|  |
| --- |
| **CHANGE REQUEST** |
|  | ETSI TS 103 601 | **Version** | 1.1.1 | **CR** | 1 | **rev** | - |  |
|  |
| **CR Title** | Correct specification of the requirements for the P2P CRL/CTL request service in clause 5.3. |
|  |  |
| **Original Source** | ITS WG5 |
|  |  |
| **Work Item Ref** | RTS/ITS-00550 | **Submission date** | *06/01/2023* |
| **Approving TB**  | ITS | **Approval date** | *20/01/2023* |
| **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** | In the current version of ETSI TS 103 601, the specification of the P2P CRL/CTL distribution service in clause 5.3 is using an old proposition which intended to use and extend the field missingCrlIdentifierof the headerInfo data structure, but was finally abandoned. Instead the new extension mechanism Contributed Extensions (in HeaderInfo) was designed commonly with the IEEE 1609.2 standardization subgroup and this new extensibility mechanism is used for the specification of the P2P CRL/CTL request service. |
|  |  |
| **Consequence if not approved** | The requirements specified in the standard cannot be fulfilled or if fulfilled, the request for CRL/CTL inserted in the transmitted secure message (SPDU) would create an interoperability issue (the receiver would reject the received messages as non-compliant to the profile of TS 103 097). |
|  |  |
| **Summary of change** | Correction of requirements for the transmission of a request for CRL/CTL inserted in the HeaderInfo of a secure PDU.  |
|  |  |
| **Clauses affected** | 5.3.1; 5.3.4.1; 5.3.6 |
|  |  |
| **Linked Change Requests** |  |  |
|  |  |  |
|  |  |
| **Other comments** |  |
|  |  |

*Add the affected clauses with track changes.*

5.3.1 Overview

…………..

To provide the peer-to-peer distribution service, the ITS-Ss shall provide the following capabilities:

* The ITS-S requester shall provide functionalities to add a missing CRL/DeltaCTL request field ~~(missingCrlIdentifier)~~using the ETSI originating’s Header Info extension specified in ETSI TS 103 097 [3] clause 4.2.2, which is inserted in a transmitted secure F-PDU (e.g. a CAM, etc.) to request other ITS-Ss to provide the missing CRL/DeltaCTL and to receive the response using the in-band communication (short-range communication via a ITS 5,9 GHz channel, e.g. SCH).

NOTE: for the purpose of peer-to-peer distribution of CTL and CRL, the ETSI TC ITS group has specified two extensions in its reserved contributed extension block: etsiTs102941CrlRequest and etsiTs102941DeltaCtlRequest.

5.3.4.1 General

…………..

The requesting ITS-S starts to transmit P2P CRL/CTL Distribution (P2PCXLD) request inserted in the secured F-PDU (e.g. CAM, etc.) under precise trigger conditions which are specified in clause 5.3.~~5~~6.

### 5.3.6 P2P CRL/CTL request message trigger, repetition and termination

…………..

* when the ITS-S receives a signed PDU which contains an ETSI originating extension block in the HeaderInfo structure (component of type ContributedExtensionBlock identified by etsiHeaderInfoContributorId (2)) including an extension of type CTL request (EtsiTs102941DeltaCtlRequest) from another ITS-S and finds out that the value lastKnownCtlSequence associated to the certificate Identifier of the issuer (TLM or RCA) is higher than the sequence number of the CTL of TLM or RCA stored in the ITS-S memory.
* when the ITS-S receives a signed PDU which contains ~~a missingCrlIdentifier in the SignedData structure~~  an ETSI originating extension block in the HeaderInfo structure (component of type ContributedExtensionBlock identified by etsiHeaderInfoContributorId (2)) including an extension of type CTL request (EtsiTs102941DeltaCtlRequest) from another ITS-S and finds out that the value ~~ctlSequence~~lastKnownCtlSequence associated to the certificate Identifier of the issuer (TLM or RCA) is higher than the sequence number of the CTL of TLM or RCA stored in the ITS-S memory.

…………..

* when the ITS-S receives secured messages from a peer ITS-S using A~~t~~Ts issued by an AA linked to its own RCA or another RCA. The ITS-S shall set ~~in the cracaId field of the missingCrlIdentifier structure~~ the ETSI originating extension block in the HeaderInfo structure (component of type ContributedExtensionBlock identified by etsiHeaderInfoContributorId (2)) containing an extension of type CRL request (EtsiTs102941CrlRequest) where the value of HashedId3 of the topmost certificate (trust anchor) of the certificate chain built from the AT used by the peer ITS-S and the lastKnownUpdate ~~thisUpdate~~ field is set to thisUpdate value of the CRL stored in the ITS-S memory.