|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CHANGE REQUEST** | | | | | | | | | | | | | | | |
|  | ETSI TS 102 941 | | | **Version** | 2.1.2 | **CR** | | 4 | | **rev** | | | | 1- |  |
|  | | | | | | | | | | | | | | | |
| **CR Title** | | Adding indirect initial enrolment. | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | |
| **Original Source** | | ITS WG5 | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | |
| **Work Item Ref** | |  | | | | | **Submission date** | | | | |  | | | |
| **Approving TB** | | ITS | | | | | **Approval date** | | | | |  | | | |
| **Category:** | | **B** | **Release** | | | | | | | |  | | |  | |
|  | | 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** | | | For harmonization with IEEE 1609.2.1, the initial enrolment shall allow indirect authentication/authorization using proprietary measures. | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Consequence if not approved** | | | Manufacturers must implement additional protocols instead of relying on existing infrastructure for authentication and authorization of systems. | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Summary of change** | | | Allow indirect authentication/authorization of systems. | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Clauses affected** | | | 6.1.2, 6.1.3 | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Linked Change Requests** | | |  | | | | | |  | | | | | | |
|  | | |  | | | | | |  | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Other comments** | | |  | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |

6.1.2 Manufacture

As part of the ITS-S manufacturing process, the following information elements associated with the identity of the station shall be established within the ITS-S itself and within the Enrolment Authority (EA):

* In the ITS-S, the following information elements shall be established using a physically secure process. The specification of this physically secure process is out of scope for the present document:
  + a canonical identifier which is globally unique (see note 1);
  + contact information for the EA and AA which will issue certificates for the ITS-S:
    - network address;
    - public key certificate;
  + the set of current known trusted AA certificates which the ITS-S may use to trust communications from other ITS-S;
  + when using the process specified in Section 6.2.3.2 for the initial enrolment: a public/private key pair for cryptographic purposes (canonical key pair); and
  + the trust anchor (Root CA) public key certificate and the DC network address;
  + in case of a multiple root CAs architecture as specified in [5], the TLM public key certificate and the CPOC network address.
* NOTE 1: The management of the canonical identifier and the means to guarantee uniqueness are not addressed in the present document.
* In the EA, the following three items of information shall be established, all associated with each other (see note 2):
  + the permanent canonical identifier of the ITS-S;
  + the profile information for the ITS-S that may contain an initial list of maximum appPermissions (ITS‑AIDs with SSPs), region restrictions and assurance level which may be modified over time;
  + when using the process specified in Section 6.2.3.2 for the initial enrolment: the public key from the key pair belonging to the ITS-S (canonical public key).
* NOTE 2: The process for establishing this information within the ITS-S and the EA is beyond the scope of the present document.

6.1.3 Enrolment

The ITS-S requests its enrolment certificate from the EA (see clause 6.2.3.2).

When an end entity applies for an enrolment certificate, it may indicate that it is entitled to the certificate *directly* or *indirectly*. Compare with Section 4.1.4.2 of IEEE 1609.2.1.

In the *indirect* initial enrolment case, the Enrolment Authority (EA) is given assurance that the end entity is entitled to the enrolment certificate by means outside the scope of the enrolment certificate request. For example, the enrolment request could happen in an environment that is trusted by the EA and the request could be transmitted over a secure connection.

In the *direct* initial enrolment case, before enrolment happens, the end entity generates a keypair known as the canonical keypair and is assigned (or generates) a globally unique identifier known as the canonical identity (cf. Section 6.1.2). The state transitions for enrolment are shown in Figure 2.

****

**Figure 2: Simplified state machine for the enrolment process**

After a successful enrolment process, the ITS-S shall possess an enrolment credential that shall be used in subsequent authorization requests.

For renewing the Enrolment Certificate at the EA, the ITS-S shall send an EnrolmentRequest signed by the previous valid enrolment credential issued by this EA.