CEN/TC 278 PT1605

Webinar #1 Session 5

Security

(15:15-16:00)

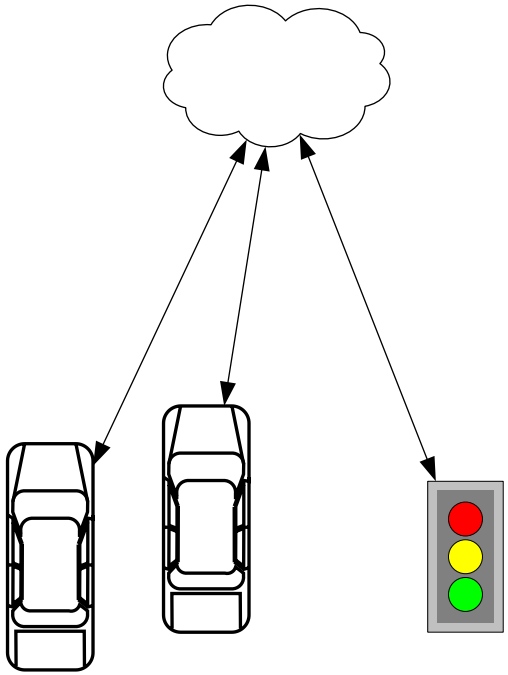
William Whyte

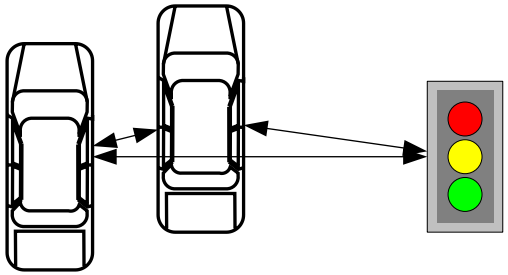
Agenda webinar #1

- **Session 1**: 13:10 – 13:25
  C-ITS standardization landscape (TR 21186-1)
- **Session 2**: 13:25 – 14:00
  Hybrid communications for C-ITS service deployment
  (TR 21186-2, TS 17496)
- **Session 3**: 14:00 – 14:15
  Generic position, velocity and time information for C-ITS services (TS 21176)
- **Break**: 14:15 – 14:30
- **Session 4**: 14:30 – 15:15
  Generic access to sensor and control data for C-ITS services (TS 21184)
- **Session 5**: 15:15 – 16:00
  Cybersecurity for C-ITS services (TS 21177, TR 21186-3)
- Questions and discussions: 16:00 – 17:00

Subsequent webinars will present in more detail these technologies.

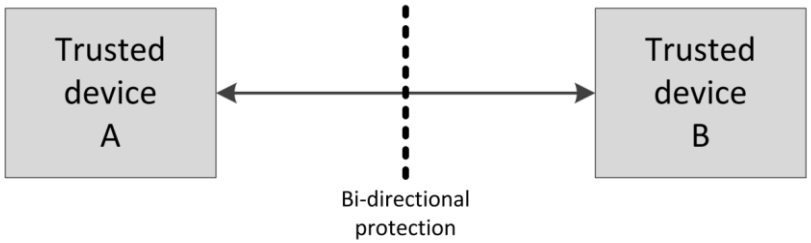
Communications topologies





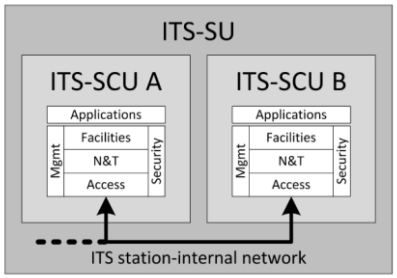
The basic situation

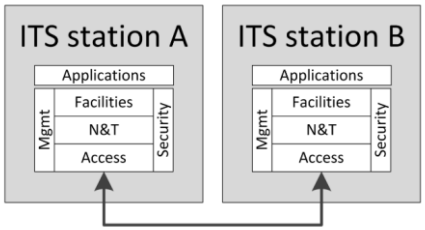
- Two devices cooperate in a trusted way, i.e. exchange information in secure application sessions.



Examples of secure application sessions

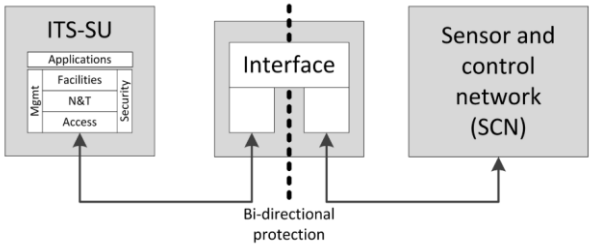
Secure ITS station management (ISO 24102-4)



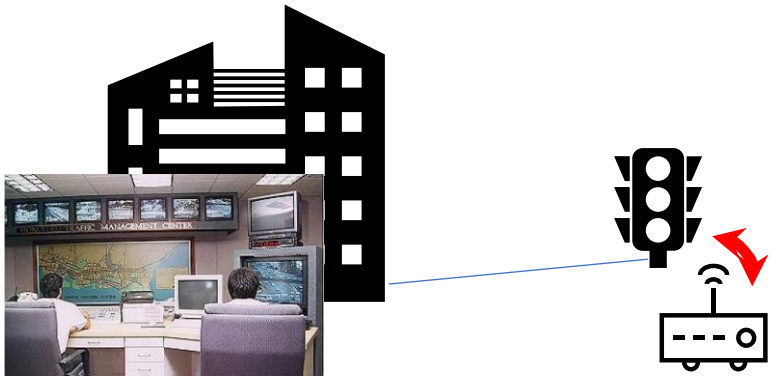


Secure application sessions between ITS station units

Secure access to sensor and control networks



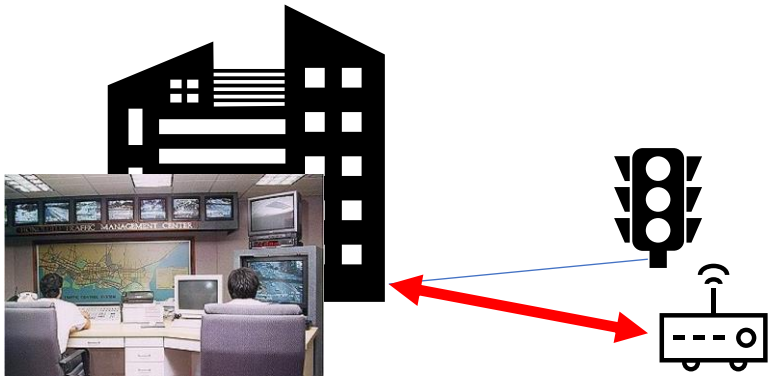
Use Cases (1)



Attaching an RSU to a Signal Controller

- Is this a valid RSU?
  - Is it entitled to run the indicated RSU apps?
- Is it owned by the traffic management system?
- Is it the actual RSU that's physically present?

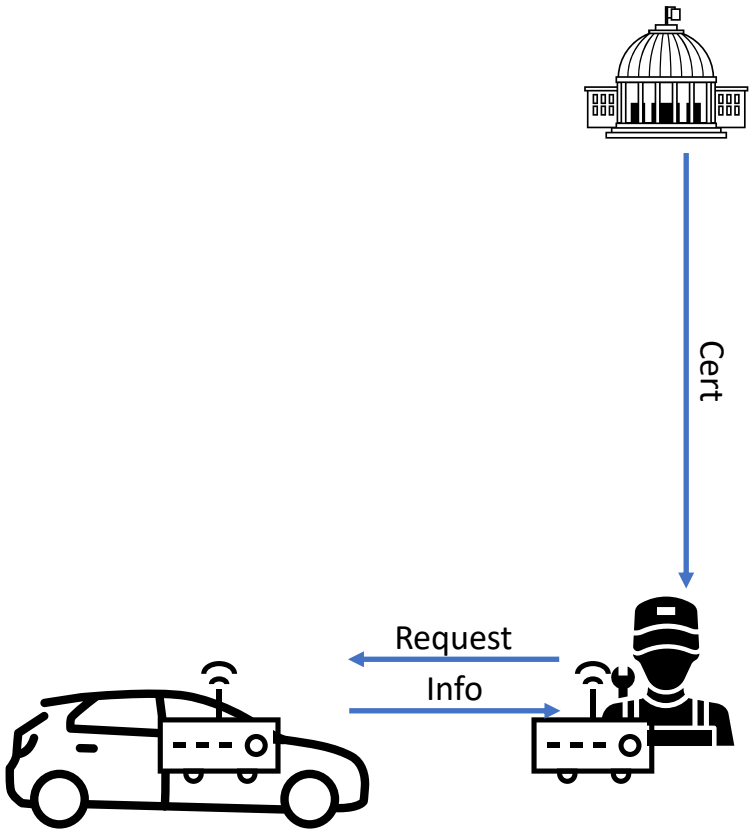
Use Cases (2)



Connecting an RSU to a TMC

- Is this a valid RSU?
  - Is it entitled to run the indicated RSU apps?
  - Is it trusted to sign central messages, e.g. TIMs?
- Is it owned by the traffic management system?

