Tactical Radio Coalition Interoperability Facilitated by ANW2 and NINE

Igor A. (Tony) Spivak – Senior Systems Engineer

Presentation Overview

- Coalition Interoperability Challenges.
- Adaptive Networking Wideband Waveform (ANW2) overview.
- NATO Network Internet Protocol Network Encryption (NINE) overview
- Key Management Aspects

Coalition Interoperability Challenges

- Existing systems were not designed with interoperability in mind.
- Desire to safeguard sovereign technology and information.
- Policies that favor “need to know” over “need to share”.
- Export Controls limit releasability to coalition partners.
- Recent successes:
  - Afghanistan Mission Network (AMN)

Overview of the Approach

ANW2

+

NINE Suite B Traffic Protection

+

NINE APPK Based KM

=

Networking Mode to Help Facilitate Coalition Tactical Radio Communications

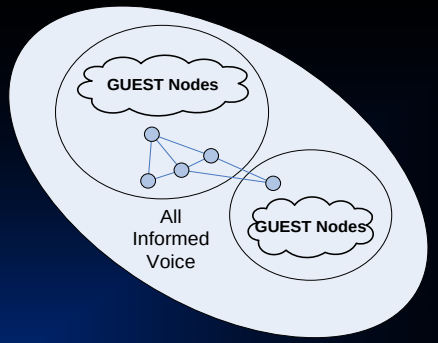
ANW2 Value

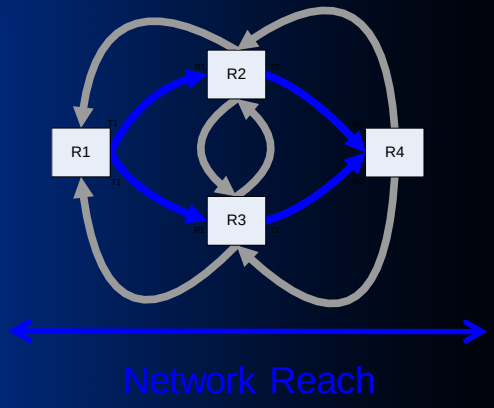
- Fully converged video, CNR voice, PLI, and data in a single waveform
- Robust modulations and adaptive data rate ideal for mobility
- Low configuration and deployment complexity
- Network scalability and interoperability
- Proven, fielded, mature
- SCA V2.2.2 compliant, implemented in a number of Harris SDRs.

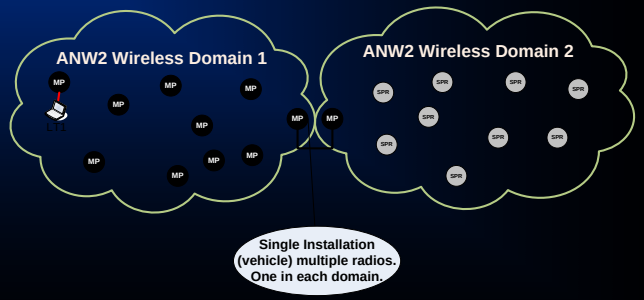
ANW2 provides any easy to deploy and use MANET capability supporting applications including video dissemination, common operational picture, and intelligence data connectivity

ANW2 Features

- Reach over 200 users with networked voice
- Up to 30 users in a single sub-domain
  - Actively transmit and receive data
  - Over 200 users with receive data
- 1.2 MHz or 5 MHz Channel Bandwidth
- High Grade or commercial network encryption capabilities
- Self-managing, forms in *seconds*
- Multi-hop relay of voice and data
- Adaptive data rate
  - Up to 2Mbps, Manpack applications
  - Up to 1.4 Mbps, Handheld applications
- Supports ranges up to 40 km
- TCP/IP Acceleration
- Dynamic routing to integrate the wireless tactical net with external IP networks







