TETRA Algorithm Transition

TCCA Critical Updates Webinar Series, 20 Nov 2026

Advancing global critical communications for a safer, more connected world

Speakers



Dave Chater-Lea
Chairman TCCA SFPG
TCCA



Harald Ludwig
Technical Forum Chair
TCCA



Steen Petersen
Principal Advisor
Danish Center of Emergency Communication (CFB)



Clive Rodmell
Senior Specialist
Sepura

Agenda

1. Introduction – Harald
2. TETRA Standard Algorithms – Dave
3. Decision Criteria – Steen
4. Products Availability & Interoperability – Harald
5. Transition Process – Clive
6. Questions & Answers – All

TETRA Algorithm Transition

TETRA Standard Algorithms

Dave Chater-Lea
Chairman TCCA SFPG
TCCA

TETRA Air Interface Security

- **Intention of Air Interface security:**
  - To make the air interface as difficult to attack as the fixed network (or even more difficult)
  - To withstand a well-resourced attacker, but not necessarily one with nation state capabilities – further measures such as end-to-end encryption can be overlaid if this is a consideration
- **What does it provide?**
  - Confidentiality – by means of standardised air interface encryption algorithms
  - Protection against fraud and misuse – by means of standarised authentication algorithms and mechanisms (explicit and implicit)
  - Encryption management – by standardised key management algorithms
  - Further secure management functions – secure enable/disable, HW & SW version number management

TETRA Standard Air Interface Algorithms

- **Original algorithm set (late 1990s):**
  - Authentication and key management: TAA1 set
  - Air interface encryption: TEA Set A – TEA1, TEA2, TEA3 and TEA4
  - TEA2 reserved for PPDR use in Europe (PPDR = Public Protection and Disaster Relief)
- **Additional algorithm set (2020s):**
  - Authentication and key management: TAA2 set
  - Air interface encryption: TEA Set B – TEA5, TEA6 and TEA7
  - TEA5 reserved for PPDR use in Europe
- **Algorithm ownership: ETSI**
- **Algorithm custodianship**
  - TAA1, TAA2, TEA1, TEA3, TEA4, TEA6, TEA7: ETSI
  - TEA2, TEA5: TCCA
  - TEA2 and TEA5 require a licence to manufacture, sell, buy, install, repair, dispose of etc
  - No equivalent licensing scheme needed for TEA1, TEA3, TEA4, TEA6, TEA7

Why an additional algorithm set?

- **Cost of computing: every year, the cost of hardware needed to mount a brute force attack on an algorithm by trying every key in turn reduces**
  - What cost tens of millions in the 1990s may only cost tens of thousands today
- **Increased threat from cryptographically relevant quantum computers, when these become feasible**
  - TETRA algorithms are not vulnerable to specific properties of quantum attacks such as factorisation
  - However, a quantum computer can still make a faster brute force attack on a conventional algorithm

➡ **Longer key lengths of the additional algorithm sets makes an attack much harder/more expensive**

  - Authentication key K (TAA1): 128 bits; key K2 (TAA2): 256 bits
  - AI Encryption keys xCK (TEA set A): 80 bits*; xCKX (TEA set B): 192 bits*

- **Security improvements, such as the MAC Address Encryption (MAE) replacement identity encryption system**

* Note that TEA1, TEA4, TEA7 have some key entropy reduction for cases where export restrictions would otherwise apply

Does this affect End-to-End Encryption?

- No – End-to-End Encryption (E2EE) is completely independent of air interface encryption
- Most E2EE applications use algorithms with longer keys already (e.g. AES128 or AES256)
- National Security agencies should periodically assess the algorithms that they use and determine whether there are any needs for change

TETRA Algorithm Transition

Decision Criteria

Steen Petersen
Principal Advisor
Danish Center of Emergency Communication (CFB)

New TEA algorithm – decision criteria

- **Why is this relevant?**
  - NIS2
  - ISO 27001
- **Do I need to change to a new algorithm?**
  - Risk assessments
- **Which algorithm should I select?**

NIS2

- **Article 21(2), point (a) of Directive (EU) 2022/2555 (NIS2):**
  - Policies on risk analysis and information system security
- **Article 21(2), point (h) of Directive (EU) 2022/2555 (NIS2):**
  - Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- **If you are covered by NIS2 then you have to perform risk assessments to identify and address the risks posed to the security of network and information systems**

ISO 27001

- **In ISO 27001 risk assessments are used to identify relevant controls**
- **When considering risks associated with confidentiality (and integrity) then this control will likely be relevant:**
  - ISO 27002: 8.24 Use of cryptography
  - Purpose: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements.

