations are required.

#### 5.2.4.2 INFOSEC Bypass and Confidentiality Services API Requirements

The IRSS Waveform API shall conform to the following requirements regarding INFOSEC Bypass and Confidentiality security services.

5.2.5-1. The Radio Platform, to include the CSF, shall only support waveforms INFOSEC Security Service requests from waveforms whose associated security policy stipulates this functionality as a necessary component of the waveforms API set and only to the extent permitted by the waveform’s security policy.

**<u>Encryption/Decryption Channel Set-up and Configuration</u>**

5.2.5-2. The IRSS API shall provide the capability for a waveform to set-up logical channels for use as a means to request encryption, decryption services from the CSF for any of the following uses.

a. Traffic encryption

b. Traffic decryption

c. File/data/token encryption

d. File/data/token decryption

e. Session Key Negotiation

5.2.5-3. The IRSS API shall provide the capability for a waveform to tear down the channels established by the service request of 5.2.5-2 when the waveform is de-instantiated or otherwise terminated.

5.2.5-4. When permitted by the waveform security policy the IRSS API shall permit the waveform to configure multiple channels for encryption or decryption, each with their own set of operating characteristics and parameters.

5.2.5-5. The IRSS API shall provide a waveform with the capability to configure an encryption or decryption channel created using the service request of 5.2.5-2 using one or more of following configuration options to the extent allowed by the waveform security policy:

a. This API operations set shall permit the definition/specification for the direction of the encryption or decryption operation and support RED to BLACK, RED-RED, BLACK-BLACK and BLACK to RED encryption or decryption operations.

b. When applicable, the API shall provide the capability for the waveform to pair-wise link encryption and decryption channels for both the cipher text and plain text operations.

c. When applicable, and not otherwise inherent to the waveform operation, the API shall provide the waveform the capability to specify the cryptographic equipment protocol (e.g. KG-84) or equivalent, and if none, then the algorithm to be used for encryption and/or decryption operations.

d. When applicable, and not otherwise inherent to the waveform operation, the API shall provide the capability for the waveform to specify the cryptographic mode to be used for encryption and/or decryption operations.

e. The API shall provide the capability for the waveform to specify the key to be used for the encryption or decryption process. The keys may be pre-placed or subsequently negotiated via an IKE or similar process and associated with the waveform channels being set-up and configured.

f. For file/token/data encryption the IRSS API shall support the option for the waveform to specify the use a private or public key associated with a specified Digital certificate for encryption and /or decryption and whether the use of the key applies to the encryption process, the decryption process or both.

5.2.5-6. The IRSS API shall provide a waveform the capability to change the cryptographic equipment protocol, the cryptographic algorithm and/or mode and/or the cryptographic key for an encryption/decryption channel previously established per 5.2.5-2.

5.2.5-7. **Reserved**

**Encryption/Decryption Channel Operations**

5.2.5-8. The IRSS API shall provide the waveform the capability to request the CSF to perform a key-negotiation or session key establishment as required by IP based networks using a channel previously created by the API operation of 5.2.5-2.e.

5.2.5-9. When the CSF completes the operation requested by 5.2.5-8, the CSF shall provide the waveform with the results via the IRSS API (i.e. success/failure) and when relevant to the operation, a reference ID for the key thus created.

Note: The reference ID would preferably be in the form of a specific parameter which is part of a standardized key tag format.

5.2.5-10. The IRSS API request of 5.2.5-8 shall provide to capability for the waveform to identify the specific protocol to be used if not otherwise inherent to the waveform’s operation.

Note: This operation is applicable to Internet Key Exchange (IKE and IKEv2) as well as protocols that may be used by proprietary national systems. The IRSS API shall provide the waveform//application, using an decryption or encryption channel previously created by the API operation of 5.2.5-2, the capability to pass traffic into the CSF for decryption or encryption according to the defined channel type, where-in the CSF shall perform the requested encryption or decryption transformation operation and pass the resultant traffic out the designated corresponding and previously associated decrypted/encrypted traffic channel.

**Bypass Channel Creation and Configuration**

5.2.5-11. The ITS RSS API shall provide the waveform with the capability for the waveform to set-up and configure bypass channels but only to the extent that they are permitted by the waveforms security policy and are required for proper waveform operation. The following channel shall be supported:

a. A plain text audio bypass. Even though configured for bypass, the bypass feature shall only be enabled by the CSF only when waveform specific conditions are met. Those conditions, as well as the specific method by which this bypass is accomplished are determined by both waveform and platform specific security design requirements.

b. A control bypass that allows a waveform specific set of control commands and associated parameters which are permitted to pass from between waveform software components located on the respective RED and BLACK sides of the radio channel subject to CSF scrutiny. This channel shall be a separate logical channel with its own CORBA port identifier

c. A header bypass channel which is a logical channel (associated with a specified cryptographic channel) through the CSF which allows specified packet header fields and associated parameters which are to be extracted from the data stream and re-inserted after the cryptographic transformation (i.e. encryption or decryption) has been applied to the data fields subject to CSF bypass scrutiny in accordance with platform and waveform specific requirements. As a separate operation this API feature can be used to define specific configuration of this bypass should such be required by a waveform.

   Note: Refer to Section 4.2.20 WF 20 for guidance.

d. This set of API operations also includes those necessary to tear down the bypass channels when the waveform is de-instantiated or otherwise terminated.

