How ISO 21217 works

Please view as a “Slide Show”

CEN PT1605
The basic situation

- Two devices cooperate in a trusted way, i.e. exchange information in secure application sessions.
Example: Multiple after-market services using OEM installed SVI

- In-vehicle domain
  - Proprietary stack (security & translation)
  - Proprietary Network Node
  - Proprietary Network Node

- External domain
  - Manufacturer Services
    - Applications
      - Facilities
      - Network & Transport
      - Access
      - Security
  - CV / C-ITS
    - Applications
      - Facilities
      - Network & Transport
      - Access
      - Security

- Diagnostic
  - Management
    - Applications
      - Facilities
      - Network & Transport
      - Access
      - Security

- Insurance
  - Management
    - Applications
      - Facilities
      - Network & Transport
      - Access
      - Security

- Fleet Mngt
  - Management
    - Applications
      - Facilities
      - Network & Transport
      - Access
      - Security

- SVI Interface can be wireless (DSRC, WiFi, 4G/5G, OBD, etc)
Security: Authentication / Authorization

- Proprietary stack (security & translation)
  - Applications
  - Network & Transport
  - Access
  - Security

- Management
  - Applications
  - Facilities
  - Network & Transport
  - Access
  - Security

- Fleet Mngt
  - Applications
  - Facilities
  - Network & Transport
  - Access
  - Security

- Insurance
  - Applications
  - Facilities
  - Network & Transport
  - Access
  - Security

- Diagnostic
  - Applications
  - Facilities
  - Network & Transport
  - Access
  - Security
Security: Authentication / Authorization

Proprietary stack (security & translation)

Management

Network & Transport

Access

Applications

Facilities

Network & Transport

Access

Security

CV/C-ITS

Proof: valid C-ITS Application

Fleet Mngt

Applications

Facilities

Network & Transport

Access

Security

Insurance

Applications

Facilities

Network & Transport

Access

Security

Diagnostic

Applications

Facilities

Network & Transport

Access

Security

Policy

autoload association

Independence drives us.
Security: Authentication / Authorization

- CV/C-ITS
  - Applications
  - Facilities
  - Network & Transport
  - Access
- Fleet Mgmt
  - Applications
  - Facilities
  - Network & Transport
  - Access
- Insurance
  - Applications
  - Facilities
  - Network & Transport
  - Access
- Diagnostic
  - Applications
  - Facilities
  - Network & Transport
  - Access

Proprietary stack (security & translation)

Proof: valid C-ITS Application

Certificate

Policy

Independent drives us.
Security: Authentication / Authorization

Proprietary stack (security & translation)

Management

Applications

Facilities

Network & Transport

Access

Security

CV/C-ITS

Applications

Facilities

Network & Transport

Access

Security

Fleet Mngt

Applications

Facilities

Network & Transport

Access

Security

Insurance

Applications

Facilities

Network & Transport

Access

Security

Diagnostic

Applications

Facilities

Network & Transport

Access

Security

I have a C-ITS certificate

Proof: valid C-ITS Application

Certificate

Policy

I have a C-ITS certificate
Security: Authentication / Authorization

Proprietary stack (security & translation)

Management

Network & Transport

Access

Applications

Facilities

Network & Transport

Access

Security

CV/C-ITS

Applications

Facilities

Network & Transport

Access

Security

Fleet Mngt

Applications

Facilities

Network & Transport

Access

Security

Insurance

Applications

Facilities

Network & Transport

Access

Security

Diagnostic

Applications

Facilities

Network & Transport

Access

Security

I have a C-ITS certificate

You can do C-ITS activities

Proof: valid C-ITS Application

Certificate

Policy
Security: Authentication / Authorization

I have a Fleet Management certificate

I’m owned by the right fleet owner

Valid fleet management device

Policy

Ownership

Proprietary stack (security & translation)
Security: Authentication / Authorization

Proprietary stack (security & translation)

Management
- Network & Transport
- Access

Facilities
- Security

Applications
- CV/C-ITS
- Policy
- Ownership

Protected fleet management device

Fleet Management activities

You can do Fleet Management activities

I have a Fleet Management certificate

I’m owned by the right fleet owner

Valid fleet management device

Management
- Network & Transport
- Access

Security

Applications
- Facilities

You have a Fleet Management certificate and you are owned by the right fleet owner.
Proprietary stack (security & translation)

Management

Network & Transport

Access

Security

Applications

Facilities

Network & Transport

Access

Security

Applications

Insurance

Network & Transport

Access

Security

Applications

Diagnostic

Facilities

Network & Transport

Access

Security

Applications

CV/C-ITS

Facilities

Network & Transport

Access

Security

I have a Diagnostics certificate

Valid diagnostic device

Policy

Ownership

autocare

Independence drives us.
Security: Authentication

Authentication

Authorization

Proprietary stack
(security & translation)

Management

Network & Transport

Access

Facilities

Security

Applications

Diagnostic

Policy

Valid diagnostic device

I have a Diagnostics certificate

I’m owned by the right repair shop

Ownership
I have a Diagnostics certificate

I’m owned by the right repair shop

… and I’m right next to you

Valid diagnostic device

Policy

Ownership
Security: Authentication, Authorization

You can do Diagnostic activities

I have a Diagnostics certificate

I’m owned by the right repair shop

... and I’m right next to you

Valid diagnostic device

Policy

Ownership

Proprietary stack (security & translation)

Management

Network & Transport

Access

Facilities

Security

Applications

Access

Network & Transport

Facilities

Security

Applications

CV/C-ITS

Management

Facilities

Applications

Network & Transport

Access

Security

Applications

Diagnostic

Insurance

Fleet Mngt

CV/C-ITS
ISO 21177

- Uses internet-standard secure communications protocol, Transport Layer Security (TLS) 1.3
- Enables use of C-ITS (IEEE 1609.2) certificates to directly state permissions
  - More appropriate than identity-based permissions in Mobile Ad Hoc Network (MANET) setting
- Allows each party to present a series of certificates to establish a detailed “authorization state” with the other party
- Becoming adopted by application standards
  - SAE J2945/3 – authenticate / authorize weather reporting applications
Requirements

- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting
Requirements

• Secure sessions – confidentiality, integrity, authorization, anti-replay

• Each party can establish the permissions of the other

• Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party

• A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting
Requirements

- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting
Requirements

- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting
Requirements

- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within another secure session so eavesdroppers learn nothing, not even what application is acting
Security: Authentication / Authorization

• Policy authorities and certificate authorities are already being established to support C-ITS

• This organizational structure can also support authentication and authorization for SVI

• OEMs can enforce reasonable security policies on certificate issuance and freshness
  • OEM security concerns are real and must be taken into account

• However, in this model OEMs are not real-time gatekeepers of access to the information
  • Nevertheless, their security requirements are met