Manpack Radio
Vehicular Backbone

1.2 MHz

ANW2 Network

5 MHz

Handheld Radio
Squad Operations

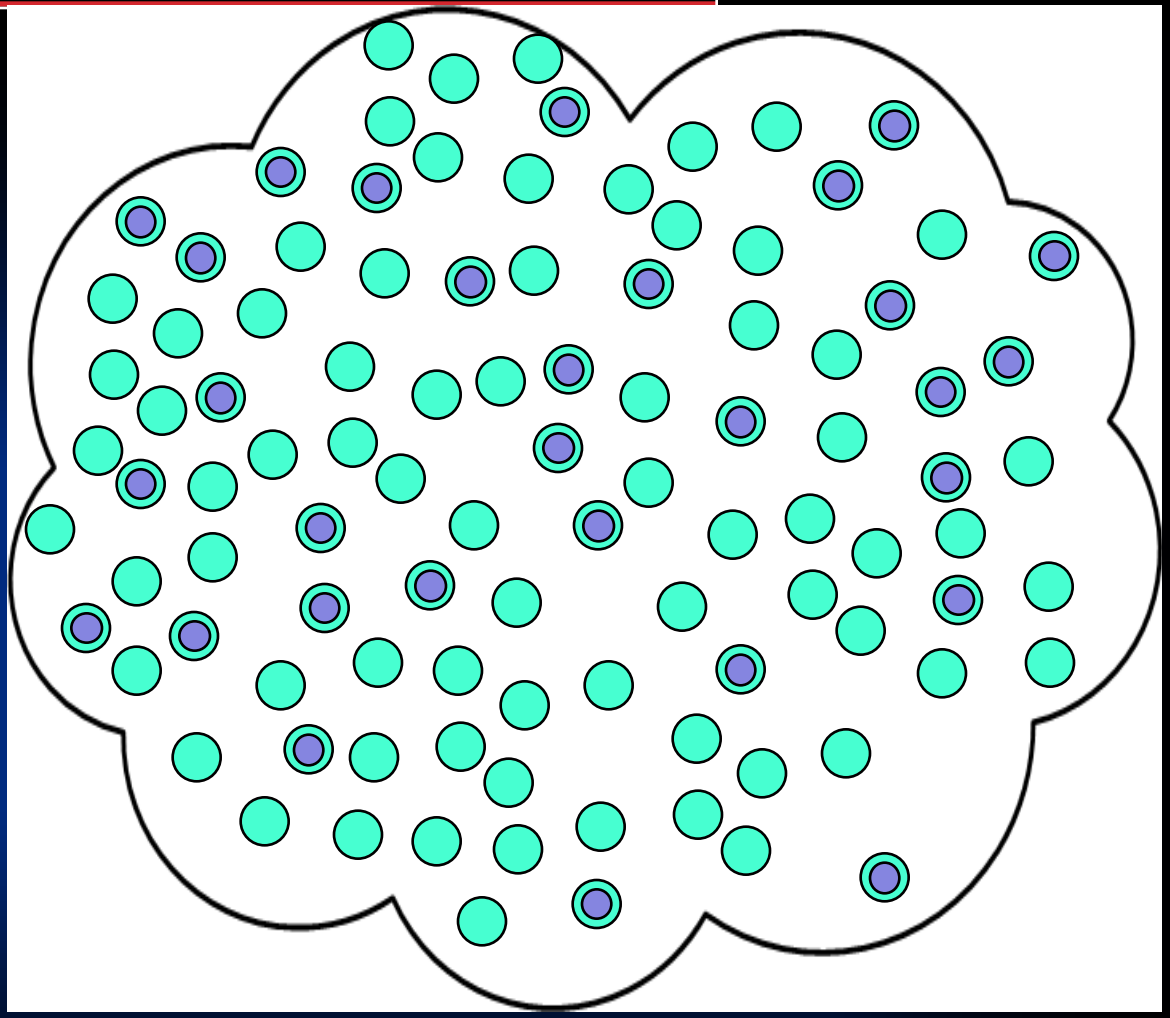
1.2 MHz

Manpack Radio
Dismount Backbone

ANW2 scalable MANET tailors the communication link to meet each end user's application for seamless information sharing across the tactical network