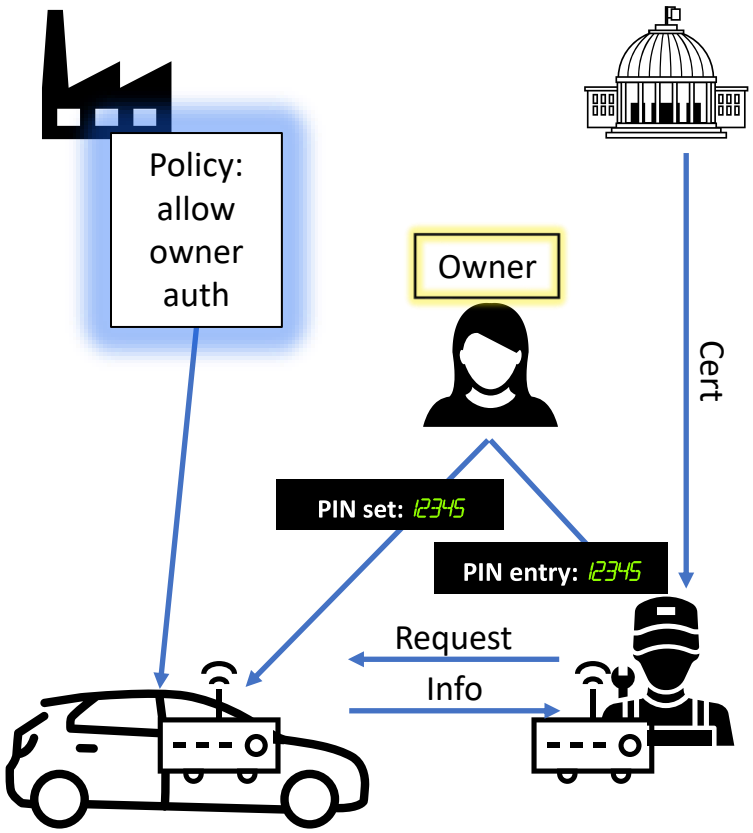
Use Cases (3)



Vehicle diagnostics

- Connect authorized diagnostic device to vehicle
  - What is it entitled to access?
- Ensure that the device accessing the vehicle is the one present

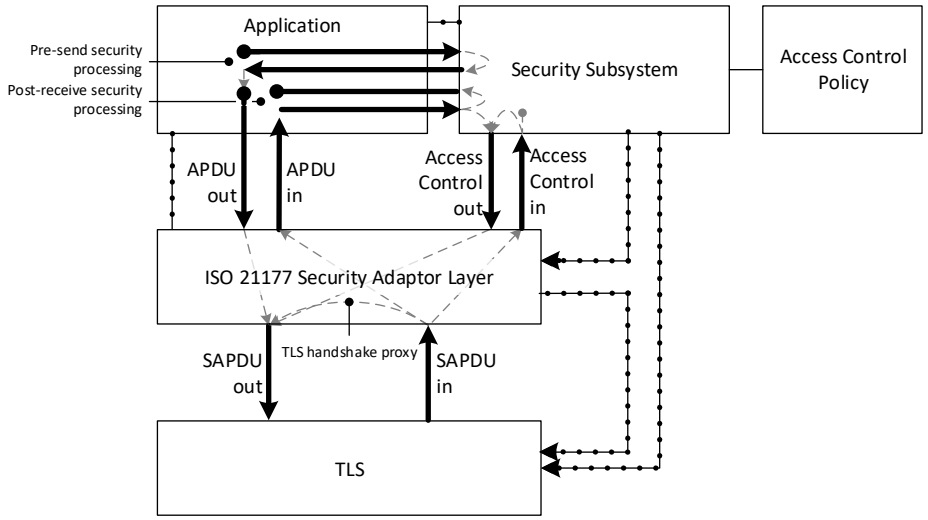
Use Cases (3)



Vehicle diagnostics

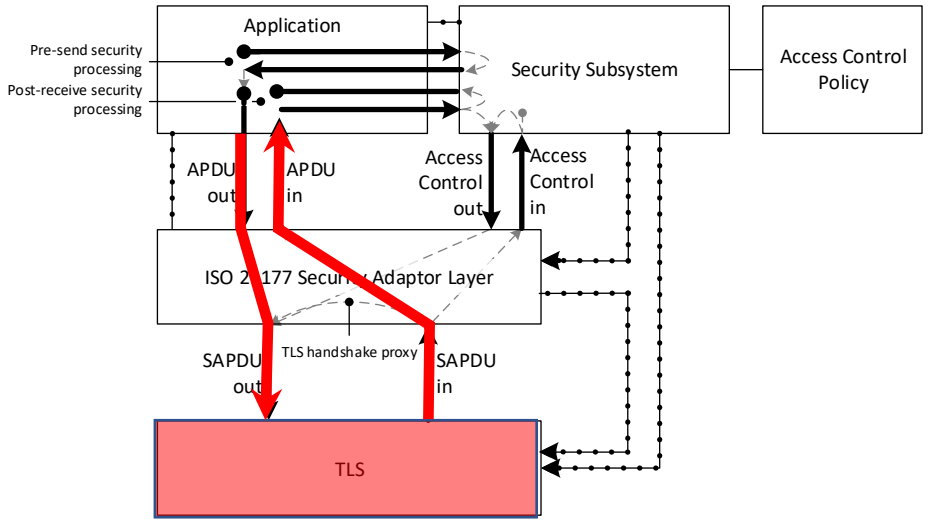
- Connect authorized diagnostic device to vehicle
  - What is it entitled to access?
- Ensure that the device accessing the vehicle is the one present

Requirements



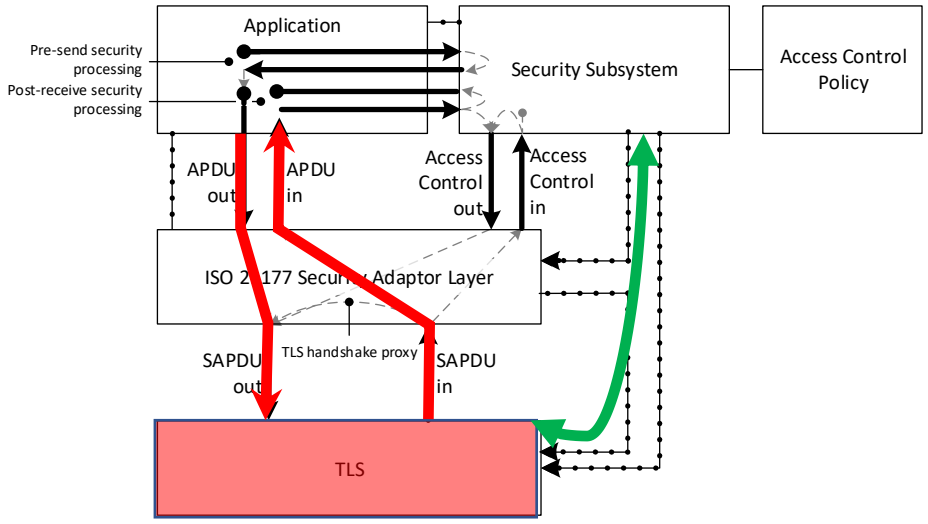
- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within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

Requirements



- Secure sessions – confidentiality, integrity, authorization, anti-replay
  - IETF TLS
  - 1.3 -- https://tools.ietf.org/html/rfc8446
- 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

