



Finnish Defence Research Agency

Armed Forces' views on shared spectrum access

11.10.2016

WinnComm-Europe 2016

Gennevilliers

France

Research Manager
Commander (GS) Topi Tuukkanen
Finnish Defence Research Agency
Information Technology Division

tel: +358 299 550 830
email: topi.tuukkanen@mil.fi

This work has been partially supported by the Finnish Funding Agency for Innovation's CORE++ project in collaboration with Nokia, VTT Technical Research Center of Finland and University of Oulu



Puolustusvoimat

Försvarsmakten • The Finnish Defence Forces



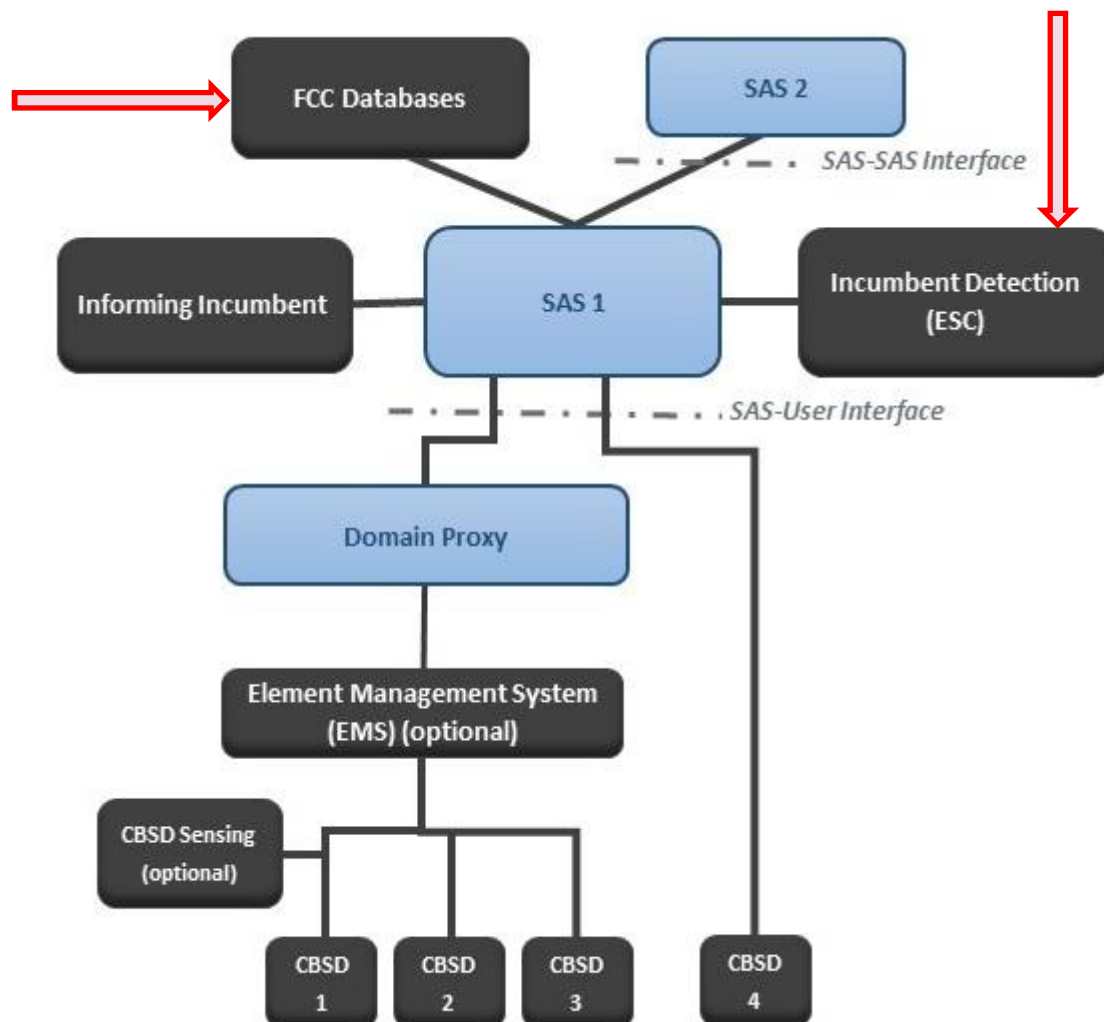
Contents

1. Introduction to shared spectrum access
 - SAS
 - LSA
 - 5G
 - Option space
2. Army Digital Battlefield
 - Scenarios
3. Use cases
4. Observations