ANW2 - Network Size

- 200 Voice Capable Radios
- 30 Simultaneous Data Sources



ANW2 can be deployed for Battalion wide communication needs

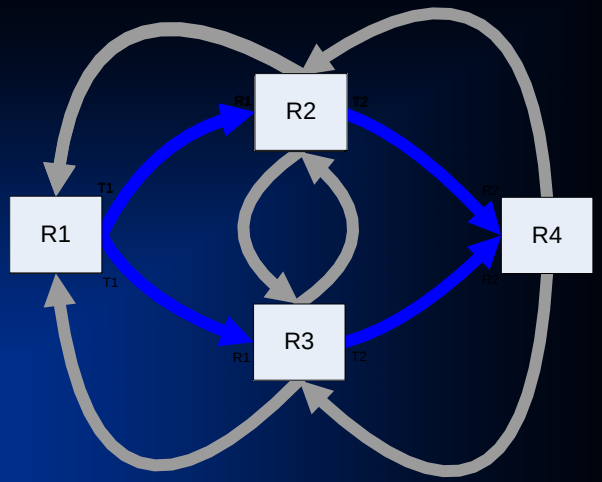
Range vs. Reach

Range
Distance from a single radio to another radio (point to point)

Voice: 40km
Data: 40km

Reach
Total communication distance in a multi-hop configuration; coverage

Voice: 40km x 9 = 360km
Data: 40km x 30 = 1,200km



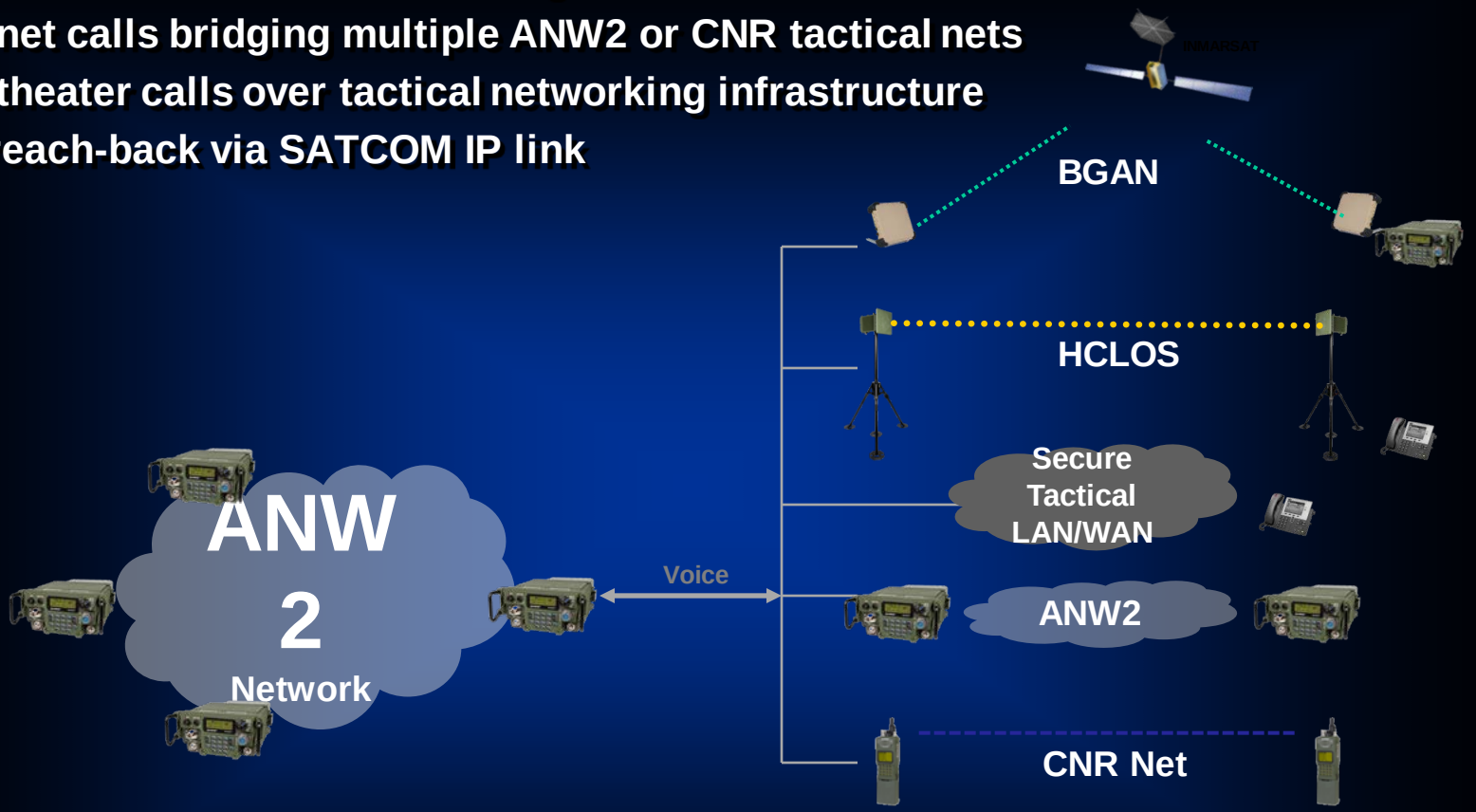
- **Avalanche Voice**
  - **Instantaneous 9-hop Voice Relaying**
  - **Combat Voice guaranteed**
- **All-Informed Data Network**
  - **30-hop Data Relaying**
  - **Ensures data transmission and GPS position reports**