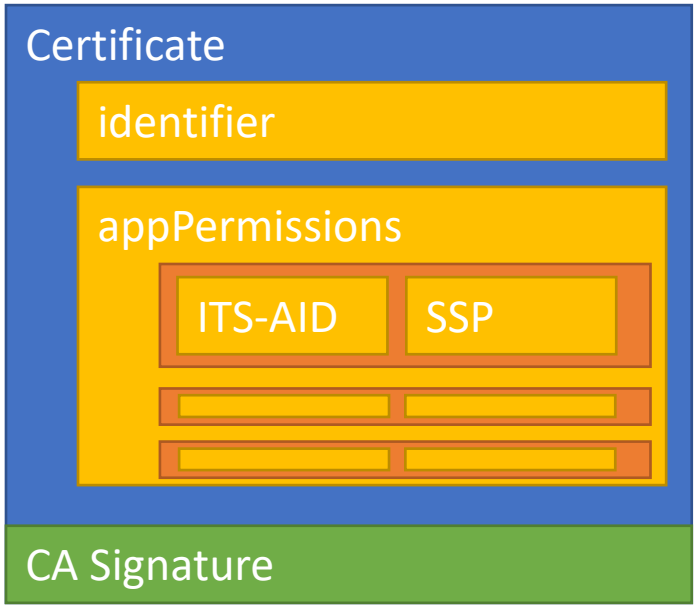
Requirements



- 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

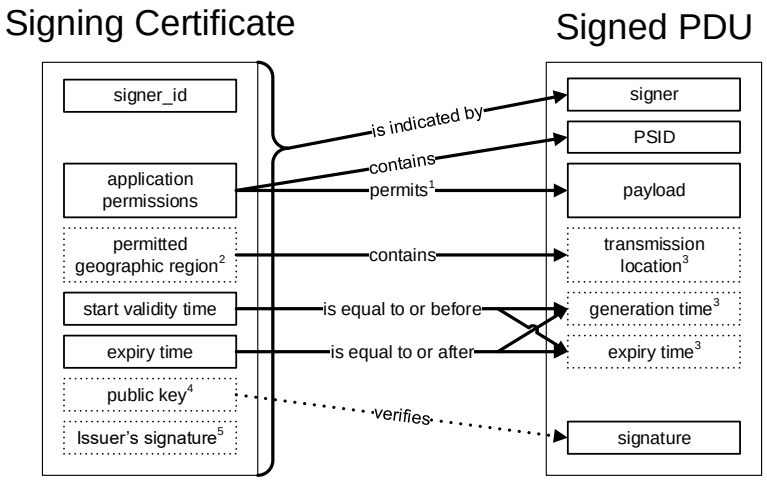
IEEE 1609.2 Certificates

- “Attribute certificates” – transmit authorizations, not identities
- Authorizations are indicated by ITS-AID and Service Specific Permissions (SSP)
  - ITS-AID identifies the “application domain”
    - Send Basic Safety Message
    - Tolling
    - Signal Phase and Timing
    - Advertise other services
    - Weather reporting
    - …
  - SSP: additional ITS-AID-specific authorization statements
    - Roles within application
    - Weather-related road management: center / vehicle
- Managed by IEEE and ISO, jointly



Consistency between signed SPDU and signing certificate

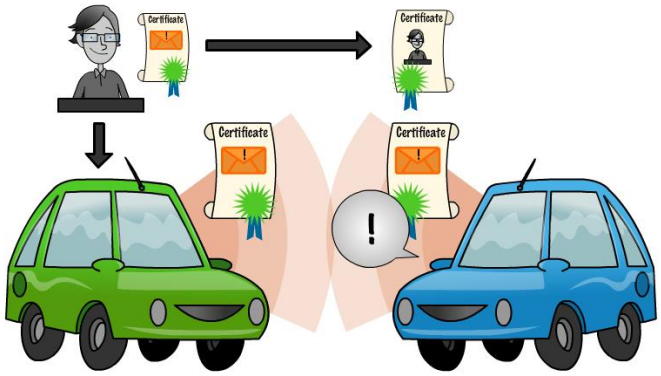
- Certificate contains a set of statements
  - Where I'm allowed to operated
  - What I'm allowed to do
  - Validity period of cert
- Receiver checks that message (PDU – protocol data unit) is consistent with certificate and rejects otherwise



NOTES:
1. Determined using the PSID and SSP. The process to determine whether the operational permissions permit the message payload is specified by the organization reserving the PSID and is out of scope for this standard.
2. Included per policy set by the appropriate authority for the region where the certificate is being used.
3. Optional. Inclusion of this data is as determined by the organization reserving the PSID. This data may be contained in the payload or within the security header fields.
4. For implicit certificates, the public key is derived rather than explicitly stated within the certificate.
5. Not included in an implicit certificate.

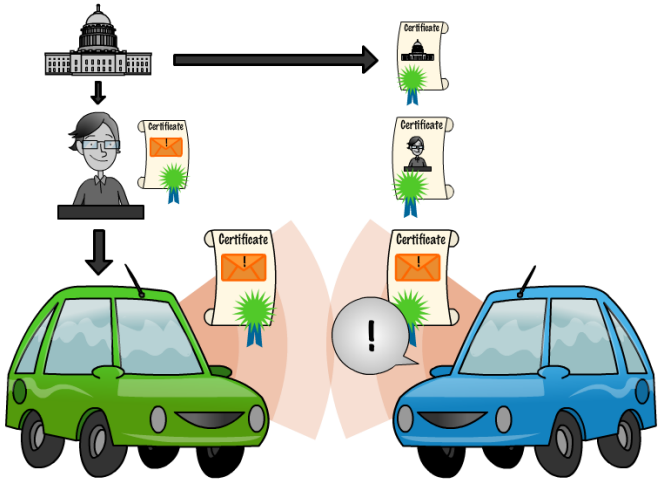
Using credentials (1)

- The certificate is issued by a certificate authority (CA) which is responsible for checking that the sender is entitled to the certificate
- The CA has a certificate itself which it binds cryptographically to the device's certificate
- The receiver knows the CA certificate
  - Checks that the CA certificate authorizes and is bound to the device's certificate
  - Checks that the device's certificate authorizes and is bound to the message
  - Trusts the message!

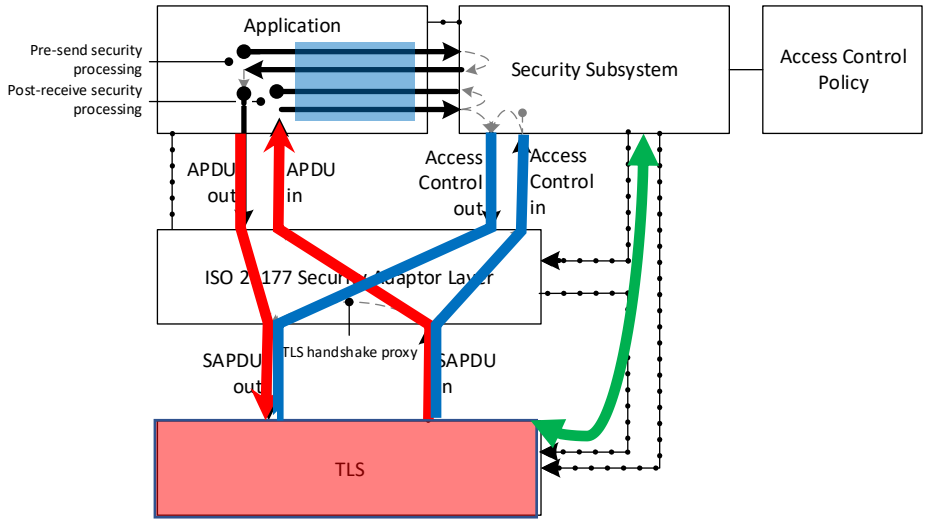


Using credentials (2): PKI

- How does the receiver know the CA certificate?
- CA certificate might be known already
- If it's new, the receiver can construct a trust chain back to a root CA.
- There's a relatively small set of root CAs
  - These can authorize an arbitrarily large number of intermediate and end-entity CAs
- Root CA management is out of scope for this presentation

