**3GPP TSG-SA3 Meeting #119** *draft\_S3-245183-r3 was* ***S3-244626***

Orlando, Florida, 11th – 15th November 2024

**Source:** **Johns Hopkins University APL*,* US National Security Agency*,* MITRE-FFRDC, OTD\_US**

**Title: New annex for eZTS Security Event Data Records**

**Document for: Approval**

**Agenda Item: 5.1**

# 1 Decision/action requested

***Propose to add a new solution for in TR 33.794 to specify the content and format of security event data records.***

# 2 References

[18] 3GPP TS 23.501: “System architecture for the 5G System (5GS); Stage 2”

[24] 3GPP TS 29.571: "Common Data Types for Service Based Interfaces; Stage 3"

[25] IETF RFC 9957: "Date and Time on the Internet: Timestamps with Additional Information"

[26] IEEE 1588: "Precision Clock Synchronization Protocol for Networked Measurement and Control Systems"

# 3 Rationale

The present document proposes a new solution for the format of security event data records.

# 4 Detailed proposal

SA3 is kindly requested to approve the below change to TR 33.794.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[3] 3GPP SP-231784, "New Study on enablers for Zero Trust Security".

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System".

[5] RFC 6749, "The OAuth 2.0 Authorization Framework".

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] 3GPP TR 33.894, 2023 September, V18.0.0: "Study on applicability of the zero trust security principles in mobile networks", Release 18.

[8] NIST Special Publication 800-207: "Zero Trust Architecture".

[9] 3GPP TR 33.738: "Study on security aspects of enablers for network automation for the 5G system phase 3".

[10] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[11] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[12] 3GPP TS 29.501: "5G System; Principles and Guidelines for Services Definition; Stage 3".

[13] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[14] IETF RFC 9113: "HTTP/2".

[15] 3GPP TS 33.117: "Catalogue of general security assurance requirements"

[16] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

[17] <https://owasp.org/www-community/Threat_Modeling_Process>

[18] 3GPP TS 23.501: " System architecture for the 5G System (5GS)".

[19] NIST SP-800-92: "Guide to Computer Security Log Management".

[20] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[21] 3GPP TS 28.541: "Management and orchestration; 5G Network Resource Model (NRM); Stage 2 and stage 3".

[22] O-RAN.WG11.SecReqSpecs.0-R003-v09.00 "Security Requirements and Controls Specifications"

[23] 3GPP TS 29.552: "5G System; Network Data Analytics signalling flows".

[24] 3GPP TS 29.571: " Common Data Types for Service Based Interfaces; Stage 3".

[25] IETF RFC 9957: " Date and Time on the Internet: Timestamps with Additional Information".

[26] IEEE 1588: " Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Mapping of Solutions to Key Issues

**Table 6.3-1 Solutions versus key Issues**

|  |  |  |
| --- | --- | --- |
|  | KI #1 | KI #2 |
| Sol #1 | X |  |
| Sol #2 | X |  |
| Sol #3 | X |  |
| Sol #4 | X |  |
| Sol #5 | X |  |
| Sol #6 | X |  |
| Sol #7 | X |  |
| Sol #8 | X |  |
| Sol #9 |  | X |
| Sol #10 |  | X |
| Sol #11 |  | X |
| Sol #12 |  | X |
| Sol #13 | X |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

7.13 Solution #13: Security event data record format

7.13.1 Introduction

The solution addresses the requirement of key issue#1 to facilitate collection of data potentially relevant for security evaluation and monitoring.

7.13.2 Solution Details

Table 13‑1 Security Event Data Record Format indicates the content and format of security event data records. A security event is an indication of a change in status of one or more monitored security incidents listed in clause 8.1. A threshold may be applied to the type and level of change as indicated by an operator-configured policy. A security event log record captures the data associated with the change in status of one or more monitored security incidents listed in clause 8.1, conclusion for Key Issue #1: Data exposure for security evaluation and monitoring.

Refer to 23.501Annex E.1 [18] for methods that may be employed for communicating data records between Network Functions.

