

Smarter technology for all

Release 19

Study on enablers for Zero Trust Security (eZTS)

Sheeba Backia Mary B. | **Lenovo, Motorola Mobility**

The Lenovo logo is a vertical rectangle with a red-to-orange gradient background. The word "Lenovo" is written vertically in white, bold, sans-serif font.

Motivation (1/2)

To Enable Zero Trust Security Adaptations for 5G Core Network

- Service Access and Interactions in 5G system are built on certain security principles:
 - Authentication and/or Authorization
 - Secured connection establishment
- Heterogeneity and varied NF(s) deployment options (could be distributed across cloud infrastructure/locations):
 - May run into errors due to configuration issues
 - May get exposure to insider threats
 - May get compromise due to cyber attack
- Trust over a NF or AF can't be assumed static and intact throughout its lifetime despite it's security pre-configurations
- If any NF gets compromised in its life-time:
 - Impacts set of UEs service
 - May impact other network services e.g., connected NFs (i.e., by lateral movement of the attack)

Motivation (2/2)

Zero Trust Security

- The core principle of Zero Trust includes:
 - Continuous security evaluation/monitoring, trust validation and minimizing impacts if any security breach occurs due to external (example., end-users) or by an insider (example., compromised or malicious NF)
 - Adaptation of Zero Trust approach can prevent the lateral movement and further compromises limiting the threats and associated risks.

In the scope of 5G Core:

Existing 5GS core network features considers NFs, set with initial access configurations as trusted (i.e., reliable) throughout its life-time.

- Adaptation of Zero Trust approach in 5G Core can benefit largely to:
 - prevents the threat lateral movement and further compromises (limiting the threats & associated risks).
 - ensures service reliability among network functions and for the end users.

Related ZTS effort made in Release – 18

TR 33.894 - Study on applicability of the Zero Trust Security principles in mobile networks

- Recommendations from the study (1/2):

- **Key Issue(s):**

- **Key Issue #1: Need for continuous security monitoring**

- Security Threats:

- If any NF that has been deployed in the core network, becomes compromised or starts to behave maliciously, and remain undetected then the NF could be misused in attacks leading to a service failure, data loss/theft, etc.

- Potential security requirements:

- The 5GS is required to support mechanisms to collect necessary data to enable security monitoring.

- Conclusion:

- Solution#1 illustrates how existing services can be used to collect the necessary data listed in the solution for security monitoring purposes in line with the principles of zero trust (Tenet 5). However, no consensus could be reached on the normative work.

Evaluation Outcome – Tenet 4,5,6 and 7 [Needs further work]

A Short Summary - TR 33.894 - Recommendations from the study (2/2):

Tenets	NIST	TR 33.894	Status
4	Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.	Tenet #4: Resource access	Evaluation Completed. (Related to T5) Copied some evaluation summary below: Document [2] goes to a great extent into describing the use of "behavioral attributes" as input to the access authorization process. On this particular aspect, the current security standards do not take into account this so far and do not provide any mechanisms for the definition and the collection of such attributes for NFs. Nevertheless, should there be any useful information collected from NFs for access authorization purposes, the same information would be also equally relevant in a security monitoring context. This is covered under the evaluation of Tenet 5 in clause 5.1.5.
5	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	Tenet #5: Security posture	Evaluation Completed. (Action needed!) Copied some evaluation summary below: # A security monitoring function can be outside the SBA and the security monitoring function itself would be mostly proprietary. # It is worth investigating whether there is any additional information that could be exposed by the 5G Core NFs for monitoring purposes. # In the event of that this study determines that strengthening of the external to 3GPP security monitoring is needed, with not yet specified data collection, this information needs to be well defined and explicitly specified to allow for interoperability and secure operation of installed base.
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	Tenet #6: Access security	Evaluation Completed. (Action needed!) Copied some evaluation summary below: # The currently standardized access control related security mechanisms support authentication and authorization for network service access based on identity and credentials. However, they do not consider security monitoring related information (e.g., threat assessments, security posture etc.) or any other aspect that is highly dependent on the deployment. Lack of considering security monitoring information for access decisions will allow the NFs with malicious behaviours to remain unidentifiable and continue to access the services from NF service producers which may lead to lateral movement of the attacks. # From a standardization perspective, at the 3GPP SBA layer one can investigate whether there is any additional information that could be exposed for security monitoring purposes and how such information is used for access control decisions e.g., authorization. This is covered in the evaluation of Tenet 5 in clause 5.1.5.
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	Tenet #7: Data collection to improve security posture	Evaluation Completed. (Related to T5 and T6) Copied some evaluation summary below: # Tenet 7 is an overall directive for operator network to: - facilitate data collection related to security posture, control plane network traffic (i.e., message exchanges between NFs) and access requests, - processing of data (based on operator specific implementation), and - use any insight gained to improve policy creation and enforcement (based on operator policies) in the 5GC. # The tenet reuses principles and mechanisms that are covered in detail in other tenets such as tenet 5 and 6. This tenet provides some additional clarifications on what kind of data can be collected (i.e., related to tenet 5). Consequently, any provisions for such tenets would constitute the building blocks for tenet 7. The data collection related to abnormal behaviour from NFs and related security analysis outcome considerations can help to apply more fine-grained security policies in 5GC.