**PT Audio Bypass**

5.2.5-12. When a plain text audio bypass has been configured by the operations of 5.2.5-11, the IRSS API shall permit a waveform to perform either or both of the following operations when waveform and/or radio platform specific conditions exist. Under the proper conditions it shall be possible for the waveform to perform the following bypass operations:

a. The demodulated plain text audio from the BLACK Side of the radio channel to the RED side of the radio channel, bypassing the decryption cryptographic transform, and delivering the information to the user’s audio channel in a manner consistent with Waveform and Platform Security Policy.

b. In accordance with Waveform and Platform Security Policy, when the proper conditions exist to enable the transmit PT audio bypass in a channel which is processing secure voice, the user plain text audio from the RED side of the Radio shall be passed to the BLACK side of the radio so that it can be modulated for transmission over the air without encryption. The manner in which this transmit bypass operation is achieved is a matter for waveform and platform security policy and design.

   Note: The specific means and conditions by which such a channel that has been configured for plain text audio bypass can be enabled for operation in either the receive or transmit direction will be subject to waveform and platform specific requirements.

**Control Bypass**

5.2.5-13. When a Control bypass has been configured by the operations of 5.2.5-11, the IRSS API shall provide the Waveform with the capability to pass waveform configuration, control and/or status information from the RED (plain text) side of the radio to the BLACK (cipher text) side of the radio and vice versa. This set of API operations are restricted to a designated and properly configured control bypass channel which does not share any CORBA port with any user traffic or other information. The radio platform shall provide the capability to ensure, in accordance with platform and waveform security policy requirements that only the configuration, control or status information, as detailed in the waveforms bypass security policy, passes through this channel in either direction.

**Packet Header or In-channel Bypass**

5.2.5-14. When an encryption or decryption channel has been properly configured per 5.2.5-5, the IRSS API shall provide the capability for a waveform to deliver the packets to the channel for encryption and or decryption. Either the IRSS components or the CSF may optionally extract separate the packet header data in accordance with the configuration defined by 5.2.5-3. Either of the following methods may be used to bypass the designated header information.

c. The header data shall be bypassed only to the extent permitted by the waveform and platform bypass security policies.

### *5.2.5 Transmission Security (TRANSEC) Services*

TRANSEC operations are prevalent in tactical waveforms and these operations encompass a broad range of security services. Frequency hopping and other forms spread spectrum methods are intended to provide an anti-jam (AJ) capability or alternatively and low probability of interception or detection (LPI/LPD). Other forms of TRANSEC are more akin to INFOSEC in that encryption is being used to protect waveform, network or other types of control information like that of the SATCOM orderwire or the HF 2/3G ALE link protection. The summary information in Table 12 illustrates that most, but not all, waveforms utilize TRANSEC services to one extant or another and that there is a need for the IRSS API to support the full range of services.

#### 5.2.5.1 Introduction/Overview

Some forms of TRANSEC are more security sensitive than others. In some legacy waveforms, the TRANSEC operations, including keystream generation, were fully performed by waveform components rather than a cryptographic keystream generator or other similarly protected function. Consequently the IRSS API requirements stipulated below are intended to support the ability of a waveform component to provide the full ranges of TRANSEC functionality in the event that such a capability is needed and permitted by a Radio Platform Security Policy. The IRSS API will also provide the capability to allow for all requisite TRANSEC security sensitive functions such as keystream generation and encryption/decryption of control and orderwire information to occur within the CSF. It is has been assumed that the waveform components will still be allowed to receive and apply CSF generated keystream to the process of frequency hopping and spreading during waveform operations. Radio Platform Security Policy shall define and determine the allocation of TRANSEC operations between the waveform and the CSF. The IRSS

#### 5.2.5.2 Transmission Security (TRANSEC) Services API Requirements

The IRSS Waveform API shall conform to the following requirements regarding TRANSEC services.

5.2.5-1. The Radio Platform, to include the CSF, shall only support waveform INFOSEC Security Service requests from waveforms whose associated security policy stipulates this functionality as a necessary component of the waveforms API set and only to the extent permitted by the waveform's security policy.

**<u>Setup (configure)/teardown Waveform TRANSEC Channels</u>**

5.2.5-2. The IRSS API shall provide the capability for a waveform to set-up and configure logical channels for use as a means to request and receive TRANSEC services from the CSF for any of the following uses.

a. Requesting the CSF to generate and provide keystream to the waveform for use in Waveform TRANSEC operations

b. Requesting Encryption/decryption of Waveform control/orderwire/ALE and other designated information for the waveform's use in waveform air interface and related network and transport layer operations.

c. Requesting and receiving an identified TRANSEC Key for use by the Waveform in waveform TRANSEC operations, and

d. Requesting the CSF to generate a Random or Pseudo-Random Number for use by the Waveform for TRANSEC Operations.

e. (Note: It is intended to allow operations 5.2.5-2 c. and 5.2.5-2 d. to share the same logical channel/CORBA port for these operations, but it is not required the IRSS API mandate sharing.)

5.2.5-3. The IRSS API shall provide the Waveform with the capability to configure multiple channels of the type created by 5.2.5-2 a or by 5.2.5-2b for TRANSEC operations, each with their own set of operating characteristics and parameters but only to the extent permitted by the waveform security policy.

