|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 102 941 | **Version** | 1.3.1 | **CR** | 7 | **rev** | - |  |
|  |
| **CR Title** | Specify the CPOC distribution protocol for TLM certificates, TLM link certificates, ECTL and DeltaECTL |
|  |  |
| **Original Source** | ITS WG 5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00552 | **Submission date** | *03/08/2020* |
| **Approving TB**  | ITS | **Approval date** |  |
| **Category:** | **B** | **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** | TS 102 941 does not specify how the CPOC supplies ECTLs and TLM Certificates in a machine readable form. The current standard only defines the communication protocols for requesting CRL and CTL for Root CAs. |
|  |  |
| **Consequence if not approved** | Trusted ITS entities cannot access the regular publications of (full or delta) ECTLs published by the TLM/CPOC, the regular re-keyed TLM Certificates and the TLM link certificate messages that establish the secure link to the new re-keyed TLM Certificates. |
|  |  |
| **Summary of change** | Using a machine-readable interface, each trusted ITS entity may contact the CPOC distribution centre using an HTTP GET to access the TLM certificates, TLM Link certificate messages, ECTLs and delta ECTLs via a defined web-endpoint distribution centre of the CPOC. The URL-scheme is based on the definitions for RCA-CTLs of ETSI TS 102941 V1.2.1. |
|  |  |
| **Clauses affected** | 6.1.5, 6.3.5, new Annex E, renumbering of Annexes E, F and G |
|  |  |
| **Linked Change Requests** | Link to CR TS 102 941 #0003 specification of link certificate message |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

*Add the affected clauses with track changes.*

### 6.1.5 Maintenance

If an EA or AA is added to or removed from the system, the Root CA shall inform enrolled ITS-Ss of this change.

When multiple Root CAs are used in the same Trust Domain (as specified in ETSI TS 102 940 [5]), the trust relationship between the different PKIs may be managed by a Trusted Third Party (Trust List Manager). If a Root CA is added or removed from the system, the TLM should inform enrolled ITS-Ss of this change.

The process for updating the trust information lists such as the CTL and the CRL and for publishing these lists by the associated trust authority is specified in clause 6.3 and include different possible methods for updating the enrolled ITS‑Ss:

* requesting ECTL, TLM certificates and their linkage information (TLM link certificate messages) to the distribution centre of the CPOC;
* requesting CRL and CTL from the distribution centre associated to the root CA;
* sending a trust information list (CRL or CTL) across a wireless interface e.g. using a RSU able to transmit the CRL/CTL on ITS G5; or
* providing information to a trusted maintenance entity to enable it to update an individual ITS-S in a controlled environment.

### 6.3.5 Transmission of CTL and CRL

Different methods for updating the enrolled ITS-Ss may be used as specified in clause 6.1.5. Communication profiles for transmitting the CTL or CRL CA to enrolled ITSs are specified in annex D.

The communication requirements for requesting the ECTL, Delta ECTL, TLM certificates and TLM link certificate messages to the CPOC are specified in Annex E.

……………………

Annex E (normative):
Communication profiles for TLM Certificates, TLM Link Certificate Messages, ECTLs and delta ECTLs access

### E.1 CPOC HOST URL Definition

In order to provide a machine-readable interface, the distribution of TLM certificates, TLM Link certificate messages, ECTLs and delta ECTLs shall be done via a defined HOST URL of the CPOC distribution centre.

NOTE: In the EU C-ITS Security Credential Management System (EU CCMS), the CPOC HOST URL is currently set to cpoc.jrc.ec.europa.eu [i.18].

Naming scheme and interpretation of TLM name

The TLM certificate profile specified in TS 103 097 clause 7.2.5 [3] requires that the CertificateId component of the ToBeSignedCertificate contains the TLM unique name of type string (UTF8String(SIZE(0..255))).

In the EU CCMS a mandatory naming scheme for TLM name in the CertificateID component is specified as well as a naming scheme and names meaning for Root CAs ([i.18]).

NOTE: in the EU CCMS, the naming scheme for TLM certificates is specified as follows

allowing to be able to reflect different possible levels of its operating environment:

* the CertificateID in TLM Certificates consisst of the pre-fix “EU-TLM” and an optional <TLM-ENVIRONMENT> component, combined with a separator (“\_”): EU-TLM\_<TLM-ENVIRONMENT>;
* the <TLM-ENVIRONMENT> post-fix is an optional component which is set by the TLM to create TLM certificates which are used to sign specific ECTLs for specific RCA certificate environments (in this case the same optional <RCA\_ENVIRONMENT> field is set in the RCA CertificateID component of the ToBeSignedCertificate). If the post-fix is ABSENT, the the regular operational TLM entity used to sign the ECTL.