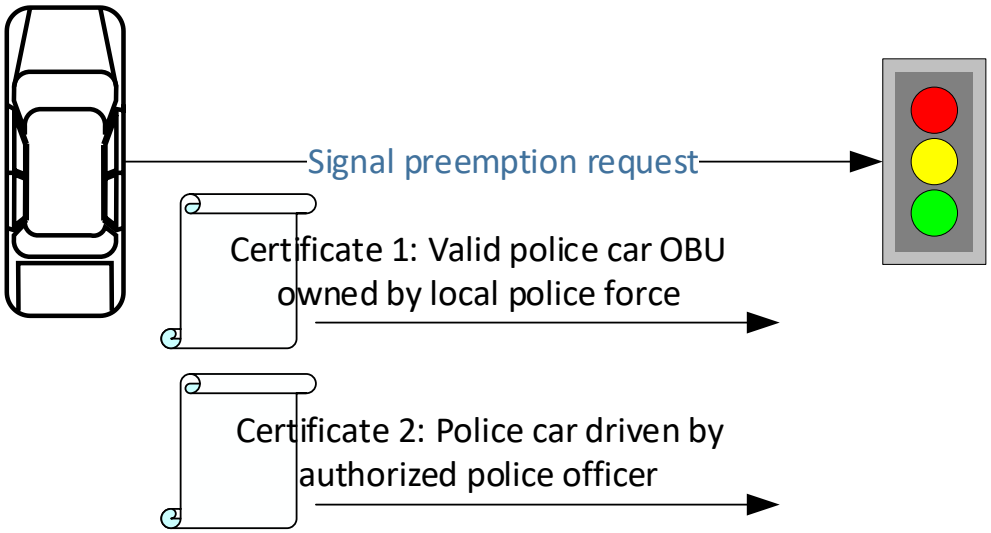


Requirements

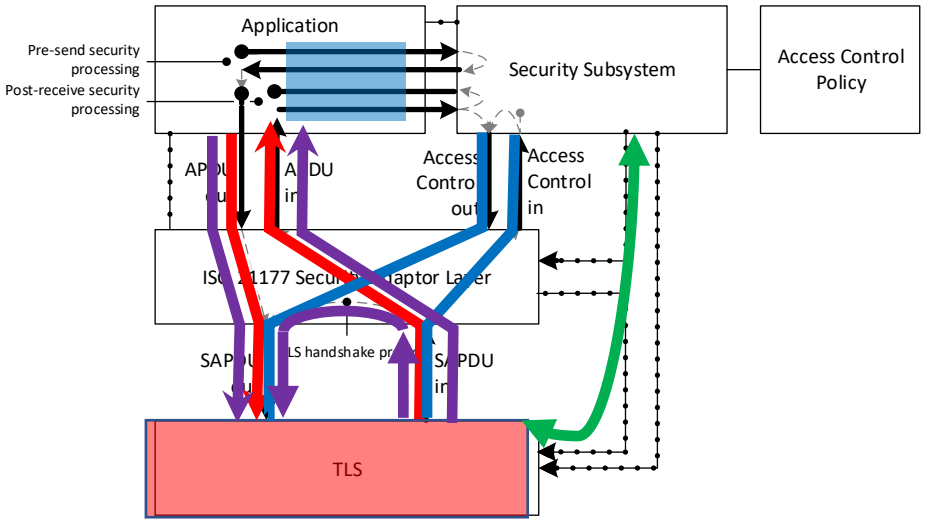


- Secure sessions – confidentiality, integrity, authorization, anti-replay
- Each party can establish the permissions of the other
- Each party can present multiple authorization statements and maintain “authorization state” with respect to the other party
- A secure session can be bootstrapped within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

Multiple certificates example



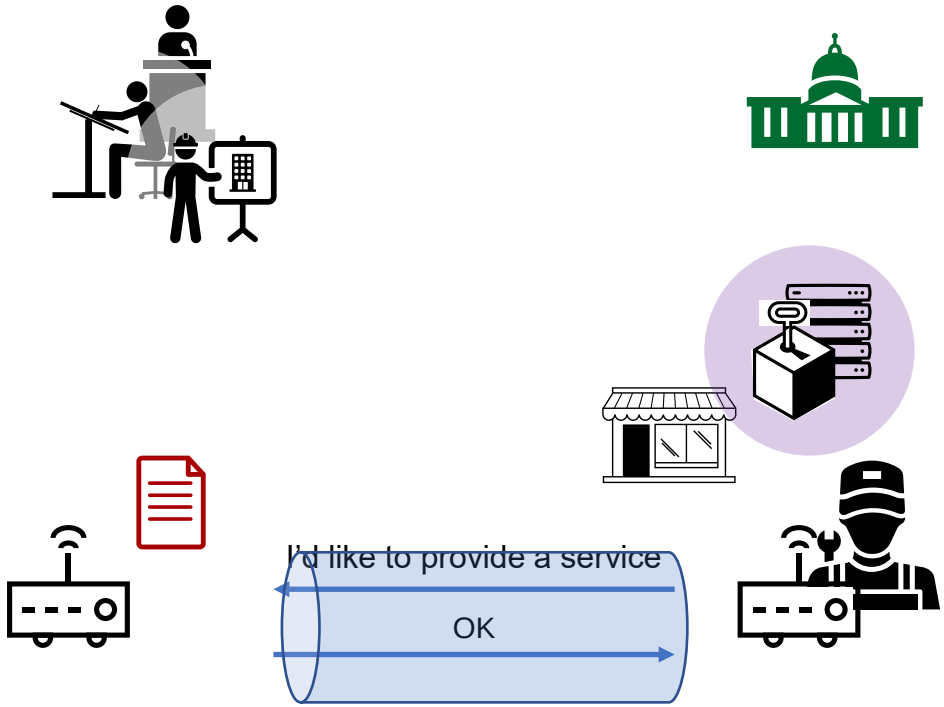
Requirements



- 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

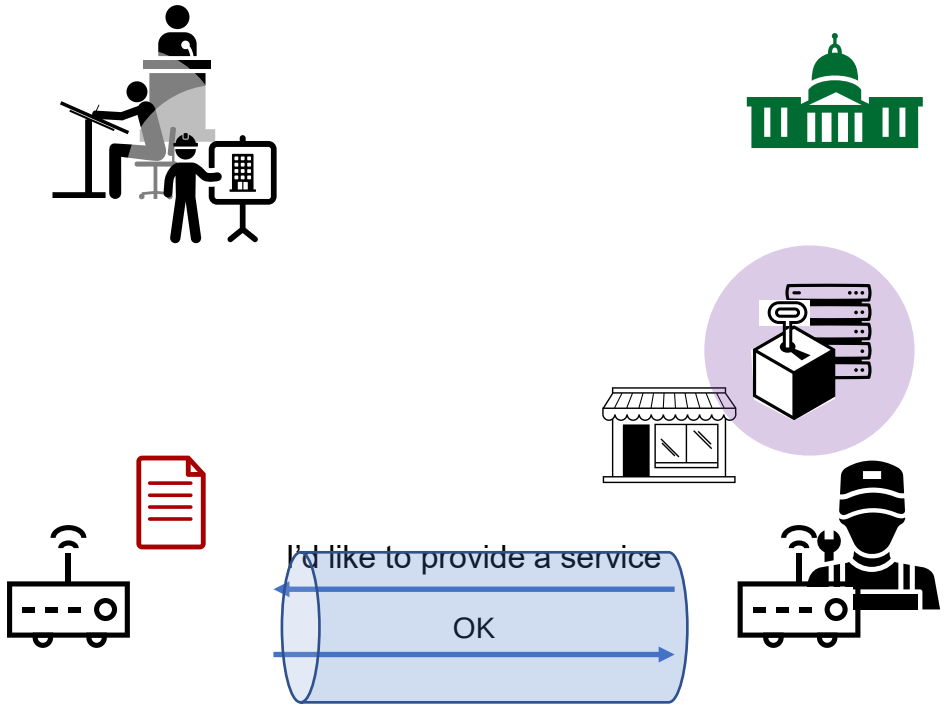
What needs to be defined for this to be done securely?

- Interface protocol specification
- Access control policy
- Data management policy
- Certificate issuance policy
- Governance



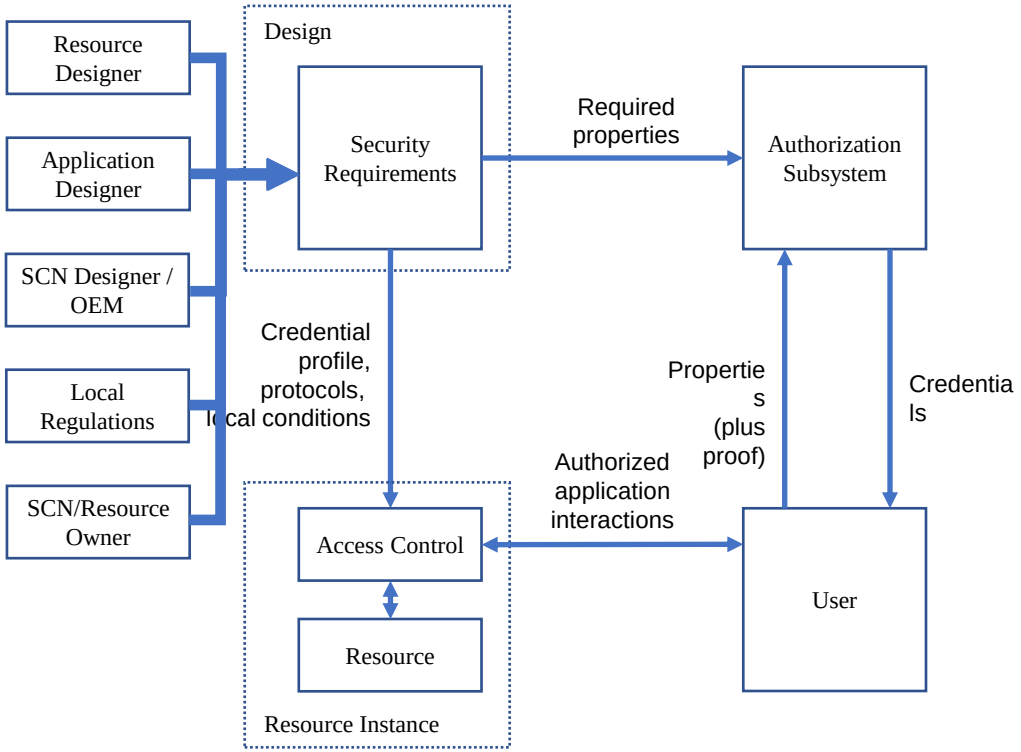
What needs to be defined for this to be done securely?