SAS Functional Architecture



Acronyms:

ESC: Environmental Sensing Capability
CBSD: Citizens Broadband Radio Service Device
SAS: Spectrum Access System

Notes:

- A SAS may not need to support all interfaces
- Each CBSD domain may optionally include some sensing capability (including possibly an ESC).

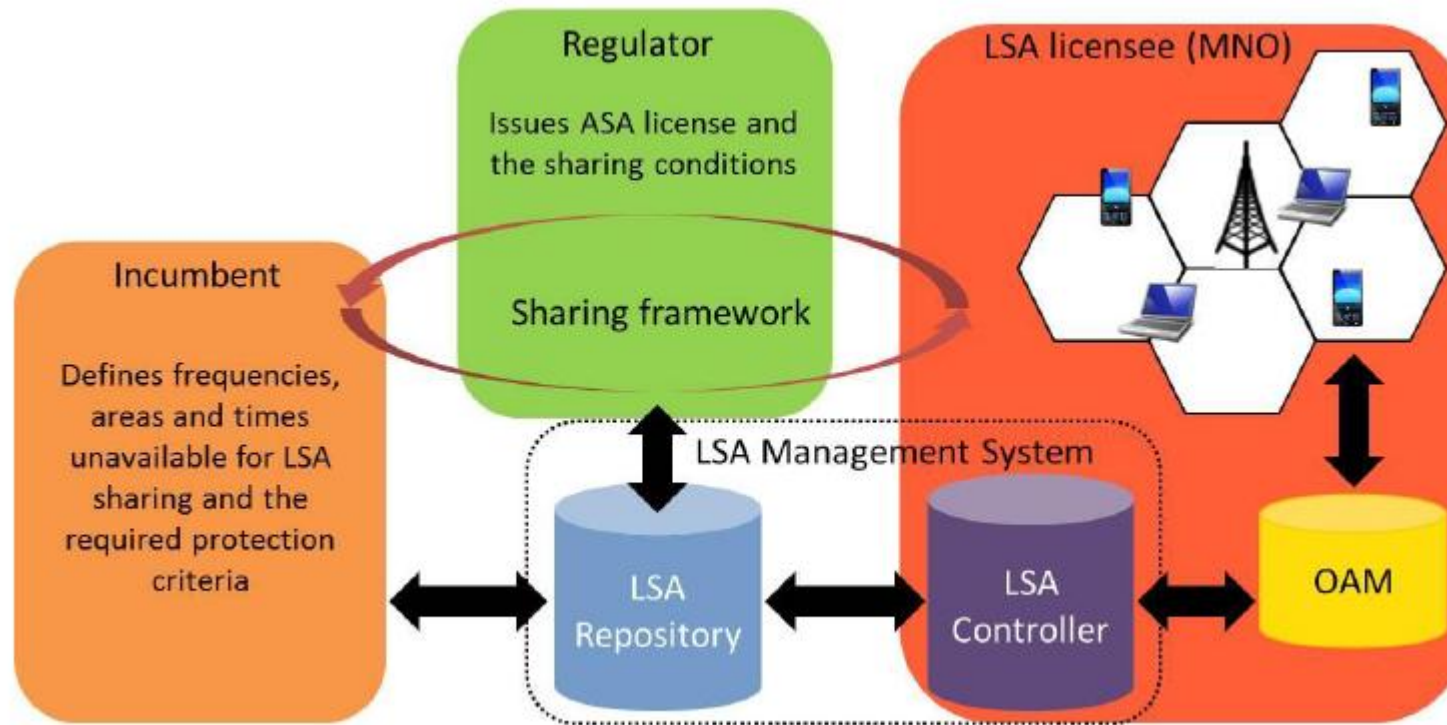
Wireless Innovation Forum, "SAS Functional Architecture", Document WINNF-15-P-0047 Version V1.0.0, 7 September 2015