5.2.5-3. When configured for the purpose of keystream generation of 5.2.5-2a, the IRSS API shall provide the Waveform with the capability for specifying the following parameters.

a. When applicable, and not otherwise inherent to the Waveform's operation, the API will provide the Waveform the capability to identify keystream characteristics such as the length of each data block of keystream provided per request, the frequency and/or application bit rate that the CSF should be prepared to support, any specialized parameters such as time of day, or offsets that the CSF must factor in to the generation of the keystream, as well as any other data that may be relevant to the keystream generation and delivery for the Waveform's TRANSEC operations.

b. When applicable, and not otherwise inherent to the Waveform's operation, the API will provide the Waveform the capability to identify the cryptographic equipment protocol (e.g. KG-84) or equivalent, and if none, then the algorithm to be used for keystream generation operations.

c. When applicable, and not otherwise inherent to the Waveform's operation, the API will provide the capability for the Waveform to specify the cryptographic mode to be used for keystream generation operations

d. The API will provide the capability for the Waveform to specify the cryptographic key to be used for keystream generation operations.

5.2.5-4. When configured for the purpose of TRANSEC encryption/decryption of waveform related control/orderwire/ALE information of 5.2.5-2b, the IRSS API shall provide the waveform of specifying the following operational parameters.

a. The API shall permit specifying whether the plain text side of these channels is located on the BLACK or RED side of the CSF unless other defined by specific waveform and/or platform security policy requirements. It is assumed that the cipher text side is always on the BLACK side.

b. When applicable, the API will provide the capability for the Waveform to pair-wise link encryption and decryption channels for both the cipher text and plain text operations.

c. When applicable, and not otherwise inherent to the Waveform's operation, the API will provide the Waveform the capability to identify the cryptographic equipment protocol or equivalent, and if none, then the algorithm to be used for TRANSEC encryption/decryption operations.

d. When applicable, and not otherwise inherent to the Waveform's operation, the API will provide the capability for the Waveform to specify the cryptographic mode to be used for TRANSEC encryption/decryption operations

e. The API will provide the capability for the Waveform to specify a reference ID to identify the cryptographic key to be used for TRANSEC encryption/decryption operations.

Note: The reference ID would preferably be a unique parameter for that key whose value has been extracted from a standardized key tag.

5.2.5-5. Notwithstanding that TRANSEC encryption/decryption may be BLACK side to BLACK side operations, the IRSS API should enforce that separate CORBA ports are required to be used by the waveform for the plain text and cipher text interface operations.

5.2.5-6. The IRSS API shall provide a waveform the capability to change the cryptographic equipment protocol, the cryptographic algorithm and/or mode and/or the cryptographic key for a TRANSEC encryption/decryption channel previously established per 5.2.5-2b.

5.2.5-7. When configured for the purpose of the TRANSEC Key extraction for application and use by the waveform, the IRSS API shall provide the waveform with the ability to identify the key using a reference ID parameter which is unique to the key. (Note: In this instance the waveform is responsible for performing all TRANSEC operations and this logical channel will be used to extract the key from the CSF. As indicated previously it may also be used for requesting and obtaining random numbers for the waveforms use.

5.2.5-8. When configured for the purpose of requesting and receiving random or pseudo-random (PN) numbers, the IRSS API shall provide the waveform with the capability of configuring the following:

a. Whether random or pseudo-random numbers, or both are needed.

b. If pseudo random (PN) numbers are required, then the waveform must identify any parameters, including algorithms and their values, needed by the CSF to properly generate the PN number unless the method is inherent to the waveform (i.e. there is only one method used by the waveform), in which case reference to the identifier which is the proper name for the algorithm/method may be used.

5.2.5-9. The IRSS API shall provide the capability for a waveform to tear down any one or all of the logical channels established by the service request of 5.2.5-2 when the waveform no longer requires the channel or the waveform is de-instantiated or otherwise terminated.

**Perform TRANSEC Encryption/Decryption Operations**

5.2.5-10. The IRSS API shall provide the waveform//application, using a decryption or encryption channel previously created by the API operation of 5.2.5-2, the capability to pass traffic into the CSF for decryption or encryption according to the defined channel type, where-in the CSF shall perform the requested encryption or decryption transformation operation and pass the resultant traffic out via the IRSS API the corresponding and previously associated decrypted/encrypted traffic channel.

**Provide TRANSEC Keystream**

5.2.5-11. The IRSS API shall provide the waveform//application, using an TRANSEC channel previously created by the API operation of 5.2.5-2, the capability to pass a keystream request into the CSF for the generation and return of the requested keystream data , where-in the CSF shall perform the requested keystream generation in accordance with the previously defined criteria and pass the resultant keystream data out via the IRSS API to the waveform over the same logical channel.

**Provide/Generate Random Number**

5.2.5-12. The IRSS API shall provide the waveform//application, using a TRANSEC channel previously created by the API operation of 5.2.5-2, the capability to pass a request into the CSF for the generation and return of a random or pseudo-random number. In response the CSF shall perform the requested random/pseudo-random number generation in accordance with the previously defined criteria and pass the number data out via the IRSS API to the waveform over the same logical channel.