Risk Assessment – 1

- **Use your risk management framework/process in relation to encryption**
- **Policies and procedures covering encryption need to be risk assessed**
- **Risk assessments are not static – they need to be re-assessed at regular intervals!**
- **ISO 27002: 8.24 Use of cryptography – Guidance:**
  - (b) Identifying the required level of protection and the classification of the information and consequently establishing the type, strength and quality of the cryptographic algorithms required;

Risk Assessment – 2

- **Factors to consider in risk assessments:**
  - Are the encryption algorithms strong enough compared to the consequence of breach
  - Does the advances in quantum computing change the risk?
  - Is there a risk associated with the “Harvest now, decrypt later” surveillance strategy?
  - Does the time to change the implementation to a new encryption algorithm impact the risk?

Which algorithm to select?

TETRA Air Interface Encryption algorithms:

TEA set A	TEA set B
TEA 1	TEA 7
TEA 2	TEA 5
TEA 3	TEA 6
TEA 4	TEA 7

Consider the new (TEA set B) algorithm corresponding to your current algorithm

In all cases consult your SwMI and MS supplier regarding availability

TETRA Algorithm Transition

Products Availability & Interoperability

Harald Ludwig
Technical Forum Chair
TCCA

Products Supporting Set B
TETRA Infrastructure Systems (SwMIs)

Vendor	*Type*	*Product/Model/Version*	*TAA2*	*TEA5*	*TEA6*	*TEA7*	*Product launch*	*IOP Tests*
TETRA Infrastructure Products								
Damm	SwMI	BS422-S (TF ver. 9.x)	✓	✓	✓	✓		2027
Damm	SwMI	BS422-H (TF ver. 9.x)	✓	✓	✓	✓		2027
Damm	SwMI	BS424 (TF ver. 9.x)	✓	✓	✓	✓		2027
Etelm	SwMI	NetisN / NetisB25		✓				
HMF	SwMI	DIB-R5 (PV 11.80)	✓	✓	✓	✓		2027
HMF	SwMI	DIB-R6 (PV 11.80)	✓	✓	✓	✓		2027
Rohill	SwMI	TetraNode (TMC 2.44)	✓	✓	✓	✓		2027
Teltronic	SwMI	NEBULA	✓			✓		2026
TETRA Infrastructure Products (Roadmap)								
Etelm	SwMI	NetisN / NetisB25	✓		✓	✓		
Leonardo	SwMI		✓	✓	✓	✓		
Motorola	SwMI	DIMETRA	✓	✓	✓	✓		2028
Teltronic	SwMI	NEBULA	✓	✓	✓	✓	2027	

Please note that not all manufacturers have responded to the survey

Products Supporting Set B
TETRA Radio Terminals (MSs)

Vendor	Type	Product/Model/Version	TAA2	TEA5	TEA6	TEA7	Product launch	IOP Tests
TETRA Radio Terminal Products								
HMF	MS	MT690	✓	✓	✓	✓		2027
HMF	MS	PT590	✓	✓	✓	✓		2027
Hytera	MS	PT590 (V2.1)	✓		✓	✓		2026
Hytera	MS	PT890Ex (V2.1)	✓		✓	✓		2026
Hytera	MS	PTC680 (V4.0)	✓		✓	✓		2026
Hytera	MS	New Mobile	✓		✓	✓		2026
Sepura	MS	SC20	✓	✓	✓	✓		2027
Sepura	MS	SC21	✓	✓	✓	✓		2027
Sepura	MS	SC23	✓	✓	✓	✓		2027
Sepura	MS	SCG22	✓	✓	✓	✓		2027
Sepura	MS	SCL3 (SC28)	✓	✓	✓	✓		2027
Sepura	MS	SCU3 (SC27)	✓	✓	✓	✓		2027
Teltronic	MS	MDT-400	✓			✓		2026
Teltronic	MS	EHT-200	✓			✓		2026