CDR Topi Tuukkanen
Research manager
Information Technology Division



Overview of LSA architecture

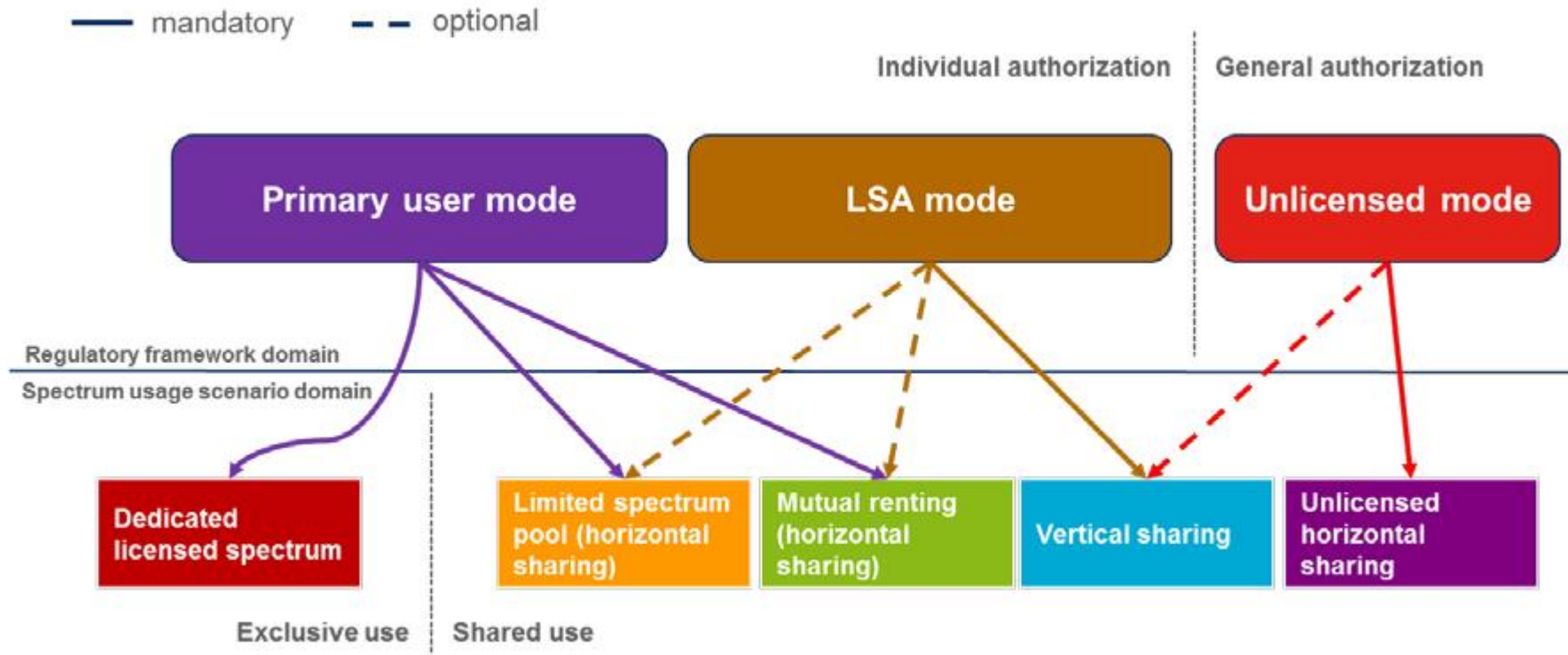


Mustonen, Miia, et al. "Considerations on the licensed shared access (LSA) architecture from the incumbent perspective." *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*. IEEE, 2014.