- Interface protocol specification
  - ISO TS 21177
- Access control policy
- Data management policy
- Certificate issuance policy
- Governance



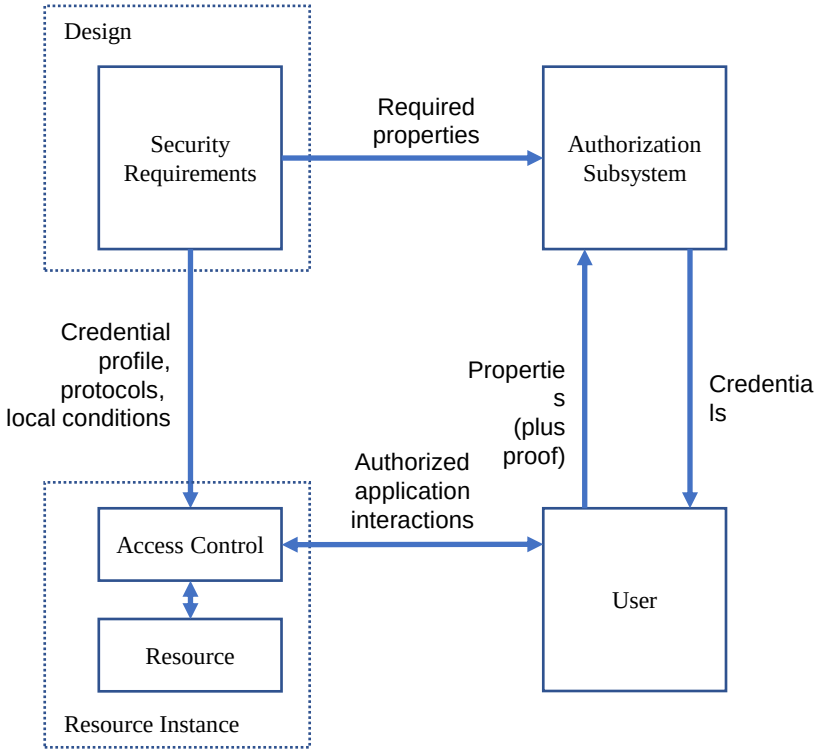
ISO 21177 overall architecture: four Actors

- **DESIGN**
  - Multiple stakeholders working together or independently
  - Sets security requirements:
    - Access requirements enforced by access control
    - Security requirements the User must meet to get access
  - Communicates requirements to Authorization Subsystem and to Access Control for enforcement, to developers of User for implementation
- **AUTHORIZATION SUBSYSTEM**
- **USER**
- **RESOURCE INSTANCE**



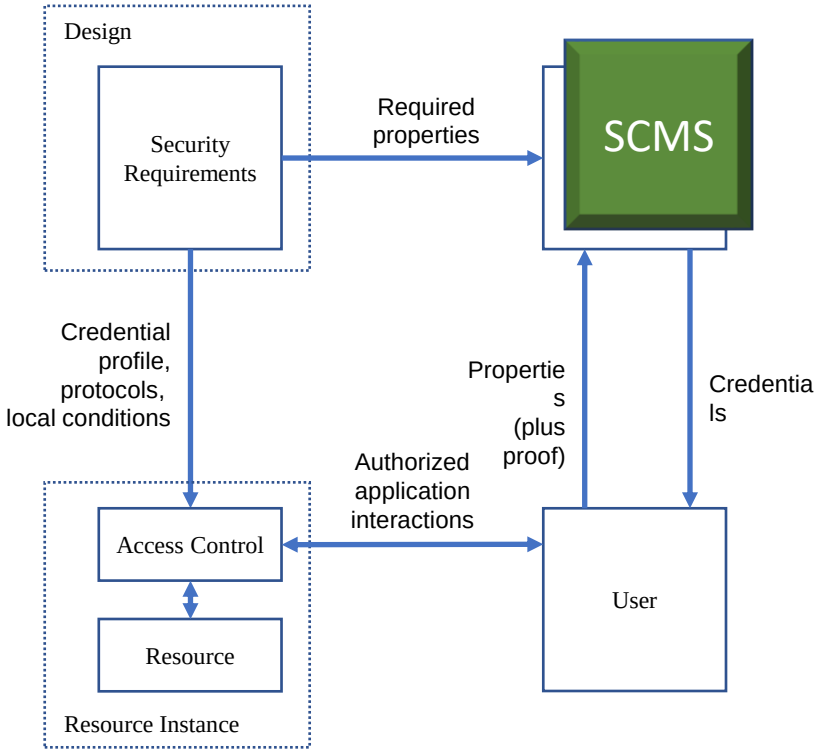
ISO 21177 overall architecture: four Actors

- **DESIGN**
- **AUTHORIZATION SUBSYSTEM**
  - Issues credentials to Users
  - Credentials are a trustworthy statement that the User matches the properties required by the Designers and is entitled to the requested permissions
  - Example: SCMS, X.509 CA, …
- **USER**
- **RESOURCE INSTANCE**



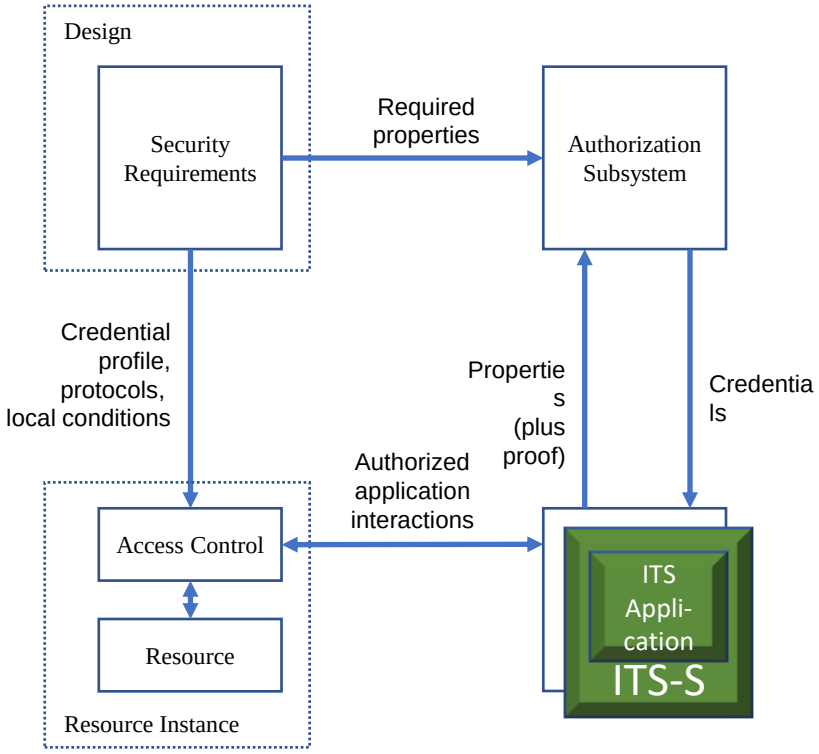
ISO 21177 overall architecture: four Actors

- **DESIGN**
- **AUTHORIZATION SUBSYSTEM**
  - Issues credentials to Users
  - Credentials are a trustworthy statement that the User matches the properties required by the Designers and is entitled to the requested permissions
  - Example: SCMS, X.509 CA, …
- **USER**
- **RESOURCE INSTANCE**