**Provide TRANSEC Key**

5.2.5-13. The IRSS API shall provide the waveform, using a channel created by the operations of 5.2.5-2 c, with the capability to request the CSF to return a TRANSEC key identified by a standardized reference ID (e.g. a parameter defined by a standardized key tag format). The waveform request will include the above "reference ID" that the CSF shall use to identify the specific key being requested and, after any radio platform security related checks, will return a copy of the key, including any relevant identifying information to the waveform for its use in waveform TRANSEC operations over the same logical channel on which the request was received.

### *5.2.6 Key and Credential Management Services*

As indicated in Table 12 every waveform class listed in the table requires some aspect of key and credential management services from the radio platforms Key and Credential Management Service within the CSF. However the majority of these services are associated with other API operations since the key/credential material is typically being stored until it is needed for waveform operations, and even then, the key material generally remains within the confines of the CSF. The exceptions to this generality are when the waveform receives a certificate and passes it into the CSF for storage, or when a waveform requests a certificate and the associated private key for its use in waveform authentication operations and finally a key may be extracted when the waveform is responsible for a TRANSEC operation fully carried out by the Waveform.

#### 5.2.6.1 Introduction/Overview

All of the above Key and Credential Management IRSS API service requirements have already been addressed in sections 5.2.2.2, 5.2.4.2 and 5.2.5.2. These primarily consist of the Waveform identifying the relevant key and certificate material to be used for CSF provided operations, and in once instance have the CSF perform the creation of a shared key created via an IKE or similar process.

To that end, the CSF is presumed to provide storage and integrity protection services for all key material and all forms of electronic credential data. The CSF Key Management Service is assumed to also be responsible for managing and maintaining the integrity and safety of the key/credential information until it has been erased, zeroized or superseded by designated newer replacement key material. The means and manner of providing confidentiality to any of this information is a matter left to waveform or platform Security Policy design requirements and will not be not subject to specification via any of the defined RSS API's.

Digital certificates for network users/devices can be received via standard protocols and used for a variety of other security services such as authentication, integrity checking etc. Consequently it is necessary that the IRSS API support the Waveform passing in certificates for temporary or long term storage and for retrieving them should the Waveform require them in support of another waveform operation. These API operations have been called out in section 5.2.2.2.

As indicated in Table 12 the remaining topic for waveform specific Key Management services involves the over-the-air initiated operations of zeroization, rekey and key file transfers. Other than P25 which supports OTAZ function there are no standardized methods regarding how an OTAZ is performed. Once again while P25 supports an OTAR operation, legacy tactical radio OTAR and OTAT operations were operator initiated and involved the use of fill devices working directly with the Cryptographic equipment. The “waveform” was essentially ignorant of the process underway. Besides P25, the only other waveform classes that are presumed to support these operations are hypothetical /future waveforms. Thus there is no specific information about these types of operations other than that for P25.

For the remaining waveforms which are representative of those whose cryptographic equipment supported OTAR and OTAT, there are no applicable waveform IRSS API requirements since this functionality is allocated to the Platform IRSS API.

These operations only apply to those waveform classes which have cognizance that such an operation has been initiated to one extent or another. This is the case for the P25 waveform which includes a set of Key Management Messages (KMMs) used for over-the-air rekeying as well as over the air zeroization.

For example the Waveform may be informed that a key management service request is required but not be aware of the specific services. In such an instance the Waveform might initiate a service request and then pass in an encrypted file which when decrypted an authenticated by CSF would be recognized as, for example, an over-the-air zeroization request. This is the case for the P25 waveform.

Alternatively the Waveform could have cognizance that an over-the-air zeroization request has been received along with an encrypted file containing the reference identifiers of all of the channel specific keys that are to be zeroized. This file could then be passed into the CSF for decryption and authentication and subsequent zeroization of the identified keys assuming that all of the listed keys were associated with the channel making the request.

Note: It is assumed that Zeroization of the waveform's channel specific key's or digital certificates is a waveform API function but general Zeroization operations affecting other channels or the entire radio are platform API functions.

The requirements in the next section have been written to allow either of these two scenarios to be applicable.

#### 5.2.6.2 Key and Credential Management Services Radio Platform Assumptions

5.2.6.2-1. It is assumed that all key material including certificates and user/device/entity credentials will be identified via standardized identifier tags and that one or more common standards are shared by the waveform and the platform for means of identifying and referencing any specific key used by the waveform.

5.2.6.2-2. It is assumed that any platform which accepts a key without a standardized tag will provide the means to create such a tag when the key material is loaded or installed onto the platform.

5.2.6.2-3. It is assumed that the radio platform will provide the capability to map non-standardized key references, such the legacy key position/slot ID number, to specific keys. Such mapping may be via a waveform configuration data file, or via the radio HMI.

#### 5.2.6.3 Key and Credential Management Services API Requirements

The IRSS Waveform API shall conform to the following requirements regarding Key and Credential Management services.

5.2.6.3-1. The Radio Platform, to include the CSF, shall only support Key and Credential Management Security Service requests from waveforms/applications whose associated security policy stipulates this functionality as a necessary component of the waveform/application's API set and only to the extent permitted by the waveform's/application's security policy.