Example of regulatory frameworks in various spectrum usage scenarios for 5G above 6GHz



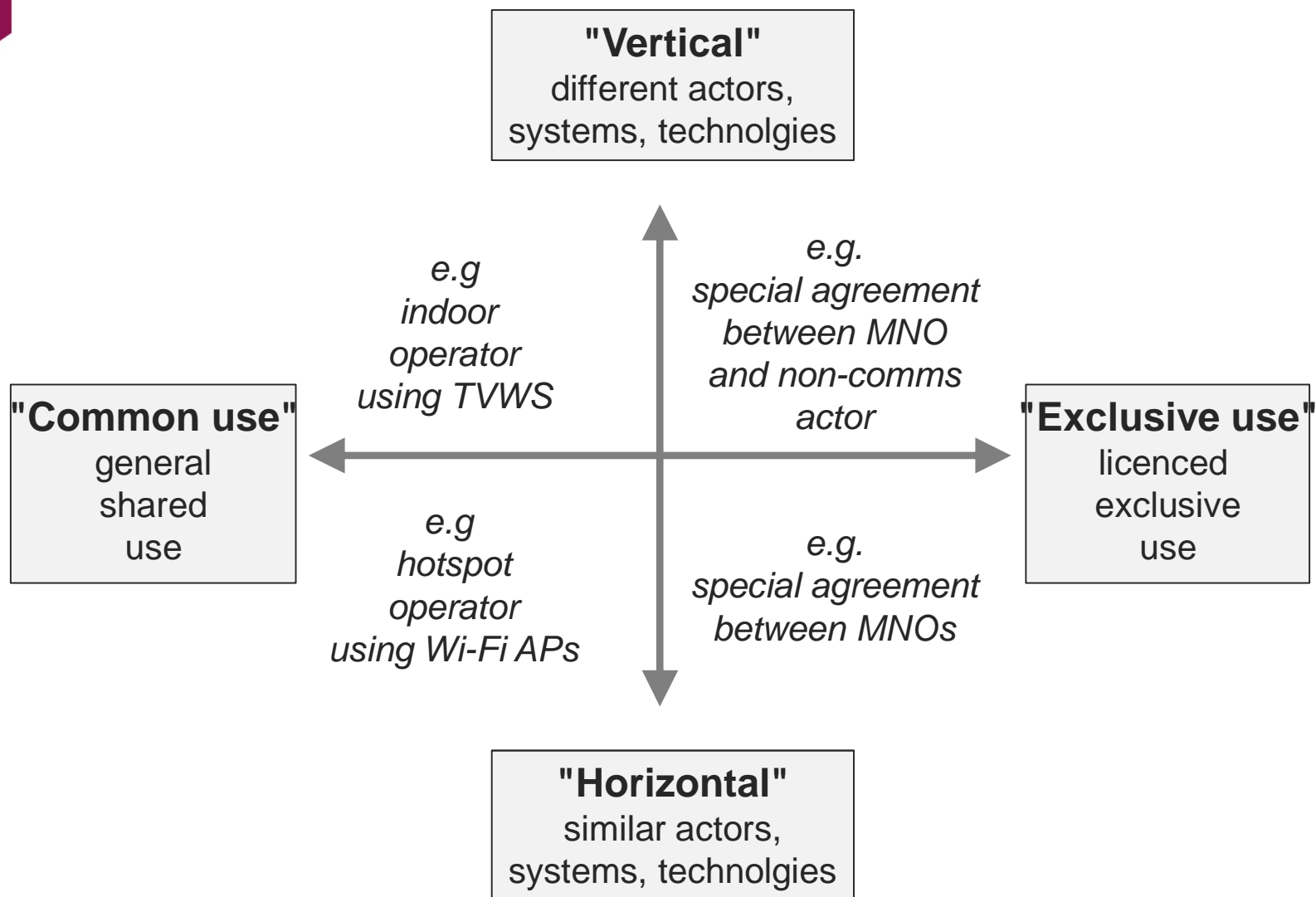
Mobile and Wireless communications Enablers for the Twenty-twenty Information Society II (METIS II), "Deliverable D3.1 5G spectrum scenarios, requirements and technical aspects above 6GHz", [Online], <http://www.5g-ppp.eu>



CDR Topi Tuukkanen
Research manager
Information Technology Division



SPECTRUM ACCESS OPTION SPACE



Ahmed, Ashraf Awadelkarim Widaa, and Jan Markendahl. "Impact of the flexible spectrum aggregation schemes on the cost of future mobile network." *Telecommunications (ICT), 2015 22nd International Conference on*. IEEE, 2015.





