ISO/TR 21186-3:2021 (E)

Cooperative intelligent transport systems (C-ITS) — Guidelines on the usage of standards — Part 3: Security

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Symbols and abbreviated terms

5 Security in C-ITS

5.1 General
5.2 Security design process for C-ITS applications
5.3 Communications security mechanisms in C-ITS
5.4 Source authentication and access control mechanisms
5.5 Certificate authorities and certification processes
5.6 Introduction to the rest of this document

6 Security analysis and controls for an IDX device

6.1 Background
6.2 IDX device concept
6.2.1 General
6.2.2 System architecture and device
6.2.2.1 Target of evaluation
6.2.2.2 General system view
6.2.2.3 Connections and trusted relationships
6.2.3 Threat modelling data scenarios and examples
6.2.3.1 Scenario 1— non-sensitive public data
6.2.3.2 Scenario 2 — privacy-protected data assets
6.2.3.3 Scenario 3 — executable or writeable data assets
6.2.4 Assumed device functions and activities
6.3 Device assets
6.4 Threats
6.4.1 General
6.4.2 Threat modelling process
6.4.3 Threat categories and actor motivations
6.4.4 Scenario comparison of threats
6.5 Security objectives
6.5.1 Summary and comparison by scenario
6.5.2 Analysis
6.6 SFR and rationales
6.7 Comparison to other common criteria PPs
6.7.1 General
6.7.2 Summary and analysis of gaps
6.7.3 Gap analysis with Car2Car HSM PP
6.7.4 Gap analysis against V-ITS base PP
6.7.5 Gap analysis against V-ITS Comms Module PP

7 ISO/TS 21177 access control implementation guidance

7.1 General
7.2 High level architecture and access scenario

7.3 Application protocol architecture and ISO/TS 21177 integration
7.3.1 General
7.3.2 Example protocol architecture
7.3.3 Protocol integration strategy
7.4 Access control policy structure
7.5 Access control approach
7.6 Access control use cases and sequence diagrams
7.6.1 General
7.6.2 Define an access policy
7.6.3 Load an access control policy
7.6.4 Configure TLS
7.6.5 Start a secure TLS session
7.6.6 Secure access-controlled resource discovery
7.6.7 Server controls access to UGP service based on role

8 C-ITS CP security requirements gaps and needs

8.1 General
8.2 Overview of European C-ITS CP
8.3 PKI threat categories and mitigations
8.4 European C-ITS CP changes to support news C-ITS applications
8.4.1 General
8.4.2 CP Section 1.6.1
8.4.3 CP Section 1.6.2
8.4.4 CP Section 6.1.5.2
8.4.5 CP Section 4.1.2.4

Annex A (informative) Scenario threats

Annex B (informative) Scenario security objectives to security functional requirements mapping

Annex C (informative) Informative proposal for improvements of TS 21177:2019: CRL request

C.1 Verbal forms for expressions of provisions
C.2 Rationale
C.3 Design considerations
C.4 Annex structure
C.5 Proposed amendment 1
C.6 Proposed modification of ISO/TS 21177:2019, 7.5.3 "Iso21177AccessControlPdu"
C.7 Proposal for new sections to be added to ISO/TS 21177:2019, 7.5
C.7.1 "SecurityMgmtInfoPdu"
C.7.2 "SecurityMgmtInfoRequest"
C.7.3 "EtsiCrlRequest"
C.7.4 "EtsiCtlRequest"
C.7.5 "IeeeCrlRequest"
C.7.6 "CertChainRequest"
C.7.7 "SecurityMgmtInfoResponse"
C.7.8 "SecurityMgmtInfoErrorResponse"
C.7.9 "EtsiCrlResponse"
C.7.10 "EtsiCtlResponse"
C.7.11 "IeeeCrlResponse"
C.7.12 "CertChainResponse"

Annex D (informative) Informative proposal for complements to TS 21177:2019: Ownership and access policy

D.1 General
D.2 Ownership use case
D.2.1 Authorization use case
D.2.2 Ownership management use case
D.3 Owner authorized flowchart

Annex E (informative) Informative proposal for improvements of TS 21177:2019: Errata, additional rationale material, and session persistence across certificate expiry

E.1 Errata
E.2 Rationale for choice of SPAKE for enhanced authentication
E.3 Session persistence across certificate expiry

E.3.1 Background
E.3.2 Processing
E.3.3 Note on presentation
E.3.4 Proposed modification of ISO/TS 21177:2019, 7.5.3: "Iso21177AccessControlPdu"
E.3.5 Proposed modification of ISO/TS 21177:2019, 7.5.8: "AtomicExtendedAuthRequest"
E.3.6 Proposed new sections to be added to ISO/TS 21177:2019, 7.5: "SessionExtensionPdu"
E.3.7 Proposed modification to IEEE 1609.2: "PduFunctionalType"

Page count: 125