|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CHANGE REQUEST** | | | | | | | | | | | | | | | |
|  | ETSI TS 102 941 | | | **Version** | 2.0.1 | **CR** | | *001* | | **rev** | | | | - |  |
|  | | | | | | | | | | | | | | | |
| **CR Title** | | CR to update versions of TLS in clause 7.3 | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | |
| **Original Source** | | ITS WG 5 | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | |
| **Work Item Ref** | | RTS/ITS-00554 | | | | | **Submission date** | | | | | *20/05/2020* | | | |
| **Approving TB** | | ITS | | | | | **Approval date** | | | | |  | | | |
| **Category:** | | **A** | **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 IP-based communications used in a unicast mode (point-to-point communication in the ISO / OSI reference model) the security protocol referred in TS 102 941 for security association is TLS v1.2. TLS v1.3 is published and many implementations are available and are being used in some C-ITS deployment initiatives in Europe like C-ROADS.  The TS 102 941 in Release 2 needs to be updated to support TLS 1.2 and TLS 1.3 as long as the requirements to protect the data transmission in integrity, authenticity and/or confidentiality are ensured. | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Consequence if not approved** | | | TLS v1.2 and TLS v.1.3 is not fully supported | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Summary of change** | | | Enables an ITS-S to support TLS V1.2 or TLS 1.3 to establish a unicast security association between the 2 peer entities when they use an IP communication link. | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Clauses affected** | | | Clauses 2.2 , 7.3 | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Linked Change Requests** | | |  | | | | | |  | | | | | | |
|  | | |  | | | | | |  | | | | | | |
|  | | |  | | | | | | | | | | | | |
| **Other comments** | | |  | | | | | | | | | | | | |
|  | | |  | | | | | | | | | | | | |

## 2.2 Informative references

……....

[i.16] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

RFC 8446 Transport Layer Security Protocol

## 7.3 Unicast SAs

……....

~~Also, security in the transport layer can be provided using methods such as the IETF Transport Layer Security (TLS) [i.7].~~

Also, security in the transport layer can be provided using protocols such as the IETF Transport Layer Security ([i.7], [i.16]). An ITS-S should support TLS 1.2 [i.7] or TLS 1.3 [i.16] and the allowed and mandatory cipher-suites to protect data transmission over the Transport layer (TCP protocol).

NOTE: The rules on allowed and mandatory cipher-suites and on allowed and mandatory extensions as specified in TLS 1.2 and TLS 1.3 are out of the scope of the present document.