Reach

ANW2 combines range plus advanced networking to extend the reach of voice and data communications

ANW2 Networked Voice Capabilities

- Guaranteed CNR voice within the ANW2 net
- Point-to-Point and broadcast calling within and outside of the ANW2 net
- Cross-net calls bridging multiple ANW2 or CNR tactical nets
- Cross-theater calls over tactical networking infrastructure
- Voice reach-back via SATCOM IP link

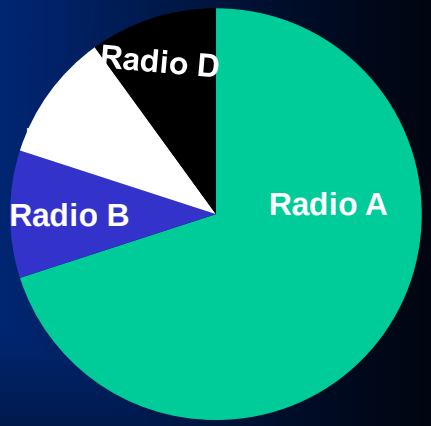


ANW2 dynamic routing and VoIP capabilities extend the reach of voice and data applications outside of the wireless wideband net

ANW2 Capabilities

- **High Performance Modems**
  - High-rate modulations support over the air rates up to 10 Mbps
  - Robust performance in varying channel conditions
  - Extended coverage area for high-speed services over previous generation capabilities

- **Dynamic Capacity Allocation (DCA)**
  - Sharing of unused data slots based on demand
  - Improved efficiency maximizes the use of available bandwidth
  - Network automatically adjusts to the application, allowing the soldier to take advantage of increased performance while focusing on the mission at hand
  - Significant increase in user throughput to maintain high-speed connectivity in larger-scale networks



DCA means data capacity on-demand

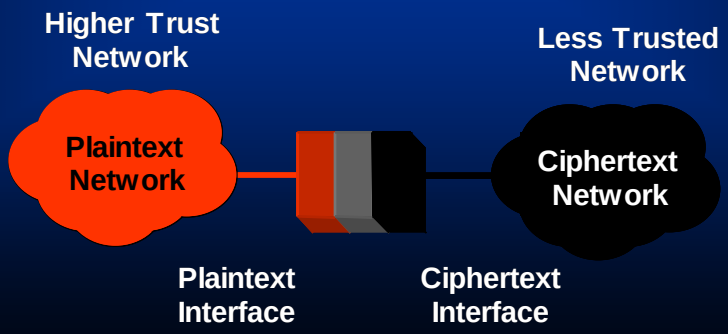
What is NINE?