Please note that not all manufacturers have responded to the survey

Products Supporting Set B
TETRA Radio Terminals (MSs) - Roadmap

Vendor	*Type*	*Product/Model/Version*	*TAA2*	*TEA5*	*TEA6*	*TEA7*	*Product launch*	*IOP Tests*
TETRA Radio Terminal Products (Roadmap)								
Leonardo	MS	*Handheld terminal*	✓	✓	✓	✓		
Leonardo	MS	*Vehicular terminal*	✓	✓	✓	✓		
Motorola	MS	MXM600	✓	✓	✓	✓		2027
Motorola	MS	MXP660	✓	✓	✓	✓		2027
Motorola	MS	*TBD*	✓	✓	✓	✓		
Motorola	MS	*TBD*	✓	✓	✓	✓		
Teltronic	MS	MDT-400	✓	✓	✓	✓	2027	
Teltronic	MS	EHT-200	✓	✓	✓	✓	2027	
Vendor A	MS	*TBD*		✓		✓		

Please note that not all manufacturers have responded to the survey

TETRA Algorithm Transition

Transition Process

Clive Rodmell
Senior Specialist
Sepura

Transition process overview

1: Plan and validate

- Check inventory and vendor offerings
- Devise strategy and schedule
- Perform small-scale trial

2: Prepare and deploy

- Procurement
- User awareness and training
- Roll-out

3: Change-over

- Authentication change-over
- Encryption change-over
- Identity encryption change-over

Check inventory and encryption scope

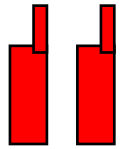


Network (SwMI)



- Hardware versions
- Software versions
- Tool versions

Terminals (MSs)



- Vendor(s) and models
- Hardware versions
- Software versions
- Tool versions

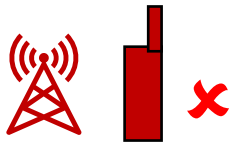
Air Interface Encryption: which aspects are relevant?

- Class 2?
- Class 3?
- Class 3G?
- Air Interface Migration?
- Direct Mode?

Check SwMI & MS vendor offerings



Is TEA Set B supported?
When will it be available?
Does it cover the relevant Air Interface aspects for my network?



Does any older hardware need to be replaced to support TEA Set B?



Do the vendors have TEA Set B IOP certification for my terminals on my network?

See SFPG Rec 17 sections 4.1.3, 4.2.3

Have the vendors tested additional capabilities relevant to transition for my network?

See SFPG Rec 17 sections 4.1.4, 4.2.4

Check SwMI & MS capabilities

SwMI

- Both K & K2 authentication keys
- Both TAA1 & TAA2 algorithm sets
- Both TEA Set A & TEA Set B algorithms
- TEA Set A with K2 authentication key
- DMO SCK/SCKX via OTAR
- Parallel TEA Set A & TEA Set B groups

MS

- Both K & K2 authentication keys
- Both TAA1 & TAA2 algorithm sets
- Both TEA Set A & TEA Set B algorithms
- TEA Set A with K2 authentication key
- DMO SCK/SCKX via OTAR or key loading
- In-field updates

Supporting more of these capabilities may provide more security and more flexibility over sequence, timing and locations of roll-out and change-over

Transition strategy decisions

Transition users in phases? (typically for large network)
Transition users all at once? (typically for small network)

Maintain confidentiality for all users during transition? Allow period of operation in clear during transition?

Change to K2 authentication and/or TEA Set B encryption as each MS is provisioned or delay until all provisioned?

Can Class 3 (or Class 2) AIE be maintained during transition?