5.2.6.3-2. The IRSS API shall provide the capability for the Waveform to discover/inquire what key material is available for the Waveform to use for a given instantiation. The request will include a listing of the type of standardized key tag data fields the CSF response to the request should include or indicate the default set. The CSF response to this request will be a listing of the standardized identifiers of keys available to the waveform instantiation along with the specified or default key tag data fields.

5.2.6.3-3. For any IRSS API operation requiring the identification of a key, the API shall provide the capability for the waveform to identify keys either by defined standardized identifiers (which may be platform specific) or those which may correspond to legacy methods such as "key position/slot ID" references. Any such "key position/slot ID" used by a waveform shall be considered specific to that waveform instantiation and the associated keys used by that instantiation. As such the simultaneous use of numerically identical "key position/slot" references shall be permitted by other waveforms but the associations to specific keys are unique to each such instantiation.

5.2.6.3-4. For any IRSS API operation requiring the identification of a digital certificate the API shall provide the capability for the Waveform to identify credentials by defined identifiers which may be specific to a given type of credential. For credentials such as digital certificates contents within the X.509 "Distinguished Name" field shall be capable of being used in addition to any platform specific reference scheme based on the use of standardized key tags.

5.2.6.3-5. The IRSS API shall provide the Waveform with the capability to create a logical channel to be used for Key Management operations between the waveform and the CSF.

5.2.6.3-6. The IRSS API shall provide the capability for the waveform to pass into the CSF any externally received Key Management Messages used for any of the following purposes:

a. To download one or more keys into the CSF for the Waveform.

b. To zeroize one or more, including all keys being stored by the CSF for the waveform.

c. To cause a changeover in use for the Waveform from a current key to a new key either previously downloaded, or that is included in the changeover KMM.

5.2.6.3-7. The IRSS API shall support the capability for the CSF, using the channel created by the API operations of 5.2.6.3-5 to return an appropriate (for the waveform) acknowledgement that a KMM has been received or any other waveform appropriate response indicating the action requested by the KMM has been performed successfully which the Waveform may then process according to its requisite performance requirements.

5.2.6.3-8. The IRSS API shall support the capability for the CSF, using the channel created by the API operations of 5.2.6.3-5, to perform a sequence of operations which allow the CSF to directly authenticate the identity of a remote device/entity/application as the source of a KMM when stipulated by the waveform security policy.

Note: Other requirements regarding waveform interfacing either directly or indirectly with the KMF within the CSF have been addressed in earlier sections. These include passing in or extraction of certificates by the waveform for use in authentication processes, and the extraction of TRANSEC keys for use by the waveform to generate and apply keystream for TRANSEC purposes.

### *5.2.7 Platform Resource Security Management Services*

The range of services involved in Platform Resource Security Management is solely dependent upon the Radio Platform Security Policy and Design requirements which determine and drive the Radio Platform Security Architecture.

These might include active hardware based memory resource allocation and operations restrictions to ensure that data is not executed as code, to prevent and/or control overwriting software/firmware program memory spaces. This might include the enablement of the removal of write protection for write protected memory used to protect the integrity of the operating environment software during platform operations or during start-up and shutdown processes. It might also include active data and control bus access control to ensure proper separation and that only authorized devices/services have access to the bus at any given time for any security sensitive operation.

Other obvious services that affect the security of the radio platform, involve the Installation of updates/patches for software components which comprise the Radio Platform Operating Environment (RPOE) and for any Radio Platform applications such as the waveforms. Besides the core framework, RPOE software includes all the software components providing the RSS API, all CSF functionality to include the cryptographic algorithms, and any other services which a specific to the radio platform design.

These software management services involve primarily authentication of any downloads or updates however they may have been received, and ensuring that obsolete software retention is properly managed as mandated by the Radio Platform Security Policy. Other examples of such services include enforcement of the Radio Platform Security Policy regarding software version control including rollback to an earlier version as well as providing various measures to protect the confidentiality and integrity of the various versions of software that may be maintained in platform file systems.

Based upon the waveform functional requirement analysis there have been no specific Services in this class which have been identified that require any specific interaction between the waveform or other non-RPOE application and the CSF. Thus any APIs that may exist are relegated to the Radio Platform API set.

### *5.2.8 Logging, Auditing and Security Alarm Services*

Logging, Auditing and Security Alarm services are generic to any tactical Radio Platform and are essential tools in the detection of potential intrusion attempts or compromising activities, as well as providing evidence of any such activities. Non-repudiation records are similarly maintained in a log which may be separate or integrated with other logs.

Audit logs are typically designed to record many different types of events. Logs which maintain a record of security related events might include cognitive/DSA activities, HMI activities, non-repudiation events, and security related alarm events typically will record the name of the event and a time of occurrence as a minimum, but might include additional information such a identifiers, credentials etc., when an HMI or non-repudiation event is involved. In some cases logging can be configured to allow selective disabling of recording certain event types.

#### 5.2.8.1 Introduction/Overview

A given platform may have a requirement to count the occurrences of certain types of events and prepare and transmit a report when a threshold is exceeded for a given event types. Security Audit logs are typically reviewed on a periodic basis by authorized security officers using the radio HMI. These processes may include filtering options so that the security officer can examine selected event types, or perhaps the activities of a given individual who has HMI access. When required the security officer can request a record of the log activities, the means by which this log record may be provided would be specific to a given platform.