Network and Information Infrastructure (NII) Internet Protocol Network Encryption (NINE)

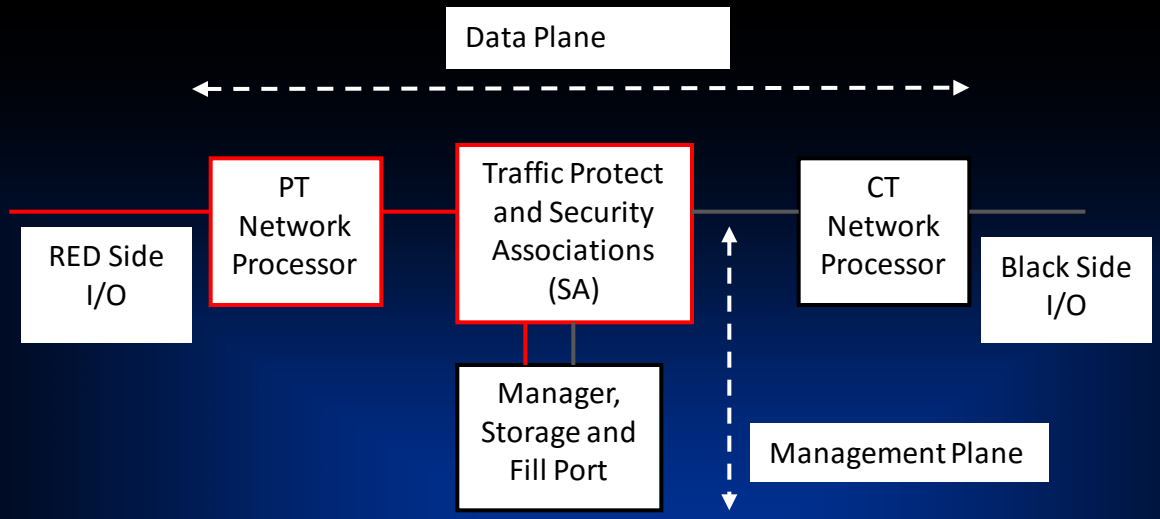
An Intellectual Property Rights (IPR) free NATO-wide Internet Protocol Network Encryption Interoperability Specification to be the basis of secure interoperable network communications for NATO, NATO Nations & Coalition Operations.

Network and Information Infrastructure (NII) Internet Protocol Network Encryption (NINE) Overview

- NINE compatible devices are programmable Internet Protocol (IP) information security devices that provide tunnel and transport traffic protection.
- NINE compatible devices have networking and management features that provide Information Assurance (IA) services when deployed in IPv4 and/or IPv6 networks.
- Network encryption provides confidentiality at the IP layer
- NINE specification defines Key Management and distribution capabilities
- The features and capabilities of NINE devices are defined in the NINE Interoperability Standard (IS), version 1.0.3, dated January 31, 2013



NINE Architecture



- The NINE architecture consists of data plane and a management plane.
- The data plane has network processors on the Plain Text and the Cipher Text inputs/ outputs.
- The management plane provides the guidance, interface and operational controls to establish controls, permissions, algorithm selections, and network operation.

Traffic Protection Features

- NINE traffic protection features provide confidentiality, integrity, and access control for user traffic.
- NINE IS specifies Type A and Type B (Suite B) traffic protection modes (crypto algorithms and authentication methods).
- For Type B, NINE specifies the following symmetric key material based modes”
  - Device Generated Secure Key (DGSK)
  - Authenticated Pre-Placed Keys [APPKs]
- Type B NINE also supports asymmetric key exchange using Elliptical Curve, Diffie Hellman (ECDH).
- NINE supports creation of manual or automatic Security Associations

Updated Suite B Guidance

- **Suite B - Set of Cryptographic Algorithms based on a set of strong commercial algorithms.**
- **NSA has updated Suite B algorithm set to better protect against the threat of quantum computing, as follows:**
  - Encryption/Confidentiality - Advanced Encryption Standard (AES) – specified in FIPS 197 (256 bits key size).
  - Digital Signature/Authentication – Elliptic Curve Digital Signature Algorithm (ECDSA) – specified in FIPS 186-3 (using the curves with 384 bit prime moduli).
  - Key Exchange – Elliptic Curve Diffie-Hellman (ECDH) – specified in Draft NIST Special Publication 800-56 (using 384 bit prime moduli).
  - Hashing – Secure Hash Algorithm (SHA) – specified in FIPS 180-2 (using SHA-384).