ARMY DIGITAL BATTLEFIELD

Our focus on national defence scenarios:

- spectrum regulatory regime's are national
- Shared access in multinational environment and especially in expeditionary environments remains unresolved

Comprises of elements, systems and interactions of and between:

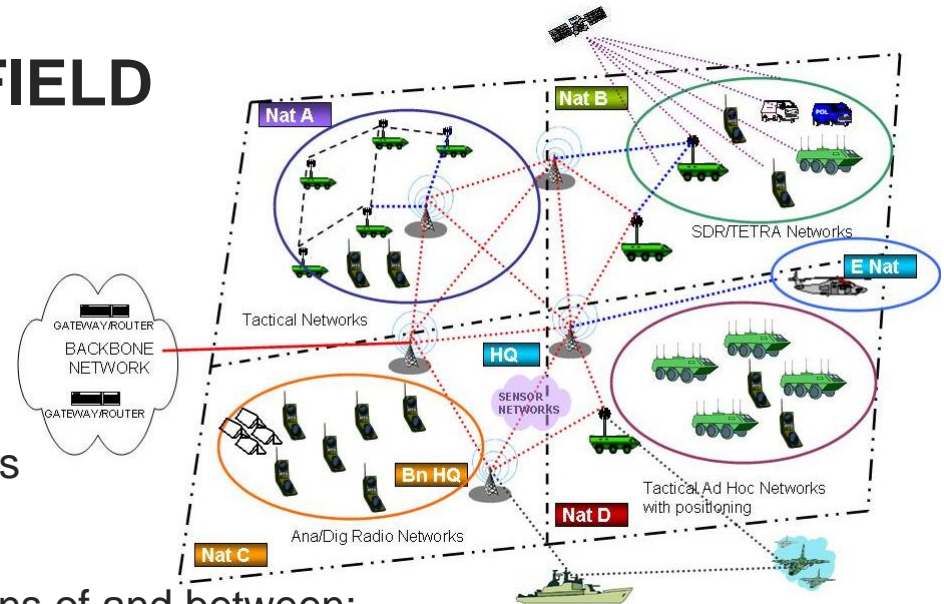
- real-time communications platform plus
- integrated sensor-, weapons-, FFT-, C4ISR

that ALL use spectrum to

- transmit or obtain information
- monitor and observe environment

Examples of army spectral use: Friendly Force Tracking, positioning services (SAT or national/tactical), counter-artillery radar, anti-air defence systems (radar, missile), anti-armour systems, C-IED, tactical communications (soldier mounted, vehicle mounted), battalion/brigade communications networks, radio relays

Source: Kosola J, Solante T, "Digital Battlefield", Finnish National Defence University, Series 1 n:o 13, 2003





SCENARIOS 1/3



1. Normal times (peace) - homeland defence

- armed forces train and exercise in garrisons and regular exercise areas
- some large scale exercises (national, coalition) may take place every now and then, even outside normal exercise areas

⇒ peace time/exercise spectral occupancy measurements shall **not** yield reliable results
⇒ peace time requirements are modest compared to full war time strength
⇒ national/military spectrum administrations "manual" planning processes capable of addressing needs
(cf. e.g. NATO STO-TR-IST-077 Cognitive Radio in NATO, 2014)