- SwMI and MSs support both authentication keys K and K2
- SwMI and MSs support both an algorithm from Set A and an algorithm from Set B

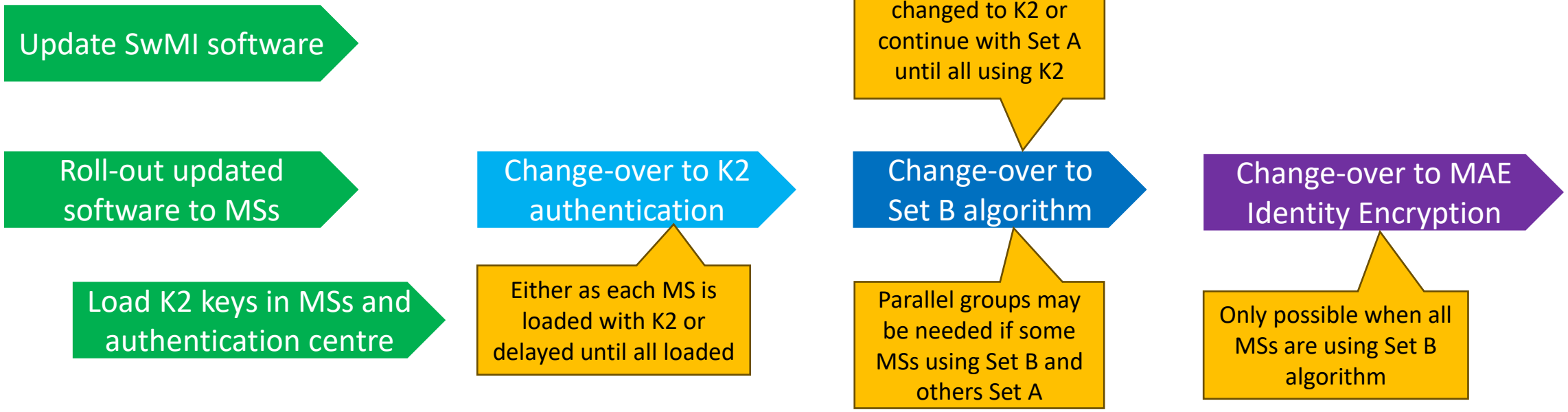
See ETSI TS 100 392-7 Annex D Table D.1 for details and for alternative scenarios if MS or SwMI doesn't support both

Group call downlink can only be encrypted with one algorithm and one key

Managing groups during transition:

- Parallel Set A & Set B groups?
  - Increases network load
  - User intervention required
- Temporarily operate affected groups in clear?

Devise a transition schedule



Small-scale trial: environment & tools

Test network trial

- Trial first on a test network if available
- Use a few test MSs, not user MSs
- Using dummy key material may simplify testing and diagnostics
- Also trial Set B in DMO if required