NINE Suite B Encryption Cryptography

Feature	Algorithm
Encryption Algorithm	AES
Data Integrity Algorithm	GCM-128
	GCM-96 (Default)
	GCM-32
	GCM-0
Hash Algorithm	SHA-384
Cryptographic Block Size	4 bytes
Authentication Method	Authenticated Pre-Placed Key (APPK)
Certificate Authentication	X.509v3 Certificate IA(M), ECDSA
Encapsulation Mode	ESPv3 Tunnel Mode
	ESPv3 Transport Mode
Asymmetric Key Exchange	ECDH

Security Association (SA) Properties

- The manual SA can be established by an administrator configuring the necessary information in each NINE device that will participate in the secure communications.
  - Manual SAs are the only choice for SAs running over simplex connections and for multicast architectures.
  - Manual SAs use Pre-Shared Key (PSK) (DGSK and PPK for Type A and DGSK and APPK for Type B).
  - PSKs are updated every day, using a key update algorithm.
  - A new PSK is used every month. PSKs can be chained such that 1 year's worth of key can be loaded and configured in a NINE at one time.
- The Automatic SA can be established using Internet Key Exchange version 2 (IKEv2).
  - IKEv2 allows NINEs to perform a key exchange using Shared Secrets or certificates for authentication.
  - Key agreements are achieved by use of the asymmetric Elliptical Curve, Diffie Hellman (ECDH) or negotiated symmetric Pre-Shared-Key (PSK).

Network Management Features

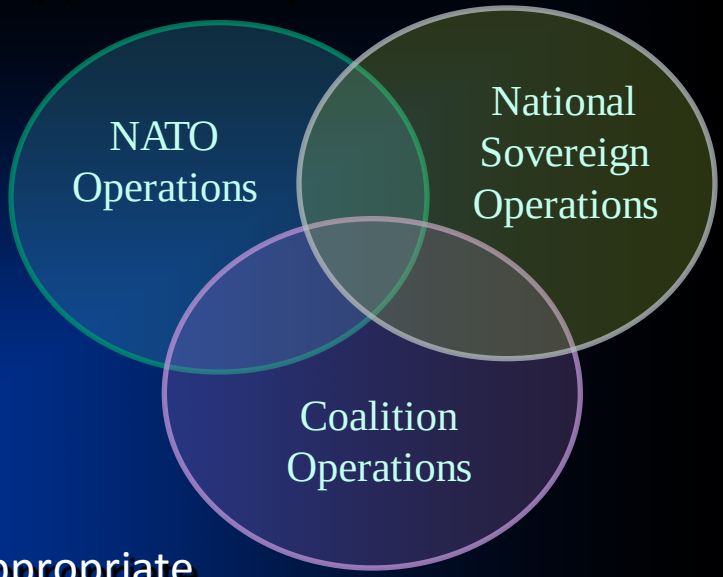
- NINE supports both local and remote network management
- Local control is provided through vendor specific terminal console
  - Example: Download of signed configuration file
- Remote Control is provided using Secure Network Management Protocol version 3 (SNMPv3)
  - SNMPv3 provides confidentiality, integrity and authentication of network management traffic at the application layer.
  - NINE specifies inclusion of the User Security Model (USM) and View-based Access Control Model (VACM) components of SNMPv3.
  - The NINE and the management workstation need to be configured with suitable SNMPv3 USM user names and passwords for confidentiality and authentication.
  - A NINE can be managed from either its PT or CT interface.