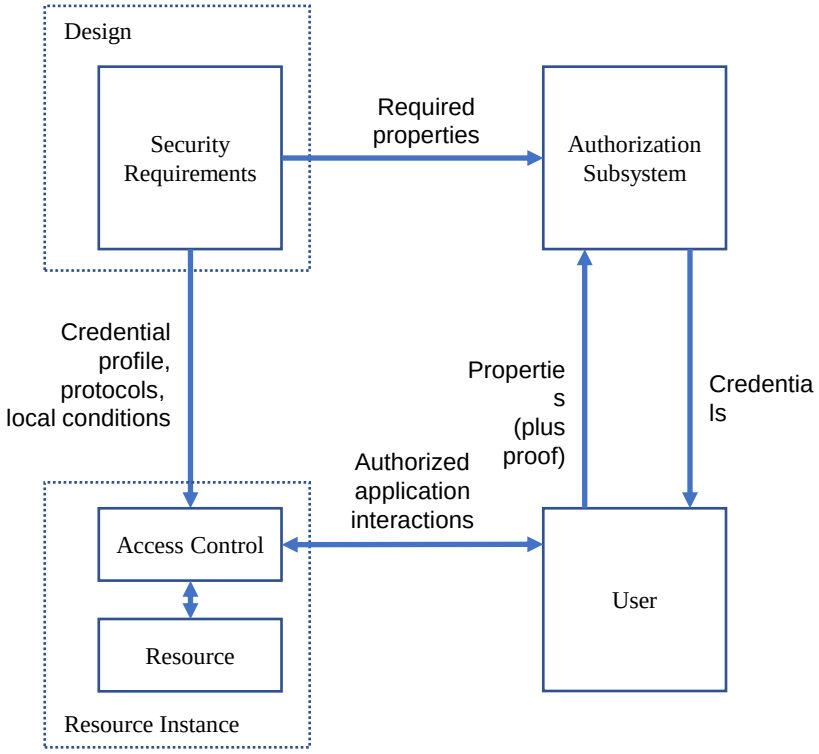
ISO 21177 overall architecture: four Actors

- **DESIGN**
- **AUTHORIZATION SUBSYSTEM**
- **USER**
  - A trusted application running on a trusted device
  - For example, an ITS Application running on an ITS Station
  - The Authorization Subsystem is responsible for establishing that the device and application are trusted for the specified interactions according to the requirements set by Design
- **RESOURCE INSTANCE**



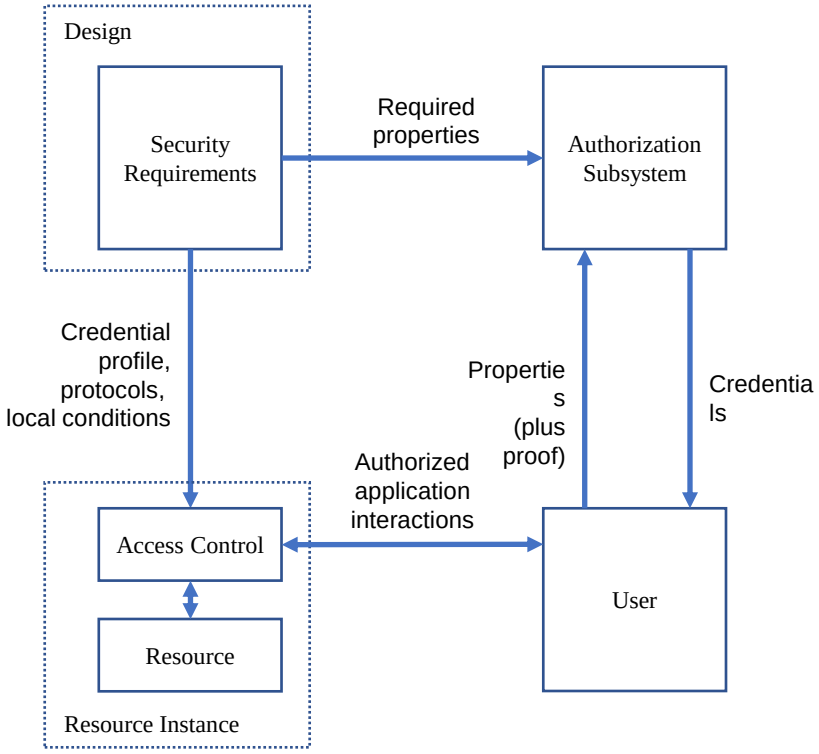
ISO 21177 overall architecture: four Actors

- **DESIGN**
- **AUTHORIZATION SUBSYSTEM**
- **USER**
  - A trusted application running on a trusted device
  - For example, an ITS Application running on an ITS Station
  - The Authorization Subsystem is responsible for establishing that the device and application are trusted for the specified interactions according to the requirements set by Desgin
- **RESOURCE INSTANCE**



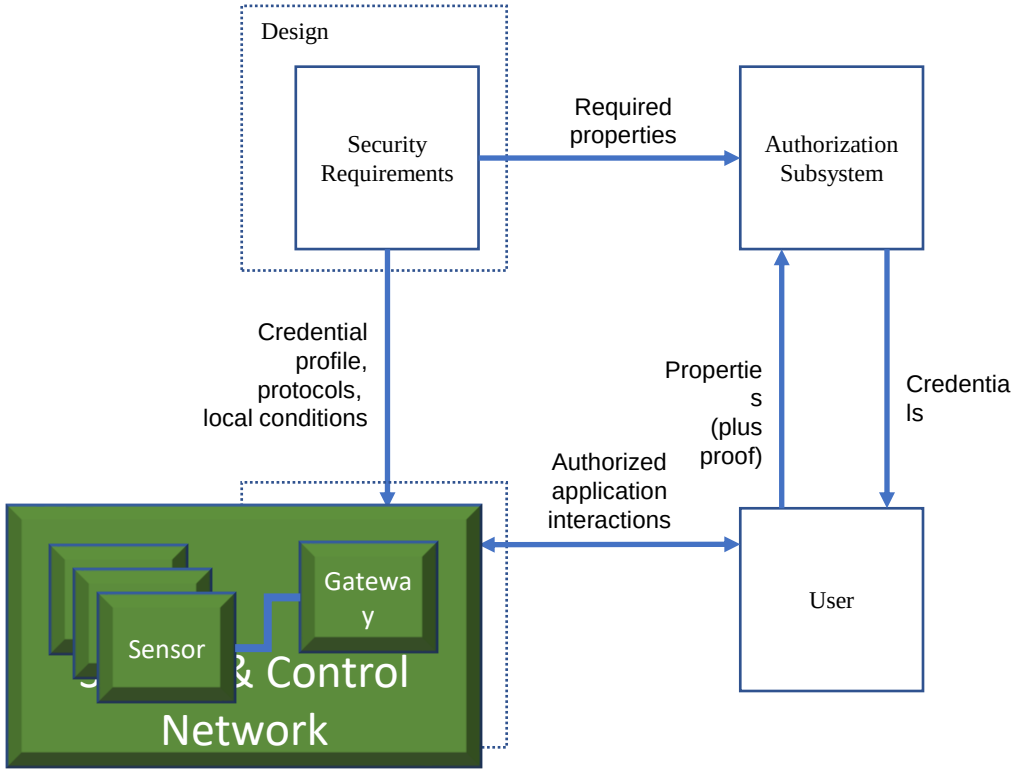
ISO 21177 overall architecture: four Actors

- **DESIGN**
- **AUTHORIZATION SUBSYSTEM**
- **USER**
- **RESOURCE INSTANCE**
  - The combination of Access Control and the resource itself
  - Access Control enforces the access rules provided by Design
  - One instance of Access Control may control access to multiple resources
  - Access Control also prioritizes access among multiple users
  - Example: Access Control is the Gateway and Resource is a Sensor in a Sensor & Control Network



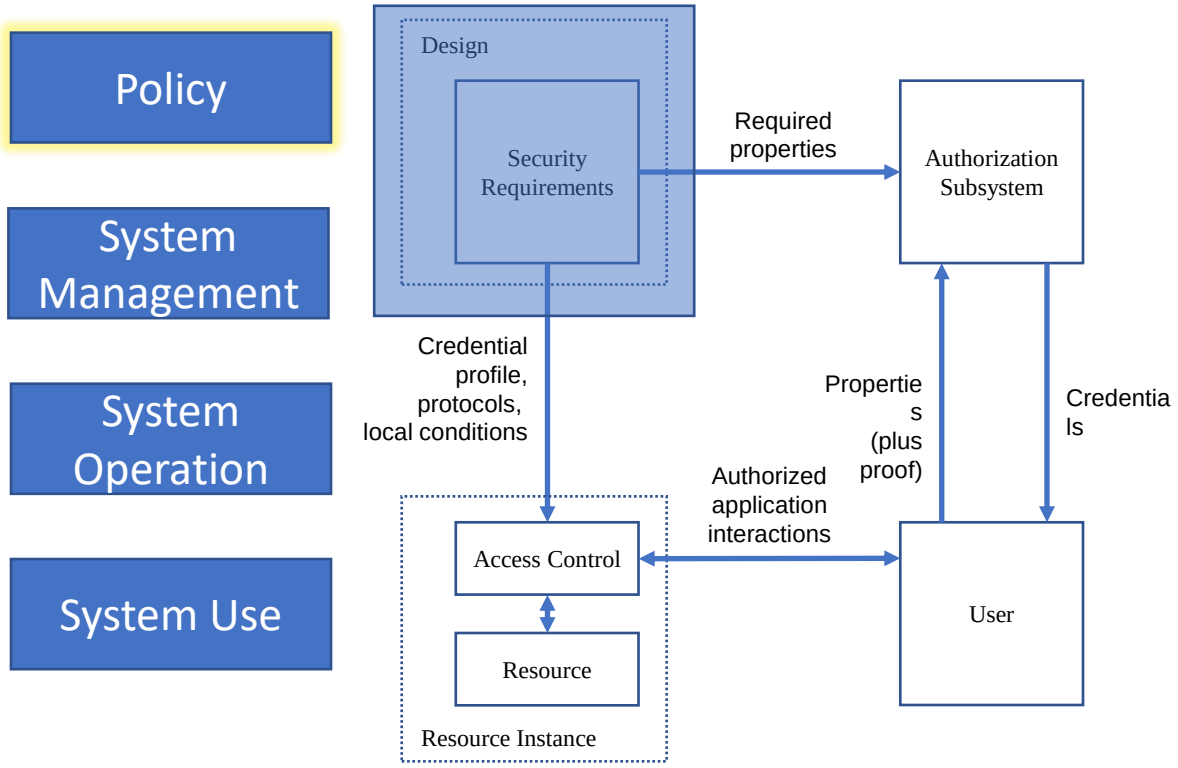
ISO 21177 overall architecture: four Actors