In the context of the Software Communications Architecture, one of the services that is a part of the core framework is a logging service and this may be used by any process to record activities. Where and how the log is maintained is not specified in the SCA. However, Radio Platform Security Policy (RPSP) may require that security related events be recorded in a protected log within the CSF and the contents may be stored in encrypted form as well as provided cryptography based integrity protection. The RPSP may also mandate that security related events are reported to a different functional interface than other types of log events, thus there might be a regular SCA based logging service and another maintained by the CSF. Any such differences would typically be accommodated in the waveform porting process.

IP based waveforms involve many different types of activities, some of which may generate events which are needed to be recorded in a log and some of these may be security related. Thus in the analysis of Section 3, it was determined that access to logging, auditing and security alarm services should be included as part of the waveform AP. Note that the Radio Platform side of the API will be subject to RPSP requirements.

Modern tactical radio networks are typically managed using resources that are either part of the network or have direct access to the network so that they can disseminate and retrieve information. An example could be a network management/planning center, or a Key Management Facility. While radios might have a hardware interface which can support log extraction among other activities, an air interface supporting network management commands would provide a means to gather information without the need to physically access the radio. For the IPBAHN and other future waveforms, the ability for the IRSS API so support such requests has been identified in Section 3.

External requests for these services may apply to just waveform related events and activities or to the entire Radio Platform. The extent to which they apply to an entire radio platform's log activities is a matter subject to the Radio Platform Security Policy.

#### 5.2.8.2 Logging, Auditing and Security Alarm Services API Requirements

The IRSS Waveform API shall conform to the following requirements regarding logging, auditing and security alarm services.

5.2.8.2-1. The Radio Platform, to include the CSF, shall only support Logging, Auditing and Security Alarm Service requests from waveforms/applications whose associated security policy stipulates this functionality as a necessary component of the waveform

API set and only to the extent permitted by the waveform's/application's security policy.

5.2.8.2-2. The IRSS API shall provide the waveform with the capability to create one or more logical channels to be used for Logging, Auditing and Security Alarm related operations between the waveform and the CS as follows:

a. To provide the capability for the waveform to pass into the CSF messages received from a Network or Security Management entity.

b. To provide the capability for the CSF to return an appropriate (for the waveform) acknowledgement that a Network/Security Management Message has been received via the waveform and/or a response indicating the action requested in a received message has been performed successfully/unsuccessfully that the Waveform may then process according to its requisite performance requirements.

c. To provide the capability for the CSF to perform a sequence of operations which directly authenticates the identity of a remote device/entity/application as the source of Network/Security Message when required by the waveform or Radio Platform Security Policy.

d. To provide the capability for the CSF to return the requested log contents in accordance with an authenticated and authorized log request.

5.2.8.2-3. The IRSS API shall support the capability for the Waveform to act as the proxy for the remote entity (i.e. the waveform processes the management message) and to request that the CSF perform one or more of the actions supported by the API for this purpose.

5.2.8.2-4. The IRSS API shall provide the capability for an authorized entity via the Waveform to request a copy of waveform and/or platform related log events. These may include as examples Security Event logs, non-repudiation logs, HMI activities logs, Cognitive Behavior/Direct Spectrum Access logs and Configuration Management logs.

5.2.8.2-5. The IRSS API shall provide the capability for waveform's extraction request to permit the following:

a. The identification of a date ranges, either specific (from this date to another date) or more general (the last day, week, month), and whether or not that portion of the log may be deleted/overwritten.

b. The identification of specific types of events or designated event subsets (e.g. alarms).

c. The identification of a symmetric key and the algorithm to be used for encryption of the log and/or a digital certificate and its associated private or public key to be used for securing the content of the log and for creating a digital signature for the result log file.

d. To optionally allow the waveform to specify the hash and/or signature algorithms in the event that more than one must be supported in accordance with the waveform's or the radio platform's security policy.

### *5.2.9 Policy Enforcement and Management Security Services*

Policy Enforcement and Management related security services provided by any given Radio Platform will be governed by the specifics of the RPSP for that radio platform. The RPSP will define the scope of the services and the role of the CSF related to each type of policy that is relevant to that Radio Platform. While the enforcement of many policies may be integral to the design of the Radio Platform hardware and software, there exists situations where machine interpretable policies governing networking activities such as routing, quality of service and perhaps firewall configurations will need to be distributed and then placed into storage and then into use by the responsible processes. Future needs for cognitive radio behavior and ad hoc networking are also likely to emerge.

#### 5.2.9.1 Introduction/Overview

In section 5.2.1, 5.2.2 and 5.2.3 we have addressed Waveform security API's needed for the download process to include access control/authorization, authentication and integrity services for these policies. We also have addressed INFOSEC service needs for the download process with the API provisions of section 5.2.4. In this section we shall focus on IRSS API needs recommendations for the necessary security services during storage and for retrieval.

These types of services will ensure that if a policy is needed for a certain process or by a specific application that the correct policy, whose integrity has been maintained, is delivered to the responsible enforcement mechanism. This is the "enforcement" aspect of this service.

The actual entity which enforces the policy is likely a trusted or high assurance process and may be either a separate application/process or it may be incorporated within a centralized security service. If the former is the case, then the centralized security services may play an assisting role in the enforcement.

On the "management" side of this service, it is essential that the authentication and integrity checked version that was received, is maintained such that unauthorized changes or even deletion or substitution of the policy is prevented. This also might imply that the CSF enforced version control.