NINE Key Formats

Symmetric Key	Asymmetric Key
PPK, APPK and DGSK	ECDH
Identical keys loaded in all communicating NINE devices	Asymmetric pair-wise generated symmetric key that is unique for the individual IKEv2 pair. communicating NINE devices
Manual key assignment	Automatic assignment as a result of the Exchange
No key exchange protocol needed	IKEv2 used for key agreement
1 month crypto period (needs a new key each month)	Daily crypto period
Does not require point to point communication (operates on multicast and simplex links)	Requires point to point communication (Cannot do multicast)

NINE Network Operations

- The NINE standard can support many types of operations:
  - National Sovereign Operations
  - NATO Operations
  - Coalition Operations
    - NATO Sanctioned
    - Multi-lateral (usually a lead nation)
    - EU &/or UN Sanctioned
  - Training Activities



- Trust Management
  - NINE supports trust management to insure only appropriate entities have key generation and distribution capabilities.
  - For NATO & NATO-led Coalition Operations, NINE devices should rely on common High Assurance NATO PKI Trust Anchor based KM.
  - Sovereign Nations and Non-NATO coalitions need the ability to generate and load key material into NINE ECU devices. Unique PKI Trust Anchors will be required for those applications.

Trust Establishment

HARRIS

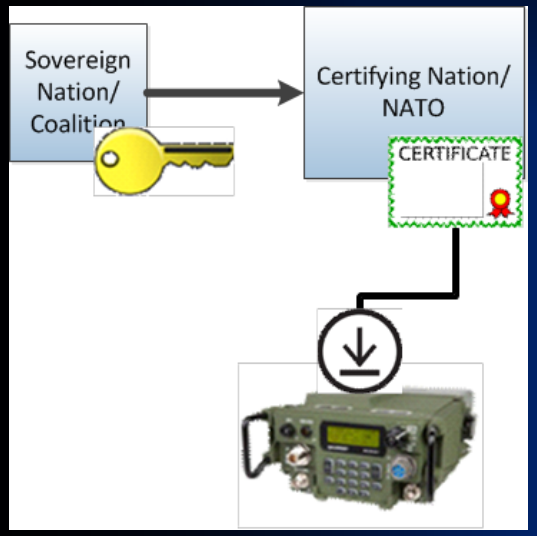
- Controlling authority must be identified for each Community of Interest (CoI).
  - Controlling authority maintains control over who is authorized to generate key material and the time period for which they are authorized
  - Allow Trust Establishment decisions to be made on a nation by nation basis rather than an ECU by ECU basis
- PKI Certificates are used to validate asymmetric PKCs and symmetric Authenticated Pre-Placed Keys (APPK) for the following use cases:
  - NATO - operations in which NATO is providing the key material.
  - Sovereign - Sovereign nation operations and training exercises.
  - Coalition - operations that may include nations outside of NATO. NATO or a lead nation provides key material.
  - Vendor Test - Training exercises for nations that do not have key generation capabilities. Only supports unclassified key material.

NINE IS Symmetric Key Management Approach Authenticated Pre-Placed Key (APPK)

- NINE IS requires use of Authenticated Pre-Placed Key (APPK) for Suite B
  - Authenticated Pre-Placed Keys signed by pre-defined private key component of the specific CoI Trust Anchors
    - NATO/DACAN
    - Coalition
    - Sovereign Nation
  - Standardized APPK format and validation requirements
- APPK Trust Anchors for different Communities of Interest
  - NATO: NATO, NATO Nation, Coalition
  - USA: USA, CCEB, NATO, NATO Nation, CHVP, High Risk, Coalition
  - Generic NATO/EU Nation: Sovereign, NATO, EU, Coalition, Other?
- Coalitions are keyed by a lead organization or a lead nation (NATO, UN, USA, UK, FRA, etc.)