Scope

- The Objective of the study includes:

- WT1 – Data exposure for security evaluation and monitoring
 - WT1.1: Based on TR 33.894 Kl#1 security requirement, conclusion, and Tenet 5 evaluation, for events which can lead to security threats, define the data to be exposed by the NF and define how those data can be securely exposed to the Operator's security functions (e.g., SIEM) to enable the external security evaluation and monitoring.
 - NOTE: The external security evaluation and monitoring is up to operator's implementation and outside the 3GPP domain. The aspects to enable OAM based data collection is up to SA5 WG. The necessary adaptations specific to exposure services for providing data to the external security function needs SA2 collaboration.
- WT2 – Security mechanism to prevent lateral movement of threat
 - WT2.1: Analyse the impacts and threats related to compromised NF(s) and abnormal NF behaviors.
 - WT2.2: For NFs that have been identified as compromised or misbehaving, study how such information can be utilized to improve access control decisions at the NRF for employing appropriate security mitigations to prevent lateral movement and minimize impact to service availability.
 - WT2.3: Study how 3GPP security policies and controls can be enhanced related to WT2.2 to mitigate threat lateral movement and service availability issues.
- WT3 – Security enhancement recommendations
 - Based on the study outcome, provide recommendations for network based security adaptation, where the recommendations may include but are not limited to requirements, technical enhancements, and procedural fixes.

TU estimates and dependencies

TU Estimate (Study)	TU Estimate (Normative)	RAN Dependency (Yes/No/Maybe)	SA2 / SA5 Dependency (Yes/No/Maybe)
<i>WT1: 1</i>	<i>WT1,3: .5</i>	<i>No</i>	<i>May be</i>
<i>WT2: 1</i>	<i>WT2,3: .5</i>		
<i>WT3: .5</i>	<i>-</i>		
<i>Total: 2.5 TUs (5 meetings)</i>	<i>Total: 1 TUs (3 meetings)</i>		
<i>NOTE: 1 TU is considered as 1.5 hours</i>			

Total TU estimates for the study phase: 2.5 TUs (5 meeting cycles)

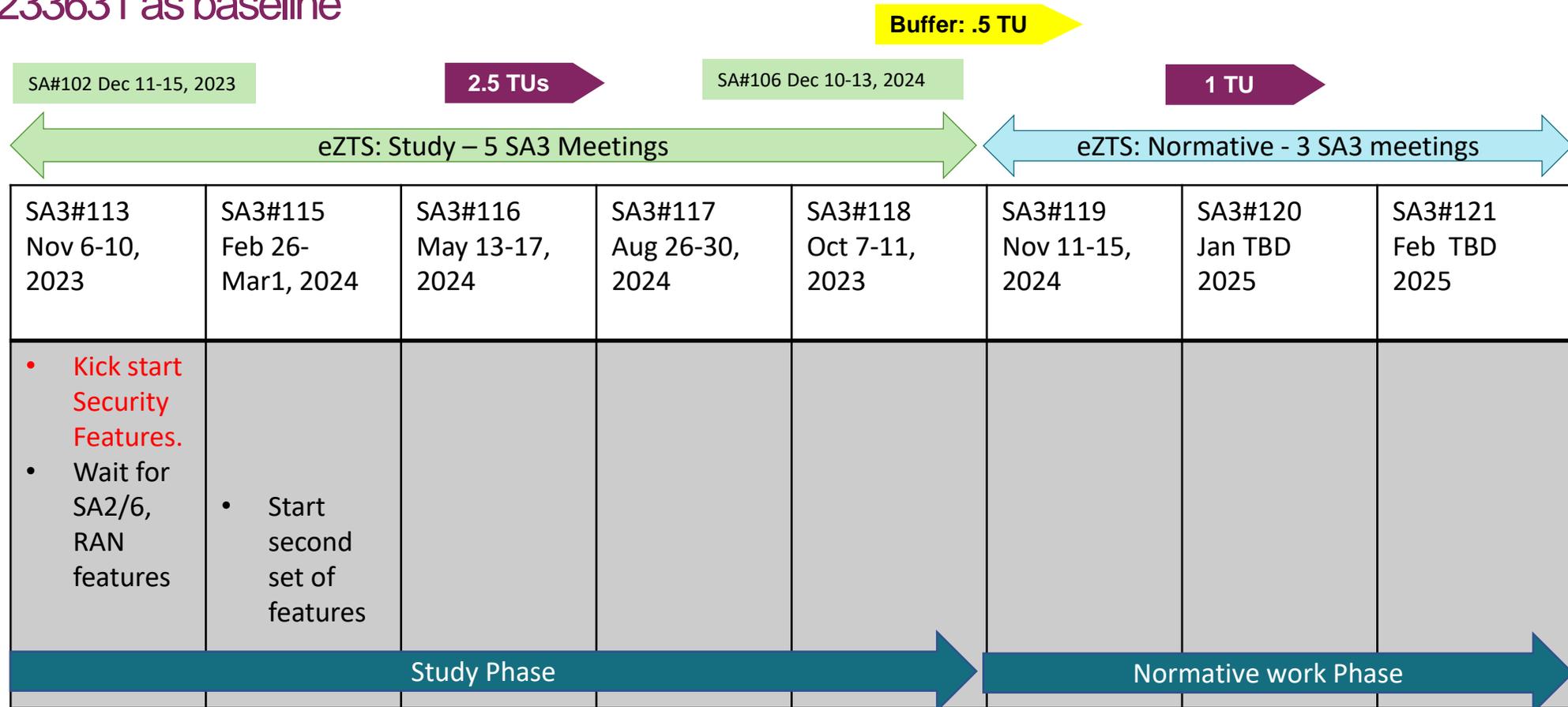
Total TU estimates for the normative phase: 1 TUs (3 meeting cycles)

Buffer TU: .5 TU

Total TU estimates: 4 TUs

Time Plan

Used S3-233631 as baseline



eZTS Study

- The proposal is related to a Security feature.
- Based on SA3 progress needs SA5 and SA2 collaboration/alignment.

thanks.

**Smarter
technology
for all**

Lenovo