2. Normal times (peace) - large scale accident / catastrophe

- regardless of national preparedness efforts, exact time and location unplanned for
- highly dynamic, high demand for real-time information, confused leadership roles and assignments, participant and actors unaware of each other and most probably unable to communicate and exchange information between each other
- from technical viewpoint on shared spectrum access this scenario resembles those of large scale military exercises (especially involving multinational units)





SCENARIOS 2/3

3. Rapidly developing international conflict

- number of spectrum users, including those unauthorized and hostile, significantly more numerous than in previous scenarios.
- some spectral congestion may occur when defender and hostile units converge
- limited hostile electronic warfare e.g. jamming may take place in support of enemy action
- due to low preparedness and enemy surprise defender units may become isolated pockets with relatively high concentrations of subscriber devices
- these pockets and enemy units in-between may operate in urban environment with large numbers of civilian population



- ⇒ depending on the time scale of the conflict eruption military and/or civilian authorities may not yet have emergency legal statutes or legal authority to change spectrum regulations or allocations as of today
- ⇒ future shared spectrum access methods and regulations may facilitate national spectrum regulatory authorities and governmental authorities including military to dynamically adjust spectrum regulations and allocations
- ⇒ for military shared spectrum access seriously challenged by the need of civilian emergency authorities that have a need to operate among urban population left in the area





SCENARIOS 3/3

3. Homeland defence (large scale - slow development)

- population evacuations from anticipated battle zones
- military spectral needs increase dramatically
- legal statutes available for authorities to adjust spectral use and allocations



- ⇒ for military little or no incentives to endorse unfavorable shared spectrum access frameworks or agreements
- ⇒ military would greatly benefit from military internal / government internal dynamic spectrum access methods





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	MIL	GOV	MNO	Current regulatory framework does not consider other alternatives
LSA1	MIL	MIL	-	Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2	MIL	GOV	-	
LSA3	MIL	MNO	-	
LSA4	GOV	GOV	-	Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA5	GOV	MIL	-	
LSA6	GOV	MNO	-	Beyond scope of this article
LSA7	MNO	MNO	-	Beyond scope of this article
LSA8	MNO	MIL	-	
LSA9	MNO	GOV	-	Beyond scope of this article





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	MIL	GOV	MNO	Current regulatory framework does not consider other alternatives
LSA1	SAS: Appropriate for military requirements in all scenarios, preferable over LSA			Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2	MIL	GOV	-	
LSA3	MIL	MNO	-	
LSA4	GOV	GOV	-	Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA5	GOV	MIL	-	
LSA6	GOV	MNO	-	Beyond scope of this article
LSA7	MNO	MNO	-	Beyond scope of this article
LSA8	MNO	MIL	-	
LSA9	MNO	GOV	-	Beyond scope of this article





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	MIL	GOV	MNO	Current regulatory framework does not consider other alternatives

LSA1	MIL	MIL	-	Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2	<div>LSA1: MIL-MIL shared access not in LSA-standards but military internal / military specific <u>dynamic spectrum access</u> worth investigation especially in large scale military counter-attack or joint operations scenarios</div>			
LSA3				
LSA4				Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA5	GOV	MIL	-	
LSA6	GOV	MNO	-	Beyond scope of this article
LSA7	MNO	MNO	-	Beyond scope of this article
LSA8	MNO	MIL	-	
LSA9	MNO	GOV	-	Beyond scope of this article





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	MIL	GOV	MNO	Current regulatory framework does not consider other alternatives
LSA1	MIL	MIL	-	Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2	MIL	GOV	-	Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA3	MIL	MNO	-	
LSA4	MIL	GOV	-	
LSA5	MIL	MNO	-	
LSA6	MIL	MNO	-	Beyond scope of this article
LSA7	MIL	MNO	-	Beyond scope of this article
LSA8	MIL	MNO	-	Beyond scope of this article
LSA9	MNO	GOV	-	Beyond scope of this article

LSA2: Relevant use case when governmental emergency services (first responders) would have the need to augment their own already existing pool of channels/spectrum. Scenario may have limited applicability also to military spectrum used for national territorial surveillance.