APPK Trust Management Example

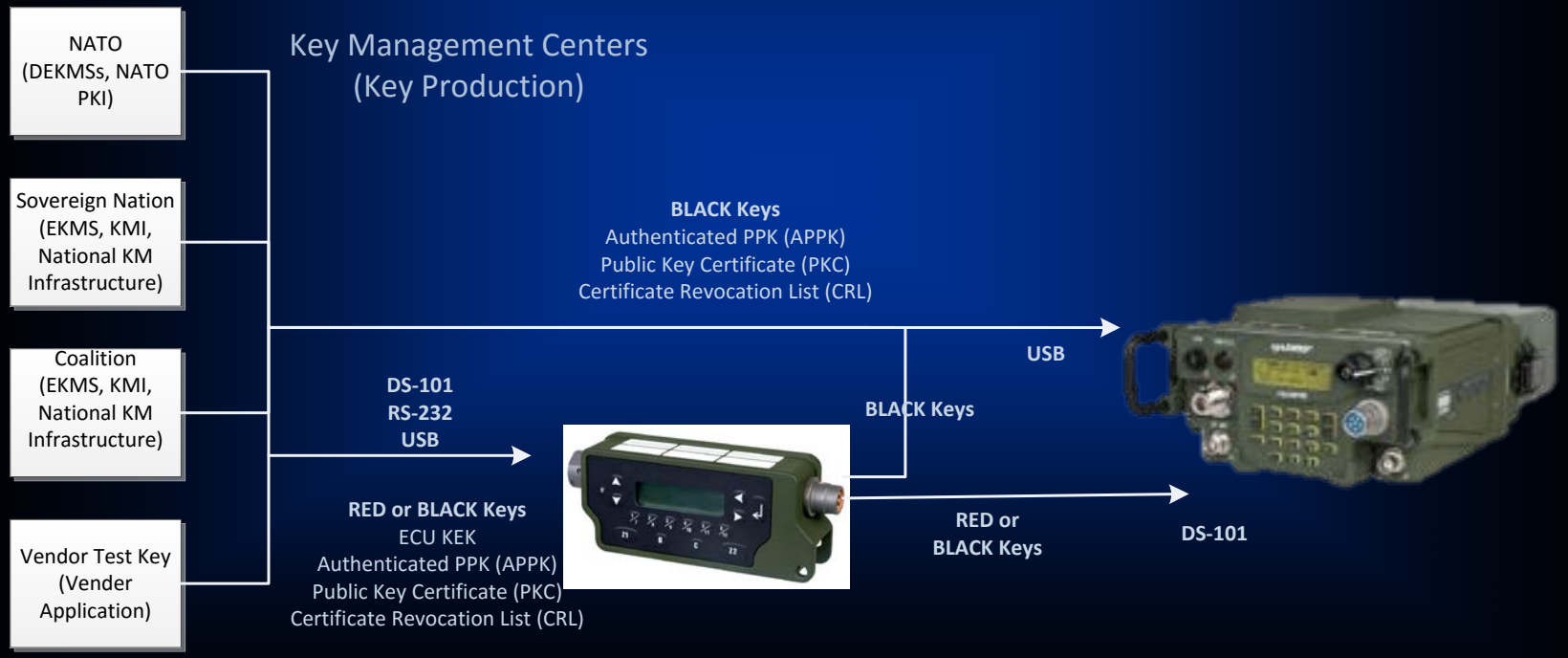
1. NINE compatible radio supports Authenticated Pre Placed Keys



2. DACAN (NATO CoI) or Sovereign nation produces public / private key pair.
3. Certifying nation/NATO authorizes APPK capability and generates a signed APPK trust anchor (based on public key provided by sovereign nation or coalition)
4. Signed APPK Trust Anchor is loaded and authenticated against the existing Trust Source (Trust Anchor of Certifying nation or NATO).
5. Radio will now accept APPKs generated and signed by sovereign nation or coalition.

APPK Generation and Loading Example

- Key material (APPK, PKC, etc.) is generated and signed by authorized source (Sovereign nation or NATO DACAN)
- Key material is loaded to the radio
- Radio accepts the keys after authenticating it against the appropriate CoI (NATO DACAN, Coalition, Sovereign Nation) Trust Anchor



Conclusions

- Multinational coalitions require secure, interoperable tactical radio communications solutions in order to meet mission requirements.
- Defining an SCA compliant waveform that can be ported to a variety of tactical radio platforms is the most effective way to enable tactical radio coalition interoperability.
- ANW2 is a high performance, robust and flexible tactical networking waveform that can accommodate a variety of the required operational use cases.
- ANW2 can be easily integrated with NINE to provide an standard SCA waveform to help facilitate wideband networking tactical coalition interoperability.

Contact Information

Igor A. (Tony) Spivak

Senior Systems Engineer

Harris Corporation
Communications Systems
1680 University Ave.
Rochester, New York 14610

Telephone: (585) 242-3034
ispivak@harris.com