|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 103 097 | **Version** | 1.3.1 | **CR** | 4 | **rev** | - |  |
|  |
| **CR Title** | Delete link certificate specification |
|  |  |
| **Original Source** | ITS WG5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00557 | **Submission date** | 16.06.2020 |
| **Approving TB**  | ITS | **Approval date** | 01.07.2020 |
| **Category:** | **F** | **Release** | 1 |  |
|  | Use **one** of the following categories:**F** (correction)**A** (correction in an earlier release)**B** (addition of feature) **C** (functional modification of feature)**D** (editorial modification) |  |
|  |  |
| **Reason for change** | The document submitted in [ITS(20)038032](https://docbox.etsi.org/ITS/ITS/05-CONTRIBUTIONS/2020/ITS%2820%29038032_EU_CCMS_Follow-up_of_PlugTest_and_updates_required_in_standa.zip) (section 2.1) requires link certificates to be TS 102 941 messages and not (as currently specified) Ts103097Certificates. TS 102 941 will be update accordingly, see [RTS/ITS-00554 (TS 102 941)](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57505) |
|  |  |
| **Consequence if not approved** | Standard compliant devices cannot not trust the update of TLM certificates using link certificate and hence cannot trust ECTLs signed by the new TLM certificate.  |
|  |  |
| **Summary of change** | Delete the statements: For root certification authority link certificates, the component issuer shall be set to sha256AndDigest or sha384AndDigest as defined in IEEE Std 1609.2 [1] clause 6.4.7.For Trust List Manager link certificates, the component issuer shall be set to sha256AndDigest or sha384AndDigest as defined in IEEE Std 1609.2 [1] clause 6.4.7. |
|  |  |
| **Clauses affected** | 7.2.3 and 7.2.5. |
|  |  |
| **Linked Change Requests** | - |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

### 7.2.3. Root CA certificates

***Apply the following changes (deletions):***

This clause defines additional aspects of Root CA certificates as defined in ETSI TS 102 940 [i.1]. Root CA certificates shall be of type EtsiTs103097Certificate as defined in clause 6, with the following constraints:

The component issuer shall be set ~~as follows:~~

* ~~For root certification authority certificates, the component issuer shall be set~~ to self.
* ~~For root certification authority link certificates, the component issuer shall be set to sha256AndDigest or sha384AndDigest as defined in IEEE Std 1609.2 [1] clause 6.4.7.~~

These toBeSigned components shall be included in addition to those specified in clause 6:

* certIssuePermissions shall be used to indicate issuing permissions, i.e. permissions to sign subordinate certification authority certificates with certain permissions.
* appPermissions shall be used to indicate permissions to sign:
* CRLs and contain the ITS-AID for the CRL as assigned in ETSI TS 102 965 [2].
* CTLs and contain the ITS-AID for the CTL as assigned in ETSI TS 102 965 [2].

The toBeSigned component CertificateId shall be set to the choice name and shall contain a unique name associated to the root certification authority.

Additional requirements to Root CA certificates are defined in [i.4].

### 7.2.5 Trust List Manager certificate

***Apply the following changes (deletions):***

This clause defines additional aspects of Trust List Manager certificates. Trust List Manager certificates shall be of type EtsiTs103097Certificate as defined in clause 6, with the following constraints:

The component issuer shall be set ~~as follows:~~

* ~~For Trust List Manager certificates, the component issuer shall be set~~ to self.
* ~~For Trust List Manager link certificates, the component issuer shall be set to sha256AndDigest or sha384AndDigest as defined in IEEE Std 1609.2 [1] clause 6.4.7.~~

These toBeSigned components shall be included in addition to those specified in clause 6:

* region: this component shall contain the geographic validity restriction associated to the Trust List Manager.
* appPermissions: this component shall contain the ITS-AID for the CTL as assigned in ETSI TS 102 965 [2].

The toBeSigned component CertificateId shall be set to the choice name and contain the unique name string associated to the TLM.

These toBeSigned components shall be absent:

* encryptionKey.
* certIssuePermissions.

Additional requirements to TLM certificates are defined in [i.4].