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	MIL	GOV	MNO	Current regulatory framework does not consider other alternatives
LSA1	MIL	MIL	-	Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2	MIL	GOV	-	
LSA3	MIL	MNO	-	
LSA4	<div>LSA3: Relevant use case when Mobile Network Operators would have the need to augment their own already existing pool of channels/spectrum. Could be used as a positive starting point for negotiations between military and national spectrum regulatory authorities.</div>			Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA5				
LSA6				Beyond scope of this article
LSA7				Beyond scope of this article
LSA8				
LSA9				Beyond scope of this article

CDR Topi Tuukkanen
Research manager
Information Technology Division





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	MIL	GOV	MNO	Current regulatory framework does not consider other alternatives

LSA1				Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2				
LSA3	MIL	MNO	-	
LSA4	GOV	GOV	-	Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA5	GOV	MIL	-	
LSA6	GOV	MNO	-	Beyond scope of this article
LSA7	MNO	MNO	-	Beyond scope of this article
LSA8	MNO	MIL	-	
LSA9	MNO	GOV	-	Beyond scope of this article

LSA4: Not in LSA-standards but authorities/emergency services internal dynamic spectrum access worth investigation especially for large scale national disaster recovery scenarios





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	<p>LSA5: Theoretically possible when government/emergency services have already existing pool of channels/spectrum beyond regular/normal needs and MIL has requirement to augment already existing MIL pool of channels/spectrum. Potentially applicable for home front / military rear support element usage. Legislation/regulation/agreement - framework should include provisions to dynamically adjust this arrangement to MIL (PU) - GOV (SU).</p>			Current regulatory framework does not consider other alternatives
LSA1				Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2				
LSA3				
LSA4				Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA5	GOV	MIL	-	
LSA6	GOV	MNO	-	Beyond scope of this article
LSA7	MNO	MNO	-	Beyond scope of this article
LSA8	MNO	MIL	-	
LSA9	MNO	GOV	-	Beyond scope of this article





USE CASES OF SHARED ACCESS

USE CASE	PRIMARY USER	SECONDARY USER	GENERAL USE	Remarks
SAS	<p>LSA8: Theoretically possible when Mobile Network Operators have already existing pool of channels/spectrum beyond regular/normal needs and MIL has requirement to augment already existing MIL pool of channels/spectrum. Potentially applicable for home front / military rear support element usage. Legislation/regulation/agreement - framework should include provisions to dynamically adjust this arrangement to MIL (PU) - MNO (SU).</p>			Current regulatory framework does not consider other alternatives
LSA1				Not according to planned standardisation, implies organization internal shared access e.g. among army and air force radar spectrum
LSA2				
LSA3				
LSA4				Not according to planned standardisation, implies organization internal shared access e.g. among Coast Guard and Board of Navigation
LSA5		MIL	-	
LSA6	GOV	MNO	-	Beyond scope of this article
LSA7	MNO	MNO	-	Beyond scope of this article
LSA8	MNO	MIL	-	
LSA9	MNO	GOV	-	Beyond scope of this article



SOME OBSERVATIONS

- SAS/LSA based on premise that both PU/SU have basic pools of channels/spectrum already available, SAS/LSA thus augment SUs base services
- SAS/LSA have intelligence in networks to keep end-user devices simple and affordable. No requirement for end-user device spectrum monitoring. If connection to the network controller/spectrum database is lost, shared parts of spectrum are to be avoided.
- For military, SAS preferable over LSA
- Neither is adequate for military as principal architecture / only solution.
- Nevertheless, shared access technologies and solutions may have potential applications for military
- Organization internal (MIL-MIL or GOV-GOV) dynamic spectrum access should be investigated in more detail
- LSA sharing framework standardization should be augmented with provisions for situation dependent, geographically and temporally dynamic adjustments among agreement partners.
- These observations are valid for homeland defence (allied or non-aligned). However, worldview behind armed force's tasks (e.g. emphasis on expeditionary coalition operations) may have impact on R&D priorities and willingness to assign military R&D funding to this area.



CDR Topi Tuukkanen
Research manager
Information Technology Division