- **DESIGN**
- **AUTHORIZATION SUBSYSTEM**
- **USER**
- **RESOURCE INSTANCE**
  - The combination of Access Control and the resource itself
  - Access Control enforces the access rules provided by Design
  - One instance of Access Control may control access to multiple resources
  - Access Control also prioritizes access among multiple users
  - Example: Access Control is the Gateway and Resource is a Sensor in a Sensor & Control Network



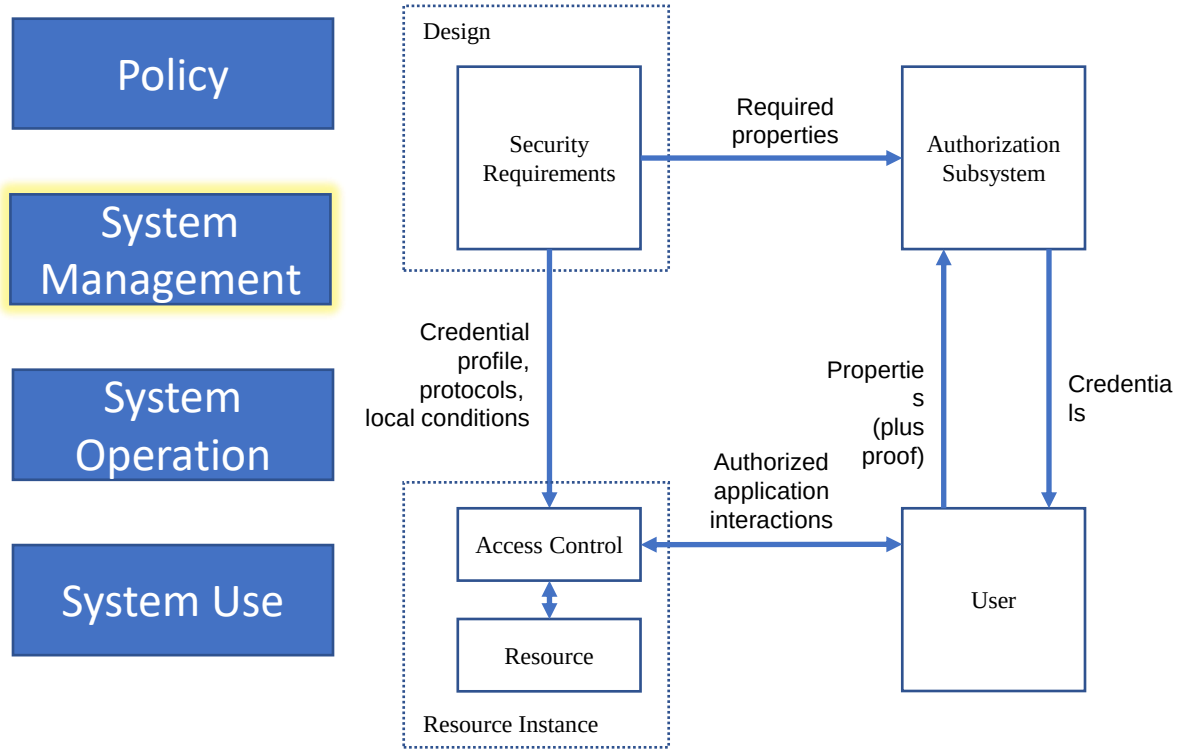
Governance and operations

- Policy
  - Includes Design decisions
  - Also includes governance – who has a seat at the table to make Design decisions
  - Medium-sized group, very active when a service group is being created, meets rarely after that



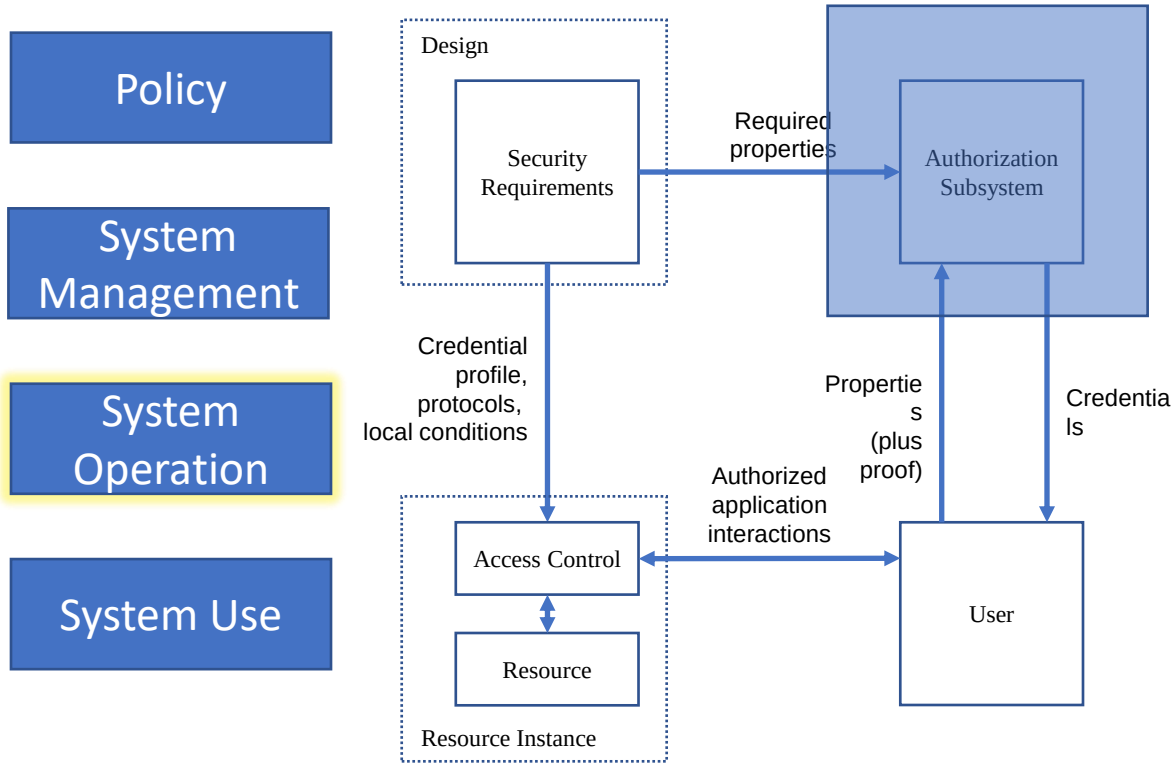
Governance and operations

- Policy
- System Management
  - Appoints top-level service providers
    - Root CA, …
  - Accredits others
    - Test labs, …
  - ISAC
  - Small group, oversight role, meets occasionally (ISAC may meet more frequently)