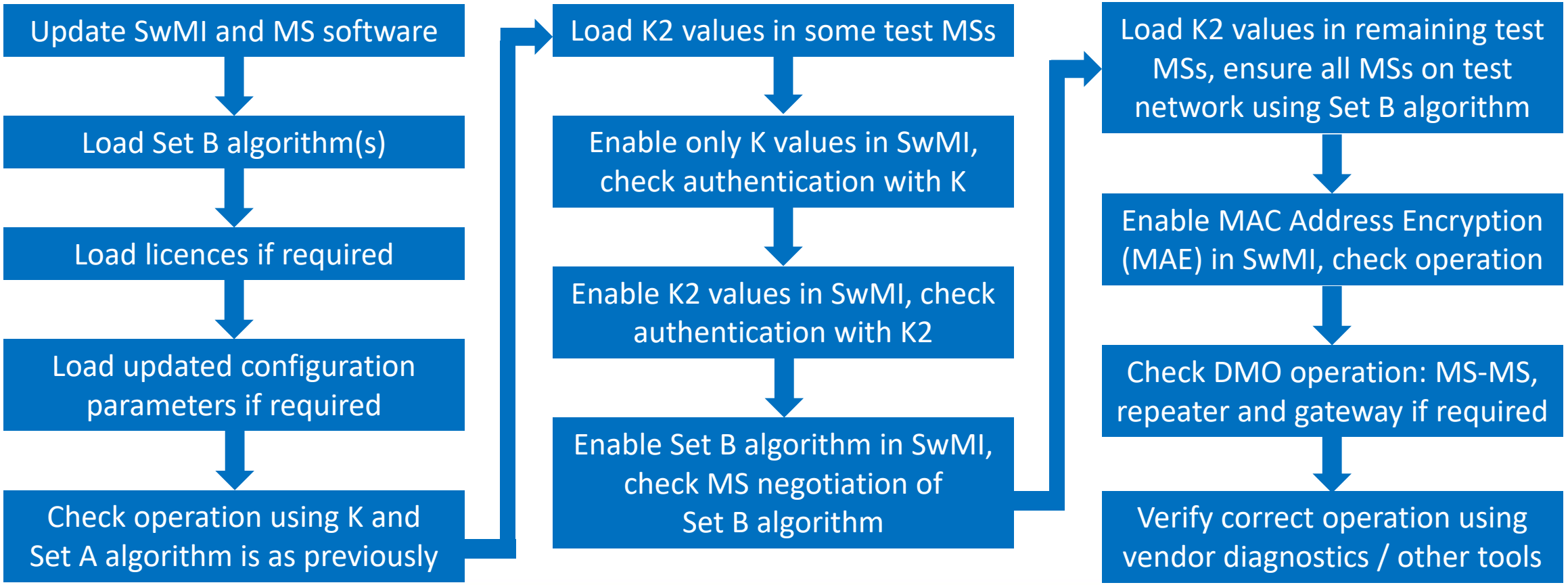
Live network pilot

- If test network trial successful, perform a small pilot trial on part of the live network with less critical users

Tools readiness

- Programming, configuration and key-management tools may first need updating to handle Set B (check with vendors)
- Ensure all tool operations are understood and function correctly
- SwMI and MS may provide diagnostics to determine which algorithms and keys are in use (check with vendors)

Small-scale trial: operations



Procurement

- Identify any hardware needing replacement
- Obtain quotes for hardware, software, algorithms, licences and tools as required
- Resolve budgetary responsibilities
- Place order(s) with sufficient lead-time prior to planned deployment
- Obtain or generate key material e.g. K2, SCKX, CCKX, GCKX

User awareness and training

User awareness

- Explain why the update is needed
- Request co-operation with the roll-out programme
- Communicate the schedule for roll-out and change-over

Training prior to change-over

- Any user actions required during change-over e.g. power cycling MSs
- Any temporary operational changes e.g. using parallel groups, clear groups
- Possible disruptions to normal operations
- Fall-back procedures to adopt in case of problems

Roll-out

Determine processes for updating SwMI and MSs

Adding / replacing algorithm may involve changes to components that are not routinely updated - refer to vendor for guidance

Update programming, configuration and key-management tools as required

Update SwMI – software, algorithms, licences, configuration parameters as required

Update batches of MSs – software, algorithms, licences, configuration parameters as required

Normally performed in a secure environment

Load K2 values into MSs and SwMI authentication centre(s)

Options in accordance with planned transition / testing strategy and degree of confidence required

Test MS operation on SwMI, using K and/or K2, Set A and/or Set B

Authentication change-over

Pre-requisites:

- Select individual or multiple MSs
- MSs and SwMI contain both K and K2
- MSs and SwMI support TEA set A with K2
- Select a time of low network activity and low operational need (e.g. night, off-duty)
- MSs are switched on and registered

Actions:

- Disable K, enable K2 in SwMI for selected MSs
- Perform commanded registration or request users to power cycle MSs
- MSs may first attempt to register with K
- MSs successfully register with K2
- MSs continue to operate with TEA Set A
- In case of failures, re-enable K until fixed

Encryption change-over: TMO

Schedule change-over for quiet time for network

Multiple MSs will need to re-register, authenticate and establish new key material

Provision parallel Set A / Set B or clear groups if required

According to strategy

Provision key material in SwMI (at least CCKX)