The specifics of these services are typically defined by the RPSP and may be inherent to the security and other processes regarding download and file storage or they may be called out by a downloadable machine interpretable explicit policy statement. The RPSP should describe the characteristics of the Policy Management and Enforcement Service. While those portions of the platform policies such as waveform policy, regulatory policies, and behavioral control policy may not be part of the RPSP, nonetheless the RPSP should describe the protections afforded these elements. Similarly the Waveform design and Security policy requirements will determine the waveforms responsibilities.

For the Radio Platform the potential range for the Policy Management and Enforcement Security Service would be is responsible for assuring that other security services are woven together to assure that the appropriate policy component is available to its associated enforcement engine. More specifically this service could have responsibility for:

1. Insuring that after successful download or installation on the platform that policy components are placed in secure storage in a manner in which their integrity can be assured. (e.g., his service could apply its own signature to the policy statement).
2. When applicable, periodically checking for expiration of policy statements using platform time resources and alerting appropriate entities of the need to update policy statements.
3. Employing integrity services on secure storage to protect both the policy and the policy enforcement engine while in storage (at rest).
4. Invoking integrity and authentication services to validate that the policy has not been modified when it is retrieved from storage.
5. Authenticating that the policy enforcement executable code (policy enforcement engine) appropriate for the particular policy is active. (This code would be instantiated as a security critical process which may be a separate process or provided as part of this service).
6. Establishing a trusted channel/protected channel between the policy enforcement engine and the storage location of the authenticated policy to allow policy retrieval.
7. Supplying the policy enforcement engine with the appropriate policy.
8. Ensuring that the policy enforcement engine has been provided with all necessary platform support resources such as date and time, geo-location etc.
9. Ensuring that the specific policy enforcement engine is granted the necessary access to other platform resources required to perform its responsibilities.
10. Periodically running integrity checks on the image of the policy being enforced.

The specifics for any given platform will be determined by the platforms own functional requirements and the RPSP. AS can be seen, most, if not all of the above are likely to employ platform API’s as opposed to a waveform API. In the end, it is the responsibility of this service to ensure that all required policies are in place and being enforced by the responsible processes.

Because the majority of the Waveform’s IRSS API needs regarding policy downloads and management are met by other security services, and the specific nature of the policies to be downloaded and used by the waveform are still very general, the requirements for the IRSS API for Policy Management and enforcement can only be generalized.

#### 5.2.9.2 Policy Enforcement and Management Security Services Assumptions

5.2.9.2-1. Where and how downloaded policies are stored and enforced is a matter of platform and waveform specific security policy requirements not affecting the services provided by the IRSS API.

5.2.9.2-2. The waveform will be cognizant when waveform specific policies are received and will be able to request the appropriate combination of access control, authentication, integrity and INFOSEC services required to support the download process.

#### 5.2.9.3 Policy Enforcement and Management Security Services API Requirements

5.2.9.3-1. The IRSS API shall provide the waveform with the capability to request radio security services to enable downloading, storing (within the CSF) and retrieving policies which the waveform uses to enforce operational policies governing waveform activities (e.g., network management, network security, Quality of Service (QOS), etc.) required by the waveform/ application. These services shall include the following as a minimum.

a. Access control services

b. Authentication and Integrity Services

c. INFOSEC services

5.2.9.3-2. The IRSS API operations shall support a waveform’s need to update one or more policies relevant to that waveform’s operation.

5.2.9.3-3. The IRSS API set should support the ability of the waveform to identify the policy as to the type (e.g. security, regulatory, cognitive behavior, network, etc.) and a reference to the identity/reference number of the policy which is being updated, superseded, modified or retrieved for use.

# Appendix A: Abbreviations

| **Abbreviation** | **Meaning** |
|---|---|
| 2G/3G | 2nd and 3rd generation |
| AJ | Anti-Jam |
| API | Application Programming Interface |
| ALE | Automatic Link Establishment |
| BLOS | Beyond Line of Sight |
| CA | Certification Authority |
| CoI | Community of Interest |
| CDI | Cryptographic Device Identifier |
| CIMIC | Civil-Military Co-operation |
| CKL | Compromised Key List |
| COMSEC | Communications Security |
| CRL | Certificate Revocation List |
| CSF | Centralized Security Function (e.g. CSS + other security services) |
| CSS | Cryptographic Subsystem |
| CT | Cipher text |
| DCoI | Dynamic Community of Interest |
| DAMA | Demand Assigned Multiple Access |
| DSA | Dynamic Spectrum Access |
| ECCM | Electronic Counter Counter-Measures |
| HAIPE | High Assurance Internet Protocol Encryptor |
| HF | High Frequency |
| HMI | Human Machine Interface |
| IAW | In Accordance With |
| IKE and IKEv2 | Internet Key Exchange |
| INFOSEC | Information Security |
| IPBAHN | Internet Protocol Based Ad Hoc Networking |
| IRSS | International Radio Security Services |

