**3GPP TSG-CT WG1 Meeting #134-eC1-221331**

**E-Meeting, 17th – 25th February 2022**

(revision of CP-yyxxxx)

**Source: CT1**

**Title: New WID on CT aspects for modifying PASSporT signing and verification**

**Document for: Approval**

**Agenda Item: 17.2**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: New WID on CT aspects for modifying PASSporT signing and verification

Acronym: PP\_SIGN

Unique identifier:

Potential target Release: Rel-17

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | x |  |
| No | x | x | x |  | x |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| x | Feature |
|  | Building Block |
|  | Work Task |
|  | Study Item |

## 2.2 Parent Work Item

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 740018 | SPECTRE |  |

# 3 Justification

SPECTRE WID added the ability to cryptographically assert the authority of the calling user to use the calling identity. Implementation experience gained from authenticating billions of calls per day has revealed several new issues that, if addressed, will improve and simplify the signing process for clients and signing services.

* Servers prefer to support fewer signing resources. For example, instead of having a per-passport-type signing resource, define a single signing resource that passes the passport type as a parameter. This also has the advantage of being more forward compatible in supporting new PASSporT types.
* The server sometimes needs more information from the client than is supported by the currently defined API. One example that has been identified – a telephone Service Provider (acting as the client) wants the signing service to use different certificates depending on the type of user or type of call; e.g., based on calling user location, or based on type of service such as residential vs. commercial, or based on type of call such as domestic vs. international. Any new parameter to support this must be sufficiently abstract to support additional cases that may be discovered in the future. Such a parameter should also be added to the verification request.

- Clients would benefit from more information about verification failures. The existing verification response should be augmented to support the 4xx failure codes defined in RFC 8224. When multiple PASSporTs are being verified, the API should also provide sufficient information so that the client can associate each failure with the specific PASSporT that failed. Clients can use this information for multiple reasons; e.g., to identify verification failures that occurred because of an inadvertent signing error, or as input to analytics.

# 4 Objective

The objective of this work item is to specify in CT1 the following PASSporT signing procedures:

* Enable a single signing request to sign any PASSporT type;
* Enable the client to include information about the user and the call in the signing and verification request that will help the server do its job; and
* Update the verification response so that it conveys the 4xx failure codes/reasons defined in RFC 8224, along with additional information that correlates each failure with the failing PASSporT.

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
| 24.229 | Update the PASSporT signing/verification procedures to resolve issues discovered during implementation/deployment of STIR/SHAKEN, including simplifications for client and server, enhancements to support real-world signing/verification cases, and the ability to report more granular verification failure information. | CP-95e (March 2022) | CT1 responsibility |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Politz, Ken, Neustar, ken.politz@team.neustar

Hancock, David, Comcast; David\_hancock@comcast.com

# 7 Work item leadership

CT1

# 8 Aspects that involve other WGs

None.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Neustar |
| Comcast |
| Oracle |
| Genband Ireland |
|  |
|  |