Table 13‑1 Security Event Data Record Format

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Log Info Category** | **Attribute Name** | **Data Type** | **P** | **Description** |
| Security event type | SecEventType | String | Required | Identifies the security event type associated with a security data record. Examples of security event types include: admin, execution, protocol, authentication, and authorization. |
| Security event code | SecEventCode | Uinteger | Required | Identifies the security event associated with a security data record. A security event code identifies a monitored SBA-layer security event attribute. Examples of security event codes include: Excessive processing resource consumption, Excessive rate of received messages, Re-played messages, Failed authentication procedure, Malformed protocol message, Malformed OAuth Token. |
| Data Producer Entity | NFInstanceID | String | Required | Identifies the NF producing the security data record. The format of the NF Instance ID is described in TS 29.571 [24], clause 5.3.2 Simple Data Types. |
| NFServiceSetID | String | Optional | Identifies the service offered within an NF producing the security data record. The format of the NF Service ID is described in TS 29.571 [24], clause 5.4.2 Simple Data Types. This is optional because the source of the security event may be a service, such as a TLS service, which is not within the scope of an NF Service Set. |
| NFProfile | String | Required | Identifies attributes of the NF producing the security data record. The NF Profile is described in TS 29.510 [20], clause 6.1.6.2.2. It includes FQDN, IPv4Addresses, IPv6Addresses, nfServiceList, scheme (e.g., http), and port number. |
| EventSrcIpAddressPort | String | Optional | Identifies the address/port of the entity which originated/triggered the security event. This is optional because the source of the security event may be an entity which is not associated with an IP address, such as a hypervisor or a container manager. |
| Data Transmitting entity | IpEndPoint | String | Required | Identifies the NF which is sending the data record. The format of the IpEndPoint is described in TS 29.510 [20] clause 6.1.6.2.5. |
| Security event start time | SecEventStart | string | Required | Identifies the time-of-day at which the security event started. The format of the SecEventStart is described in RFC 9957 [25]. |
| Security event end time | SecEventEnd | string | Required | Identifies the time-of-day at which the security event ended. The format of the SecEventStart is described in RFC 9957 [25]. |
| Security event counter | SecEventCount | Uinteger | Optional | Provides a count of security events that occurred between the Event Start Time and the Event End Time. |
| Security event timestamp clock | ClockSource | string | Required | Identifies the clock source used to mark the security event start and end times. Examples of ClockSource parameter values include: Unknown, Internal free-run, NTP client, IEEE 1588 [26] PTP client. |
| ClockStatus | string | Optional | Provides operational status associated with clock source used to mark the security event start and end times. Example operational status values include: Not Sysnchronized, Attempting to Synchronize, Synchronized. |
| Security data record version | Data Record Version | string | Required | Identifies the version number of the security log record specification. |
| Data Record ExtensionID | string | Required | Identifies the data record extension identifier associated with the security data record. |
| Security data record extension information | ExtensionFieldLen | Uinteger | Required | Identifies the length of the security data extension field. |
| ExtensionFieldInfo | string | Optional | Provides the security data extension information. The content of this field is not specified. Note that best practices avoid including persistent private credentials (eg, passwords, hashes, or crypto keys) within event data records. |

7.13.3 Evalutation

The solution addresses the requirement of key issue#1 to facilitate collection of security event data that are potentially relevant for security evaluation and monitoring by providing the content and format of the security event data records.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 3rd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 8 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

## 8.1 Key Issue #1: Data exposure for security evaluation and monitoring

The security incidents or scenarios in SBA where data can be collected in the SBA layer includes

1) authentication and authorization failure event;

2) unexpected setup of TLS session and API invocation related to unauthorized reconnaissance;

3) malformed message event;

4) high service load;

5) unexpected SBI call flows; and

6) unexpected use of APIs exposed by services in SBA layer

Editor’s Note: Further aspects if any related to KI#1 is FFS.

The key issue will be addressed by requirements for data collection to enable security evaluation and monitoring on the SBA layer. No new interface nor protocol will be specified as result of the work in this report.

The following requirements address KI#1 Data exposure for security evaluation and monitoring. The requirements also address the use cases for security evaluation and monitoring described in clause 5.1.

General requirements for security event logs:

1. The NF supports the generation of security event logs.

Security event logs contain security relevant events data. Requirements related to security relevant events data for monitoring:

a. The NF collects information on the SBA layer about received malformed messages that deviate from the 3GPP specified messages or are considered invalid according to the protocol specification and network state are to be logged. (Clause 5.1.1)

b. The NF collects information about events involving a massive number of incoming messages on the SBA layer. (Clause 5.1.2).

c. The NF collects information about authentication and authorization failure on the SBA layer. (Clause 5.1.3).

d. The NF collects information about potential replay attacks on the SBA layer. (Clause 5.1.6).

Editors note: Bullet d) is FFS.

Security event logs use the format of security event data records as provided in Solution #13.

Editors note: Additional details if any are FFS.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 4th Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*