| | |
|---|---|
| IPsec | Internet Protocol Security |
| JTRS | Joint Tactical Radio System |
| KMF | Key Management Facility |
| KMM | Key Management Messages |
| LPD | Low Probability of Detection |
| LPI | Low Probability of Intercept |
| LPP | Least Privilege Principle |
| LTE | Long Term Evolution |
| LINKSEC | Link Security |
| MILS | Multiple Independent Levels of Security |
| MLS | Multi-level Security |
| MSLS | Multiple Single levels of Security |
| MUOS | Mobile User Objective System |
| NETSEC | Network Security |
| OA | Operation Authority |
| OTA | Over the Air |
| OTAR | Over the Air Rekeying |
| OTAT | Over the Air (key) Transfer |
| OTAZ | Over the Air Zeroize |
| OSP | Organizational Security Policy |
| PN | Pseudorandom |
| PKI | Public Key Infrastrcuture |
| PT | Plain Text |
| QoS | Quality of Service |
| RA | Registration Authority |
| RSS | Radio Security Services |
| RPSP | Radio Platform Security Policy |
| RPOE | Radio Platform Operating Environment |
| RPA | Radio Platform (software) Application (e.g. waveform) |

| | |
|---|---|
| SATCOM | Satellite Communications |
| SCA | Software Communications Architecture |
| SCP | Software/Content Provider |
| SDR | Software Defined Radio |
| SD | Software Distributor |
| SDRD | Software Defined Radio Device |
| SLS | Single Level of Security |
| SSP | System Security Policy |
| SDRD | Software Defined/Software Reconfigurable Radio Device |
| SU | Subscriber Unit |
| TACSAT | Tactical Satellite |
| TDMA | Time Division Multiple Access |
| TIA | Telecommunications Industry Association |
| TRANSEC | Transmission Security |
| UHF | Ultra High Frequency |
| VHF | Very High Frequency |
| WInnF, WInnForum | Wireless Innovation Forum |
| WSP | Waveform Security Policy |

# Appendix B: Glossary

| Term | Meaning (as used within this Document) |
|---|---|
| **API, Platform** | API's which are specific to the underlying platform and which do not impact waveform portability and/or interoperability. These APIs are utilized by RPOE applications and services and are not accessible to the waveform or any non-RPOE application. These API's may conform to some standard and/or portions or all of which may be proprietary. These API's are not accessible by the waveform or non RPOE applications. (See note at end of table). |
| **API, Waveform** | An API provided by the Radio Platform, all of whose characteristics/properties are relevant to Waveform/Application portability and/or interoperability. These are the API operations the Waveform/application uses to interact with the RPOE services and applications. (See note at end of table.) |
| **Channel, Radio** | Baseband RF channel |
| **Channel, Cryptographic** | Abstractions under which one or more cryptographic transforms are performed and within which all configuration details associated with the transform are encapsulated. |
| **Entity** | An "entity", depending upon situation and security service class, might be an individual, either local or remote to the SDR, a network device providing some network service (e.g. router), a remote management facility, or a similar internal SDR function or application. Specific examples of entities are identified and defined in the list of roles/actors contained in Section 2. |
| **Radio Platform Operating Environment (RPOE)** | The RPOE is comprised of the underlying hardware and software that define the operating environment for Waveforms and other non OE applications. Included within the RPOE are the Core Framework and middleware (e.g. CORBA), Radio Security Services and other CSF functionality, the file system and other applications and services provided by the radio platform. |
| **Radio Platform Application** | Any application that can be instantiated on the platform, including any waveform, that is not integral to the RPOE. |
| **Security Policy, Organizational (OSP)** | The **Organizational Security (OSP)** is the broadest and most general of the security policies. The OSP is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide. It is a document intended to guide humans rather than equipment. The OSP is enforced by individuals in the organization. It includes a definition of the assets of the Organization, including the systems and their individual components that must be protected as well as the assurance levels of protection mechanisms. These policies are then applied during the design and development phase of the Organization's systems and their component parts. |

| Term | Meaning (as used within this Document) |
|---|---|
| **Security Policy, System (SSP)** | The **System Security Policy (SSP)** is a set of rules, requirements and practices that specify or regulate how a system (e.g., the networked hardware components, the radio, as well as software and physical plant elements of the system) provide, employ or constrain security services to protect resources. The SSP is therefore a component of the System Security Architecture and Design that implement the relevant aspects of the Organization Security policy. It supplies the technical goals and objectives against which the System Security Architecture and Design are evaluated. The SSP is one element of the decomposition of the OSP. |
| **Security Policy, Radio Platform (RPSP)** | The **Radio Platform Security Policy (RPSP)** is a derivation of the SSP relevant to the radio platform. The RPSP is a set of rules, requirements and practices that specifies or regulates how the radio platform including the RPOE provides, employs and constrains the application of security services to protect resources. Policy enforcement may be either implicit in the design and/or explicit via machine interpretable expressions. In either case, these rules define and of security services, and govern or restrain a system's possible actions as defined by the SSP.<br>The RPSP is a critical required component contributing to the overall radio platform Security Architecture definition, as well as the detailed design and implementation of the entire radio**.** |
| **Security Policy, Waveform** | The Waveform Security Policy (WSP) is the portion of the SSP relevant to a specific waveform. The WSP is a set of rules, requirements and practices that specifies or regulates how the waveform provides, employs and is constrained regarding the application of security services to protect waveform and platform resources. WSP Policy enforcement may be either implicit in the waveform and Radio Platform design and/or explicit via machine interpretable expressions. |