The following clauses assume that the name for the “default TLM” (i.e. the regular operational TLM entity used for the operation of deployed C-ITS services) is specified and hence the ECTL issued by these TLM certificates is called “default ECTL”.

### E.2 Request of TLM certificate

GET http(s)://<HOST>/[<subpath>]/gettlmcertificate/[<HashedId8>]

The absolute path in the GET request shall be set to <HOST>/[<subpath>] where the <HOST> is the URL of the CPOC Distribution Centre and [<subpath>] may optionally contain a defined value in order to enable the CPOC to provide different sets of TLM Certificates and ECTLs using this specific access point.

* Inputs:
	+ <HOST>: The fixed hostname as described in clause E.1
	+ <subpath>: Optional as described above
	+ <HashedId8>: Optional: The HashedId8 of the requested TLM certificate. If omitted, the latest valid TLM certificate will be returned.
* Outputs:
	+ Content-type: application/octet-stream
	+ Content: The requested TLM certificate, COER-encoded of type EtsiTs103097Certificate.

If the <subpath> is omitted, the CPOC shall either return

* the TLM Certificate used to sign ECTLs for RCA certificates where no specific RCA environment is set (**Note:** what is currently provided as such “default ECTL” in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly) or

### no file at all.

### E.3 Request of TLM link certificate message

GET http(s)://<HOST>/[<subpath>]/gettlmlinkcertificate/[<HashedId8>]

* Inputs:
	+ <HOST>: The fixed hostname as described in clause E.1
	+ <subpath>: Optional as described in clause E.2
	+ <HashedId8>: Optional: The HashedId8 of the TLM certificate to which the TLM link certificate message links to. If omitted, the link certificate message linking to the latest issued and valid TLM certificate (“current valid TLM Certificate”) will be returned.
* Return value:
	+ Content-type: application/octet-stream
	+ Content: The requested TLM link certificate message (as specified in clause 6.4).

If the <subpath> is omitted, the CPOC shall either return

* the TLM link certificate message establishing the link to the specified TLM Certificate (through its certificate digest HashedId8)used to sign ECTLs for RCA certificates where no specific RCA environment is set (**Note:** what is currently provided as such “default ECTL” in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly) or

### no file at all.

### E.4 Request of full ECTL

GET http(s)://<HOST>/[<subpath>]/getectl/HashedId8

* Inputs:
	+ <HOST>: The fixed hostname as described in clause E.1
	+ <subpath>: Optional as described in clause E.2
	+ <HashedId8>: The HashedId8 of the signing TLM certificate which shall return the last ECTL signed by that TLM certificate.
* Outputs:
	+ Content-type: application/octet-stream
	+ Content: The requested full ECTL, COER-encoded of type TlmCertificateTrustListMessage.

Even if the TLM has already re-keyed its TLM Certificate, the TLM shall continue to provide the last ECTL signed with the specific (old) TLM Certificate through the above GET command.

If the <subpath> is omitted, the CPOC shall either return

* the full ECTL containing RCA certificates where no specific RCA environment is set (**Note:** what is currently provided as such “default ECTL” in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly) or
* no file at all.

### E.5 Request of delta ECTL

GET http(s)://<HOST>/[<subpath>]/getdeltaectl/<HashedId8>/[<EctlSequenceNumber>]

* Inputs:
	+ <HOST> : The fixed hostname as described in clause E.1
	+ <subpath>: Optional as described in clause E.2
	+ <HashedId8>: The HashedId8 of the signing TLM certificate.
	+ <EctlSequenceNumber>: Optional: The sequence number of the requested delta ECTL. If omitted, the latest delta ECTL will be returned.
* Outputs :
	+ Content-type: application/octet-stream
	+ Content: The requested delta ECTL, COER-encoded of type TlmCertificateTrustListMessage.

The EctlSequenceNumber of range [0...255] in (delta) ECTLs is reset to 0 with every new signing TLM certificate (i.e. with each TLM re-key and the first signing of a new ECTL making use of the new re-keyed TLM certificate). This is done in order to reduce the chance of overruns of EctlSequenceNumber during the lifetime of each used TLM certificate. In case the TLM has to sign more than 255 (delta) ECTLs during the validity period of a TLM certificate, the TLM shall re-key its TLM certificate before it reaches 255.

If the <subpath> is omitted, the CPOC shall either return

* the delta ECTL containing RCA certificates where no specific RCA environment is set (**Note:** what is currently provided as such “default ECTL” in the EU CCMS is subject to decision of the CPA which instructs the CPOC accordingly) or
* no file at all.

Annex ~~E~~F (informative):
Encryption of a message from a sender to a receiver

……………………

Annex ~~F~~G (informative):
Bibliography

……………………

Annex ~~G~~H (informative):
Change history

……………………