Temporarily disable Class 3G (GCK/GCKX) operation if in use

Inform / instruct MS users

For selected MSs in SwMI: disable TEA Set A enable TEA Set B

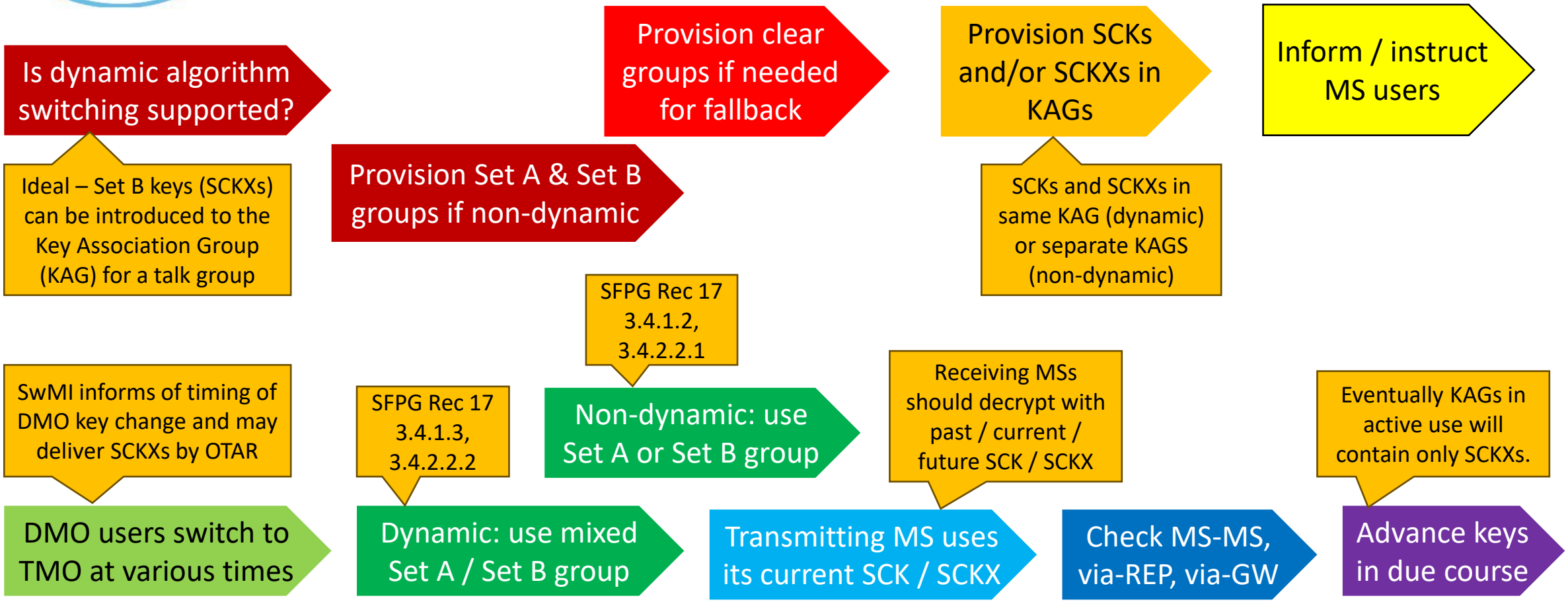
MS may initially propose using a Set A algorithm; SwMI will reject and propose a Set B algorithm; MS should re-attempt registration proposing a Set B algorithm.

MSs re-register and negotiate Set B algorithm

Investigate any failures

Distribute GCKXs and re-enable Class 3G operation if required

Encryption change-over: DMO



Identity encryption change-over

All MSs on SwMI using same TEA set B algorithm

MAE is not possible if any MS is using TEA Set A or a different Set B algorithm.

Schedule change-over for quiet time for network

Change-over occurs at a precise future time. May involve multiple MSs re-registering and break in communication.

Advertise time of change via D-CK CHANGE DEMAND

(ETSI TS 100 392-7 4.5.5.7) Optional for MSs and SwMI to support – MSs may be unaware of impending change. Inform / instruct MS users if required.

Change to MAE at scheduled time

SwMI and aware MSs will change. Unaware MSs will fail to receive encrypted messages.

(ETSI TS 100 392-7 4.5.5.7) Optional for MSs and SwMI to support – MSs may be unaware of change. Inform / instruct MS users if required.

Indicate MAE in use via extended services broadcast

Users power-cycle MSs if required

(ETSI TS 100 392-7 6.7.1.2a.1)

Re-registering MSs informed of identity encryption method

Communication restored when all MSs using MAE

Investigate any failures

For full information see:

ETSI TS 100 392-7 Annex D

https://www.etsi.org/deliver/etsi_ts/100300_100399/10039207/04.02.01_60/ts_10039207v040201p.pdf

TCCA SFPG Recommendation 17

https://tcca.info/_userfiles/pages/files/members_only/working groups/sfpg/rec17ed1.pdf

(available for TCCA members after login to the TCCA website)

TETRA Algorithm Transition

Questions & Answers



Thank you

www.tcca.info | Follow us on tcca-critical-communications

Advancing global critical communications for a safer, more connected world