New Additional TETRA Security Algorithms

TCCA Critical Update Webinar

14 June 2023

View the webinar recording here.

This document sets out the questions and answers from the webinar.

Q1. There has been some discussion about if we can have a 'transition' network with both TEA2 and TEA5 running on the same cell, to facilitate the transition of the fleet of MS?

You can implement an infrastructure in which the cell has support for TEA2 and TEA5 simultaneously, but you cannot have them interworking. Once a terminal has registered on the site it will interact with the infrastructure and determine which key sequence generator (KSG) to use. Either TEA set A or TEA set B based, in this case TEA2 or TEA5. Once it has determined this then the downlink group communication will be using the KSG determined at registration or location update. This means you cannot have any communication across two terminals if one is using a KSG from TEA set A and the other a KSG from TEA set B, unless you use two group identities and then link the groups together. This will require double capacity on that site for providing service for this group, the capacity increase will apply for each instance where interaction between TEA set A and TEA set B is required. Refer to ETSI TS 100 392-7 v4.1.1 Annex D for guidance.

Q2. All of this is purely theoretical, until someone actually presents an MS roadmap with TEA set B capable radios in all segments (intrinsically-safe, covert, mobile, handheld etc.) Could I ask the MS suppliers to provide an indication to when the MS roadmap (all of it, not just one radio) is transitioned to TEA set B?

You do not need to have all terminal products available to initiate a transition to TEA set B, it depends on what is the scenario of the specific infrastructure. If the infrastructure and the users are using intrinsically safe radios then yes they would potentially need it if you are having that user group moving to TEA set B. If you have a network that is not using intrinsically safe radios then you can still move to TEA set B for other terminals and other scenarios. You can do it on a group basis and if you have good planning and have some groups on TEA set A and TEA set B depending on their needs, you could have a mix. You can facilitate that you are moving an important organization to TEA set B regime without necessarily moving the full set of users in the network to TEA set B.
The manufacturers may have or will have a roadmap for support of TEA set B available soon but it has not been disclosed within the TETRA Industry Group yet as it is company sensitive information. We are working within the TETRA Industry Group together as an industry community to provide an ecosystem to maintain an open market situation in the same way as it has been so far with the current algorithms. We are working intensively on this for e.g. interoperability work to allow this. As the roadmaps are sensitive to the industry they may share with their customers rather than another industry member. Any customer and user organization should contact their supplier for further information.

Q3. What are the expected delays and loading on the control channels / slots with the new signalling especially during initial "load" registration? More critical on large systems.

It depends on your configuration but generally would not expect more load once the system has fully transitioned to TEA set B. There is a little bit more communication used in the security downlink element in a PDU and it may contain more information. But if planning is done right and you distribute your communication over time so you don't have too many registrations happening at the same time causing a lot of collisions, I wouldn't expect a significant change.
A transition may include linking of two GSSIs together to facilitate communication between MS's using TEA set A and MS using TEA set B. If this solution is chosen then the load on a control channel would double for each such linking.

Q4. Will Set B replace Set A over time, or will they co-exist forever?

It is important to remember that these are additional algorithms, they don't replace the existing ones. To which degree they will coexist in a specific system or a complete move will be made to TEA set B will depend on the security policy of each operator and each group of users. It is important to remember that TEA set A is still a secure set of algorithms and set B is really being provided to provide security many years into the future.

Q5. Is it expected that MS consumes significantly more battery power to handle the new longer keys?

Some prototyping work has been done on the new algorithms and they do not seem to be significantly more computationally intensive than the old ones. So, it is not expected, but you should ask your suppliers when asking about the roadmap plans. Note also that the most significant MS power drain is usually the regular operation of the radio receiver and frequent operation of the radio transmitter, which are unaffected by the algorithm in use.

Q6. How is MS initiated authentication supposed to work while the BS is in local site trunking mode?

Local site trunking mode depends on the capability of the base station, it would not change anything from today, it would still maintain local site trunking. If it falls back to security class 2 it would use SCK or SCKX as per configuration. It could use a mixture of SCKs but overall would not expect any local site trunking impact if planning is done correctly.

Q7. Will you be doing a follow up session to update with progress later in the year or beginning of next.

Yes, TCCA is planning a workshop after the summer where we can go into more detail and also have a dialogue between the users, operators and vendors to go into this in more detail. If interested please contact harald.ludwig@tcca.info.
The security algorithms are a new but hot topic. It was already part of the Focus Forum at CCW23 in Helsinki and is likely for Dubai for CCW24 as well. This will be another opportunity for an update.

Q8. What is the Forum's thoughts on who (clients) would actually use these algorithms or consider the migrate to it and that there is still the marketing push to other technologies even though TETRA best for critical comms. This could stall peoples' investment?

The vendors are currently building their roadmaps and the operators and users will have to think about their roadmaps too. At present it is not possible to predict any timescales without inputs from operators and vendors. TETRA will continue to be used several years into the future, even in parallel

when new broadband networks are being built. Keeping your network secure is a constant process which requires assessment regularly and which will trigger a decision to upgrade the network to support the additional security algorithms.

Q9. Any costs implication with new algorithms?

For a new system which are initially using TEA set B, the use of TEA set B should not have any cost implications in itself. For a current operational system currently using TEA set A the cost implications would depend on the current state of the system to be updated, such as age of equipment, geographical distribution of system and other factors, some cost should be assumed, the actual cost of the transition can only be determined by individual evaluation of an actual system.

Q10. Will this affect end to end encryption in any way?

No. End-to-End Encryption (E2EE) in TETRA uses mechanisms that are completely separate from those used for Air Interface Encryption or Authentication. The E2EE algorithm is not specified in the TETRA standard, every organization can use algorithms which they trust most.

Q11. Is protection against Quantum Cryptography assigned to the new Algorithms themselves? Or to what?

A key element in the protection against Quantum computing is the key length used in the encryption algorithms going from 80 bits in TEA set A to 192 bits in TEA set B. While the current TEA set A encryption still is strong, new computing devices such as quantum computers may appear and would allow to cryptanalyze TEA set A. The increase of classical computing power available to malicious actors may also threaten TEA set A in the future. In order to ensure continued protection against these possible threats, TEA set B has been introduced.

Q12. During the transition or in case of users are using TEA set A and TEA set B, it will not open a worst scenario case where DMO communication will not be possible?

If the MS is supporting usage of several KSG's then an MS may use a KSG from TEA set A for some groups and a KSG from TEA set B for others and therefore maintaining DMO communication is possible even during transition between a KSG from TEA set A and a KSG from TEA set B. Refer to ETSI TS 100 396-6 v2.1.1 §5.2.1, §6.4.0, §6.4.1 and ETSI TS 100 392-7 v4.1.1 Annex D.5 for guidance.

Ends