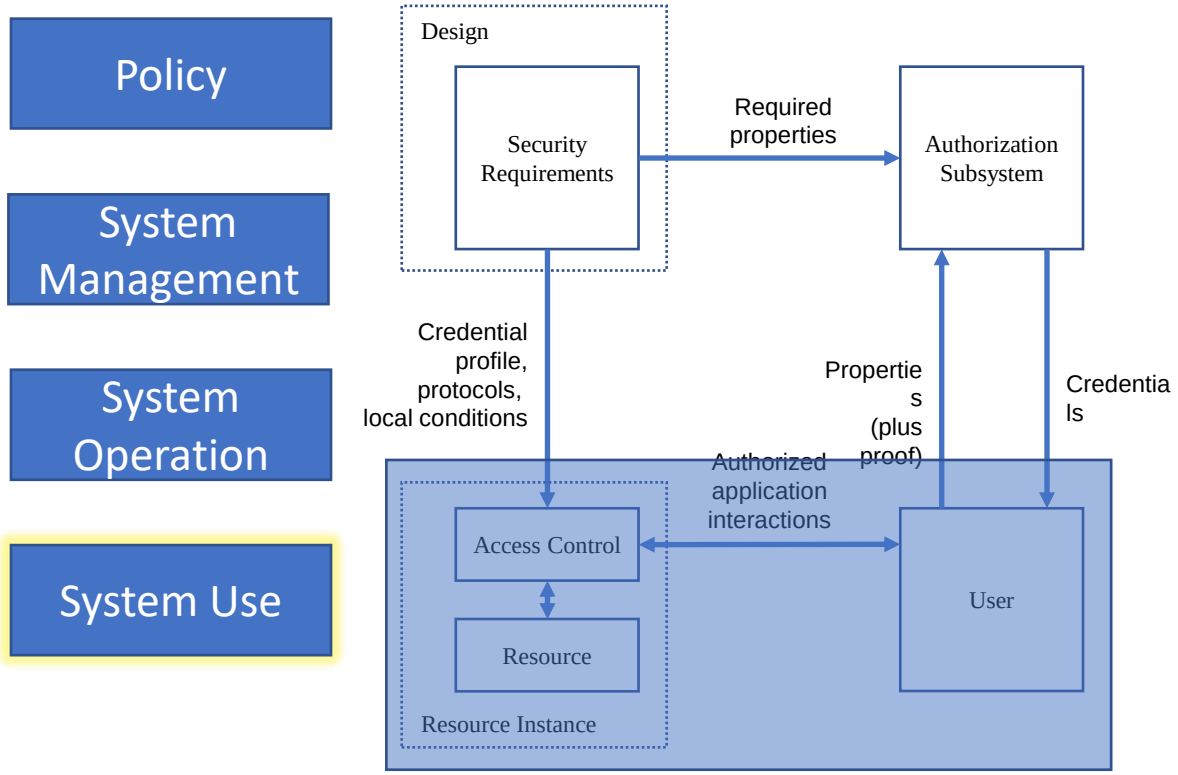
Governance and operations

- Policy
- System Management
- System operation
  - The CAs, test labs, revocation authorities …, that on a day-to-day basis ensure the correct operation of the system
  - Large group, continuous operations



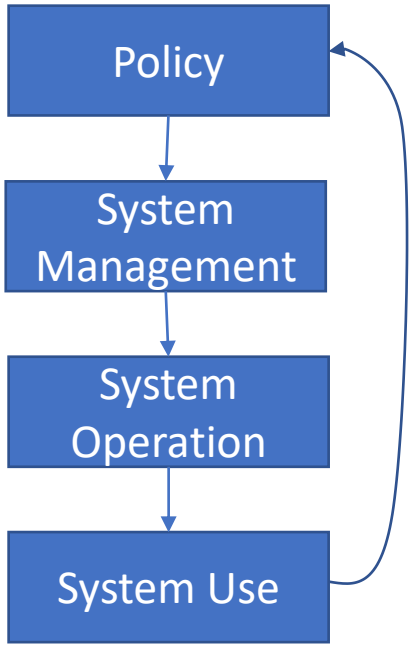
Governance and operations

- Policy
- System Management
- System operation
- System use
  - Users and resources that carry out the operations of value to system participants
  - Also includes suppliers



Governance and operations: lifecycle

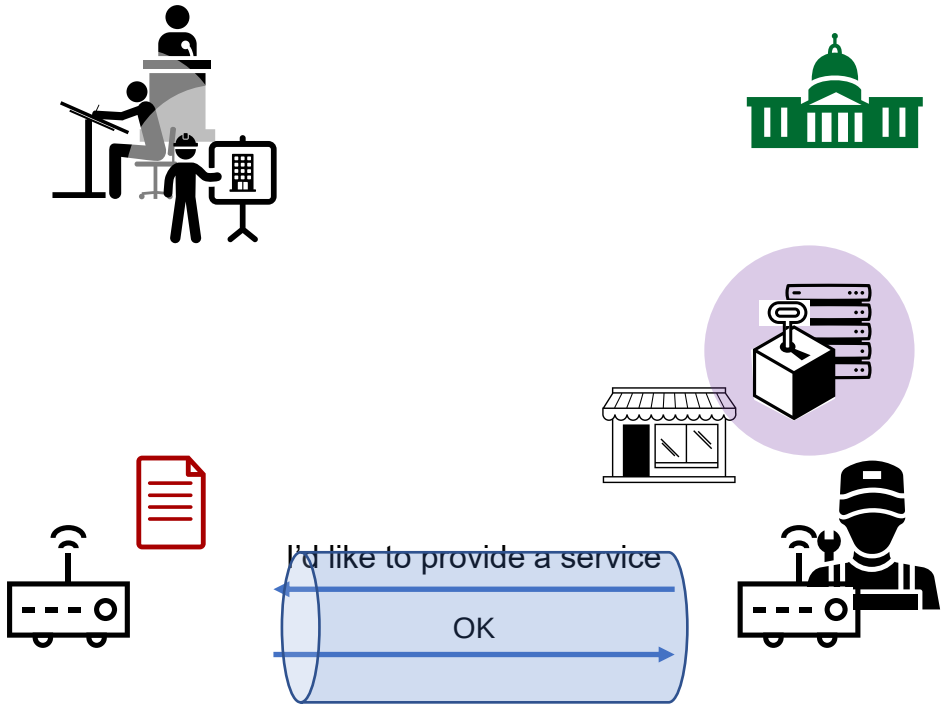
- Key stakeholders develop governance plan that includes mechanism to add stakeholders
- Initial group of stakeholders creates initial policy, stands up system management group
- System Management group accredits / engages appropriate actors within System Operation
- System Use actors engage with System Management group to get credentials
- System Use actors carry out system activities
- If it becomes apparent that policy needs to be modified, the Policy group meets and flows an amended policy down to System Management



What needs to be defined for this to be done securely?

- Interface protocol specification
- Access control policy
- Data management policy
- Certificate issuance policy
- Governance

- Now we can provide the service!



21177 implementation considerations: 21186-3

- Extensions to functionality
  - Prolong the lifetime of sessions beyond the lifetime of the certificates that started the session
  - Allow parties to establish the revocation status of certificate authorities
  - Introduce concept of an “owner” who can actively approve or reject access requests
- Complete specifications that define the deployment environment
  - How to develop an access control policy + example
    - Based on ISO 21184
  - Security requirements for platforms running ISO 21177
    - ITS Data Exchange (IDX) devices
  - Certificate policy for issuing certificates to IDX devices

Summary of the ‘Protection Profile’ Material (Section 4)

- ITS-Station analyzed for 3 different security/privacy scenarios:
  - 1) **Public Info only** - Device provides access only to public information (no privacy needs)
  - 2) **Privacy-Protected Data** – Device provides access to privacy-protected data
  - 3) **Control/Execute** – Device allows write-access or accepts executable commands that control something
- Representative of three classes of generic ITS-Station for the purposes of threat modeling and deriving broadly applicable Common Criteria Security Functional Requirements (SFR)

Summary of the ‘Protection Profile’ Material (cont.)

- Threat model Analysis (abbreviated Common Criteria process):
  - Defined each scenario’s risks
  - Mapped risks to Security Objectives
  - Map Security Objectives to CC SFRs
- Certain assumptions were made
  - E.g., even ‘public data’ needs integrity protection
- Did not delve into CC Security Assurance Requirements (these levels will be industry/gov’t policy-based most likely)
- Result:
  - A ‘skeleton’ Protection Profile for each scenario
  - A side-by-side comparison of generic ITS-S security functions needed based on the type of data they handle

Why the Protection Profile Material?

- Provide ITS security practitioners a ‘starting point’ from which to build real Protection Profiles
  - Assumptions can be modified based on real-life data sensitivity
  - Scenarios are additive, e.g., most devices will handle some combination of the 3 scenarios’ data sensitivities
  - SFRs for each easily reconciled or added to

Summary of the 21186-3 Certificate Policy Material (Section 8)

- Flagged specific threats to the C-ITS PKI. Threats included:
  - Compromised Trust List Manager (TLM)
  - Compromised CA
  - Wrong permissions in Certs
  - Exploitation of bootstrapping and enrolment processes
  - Exploitation of revocation processes
  - Compromised crypto
  - Compromised end entity identity
  - CRL dissemination problems
- For each threat, included recommended countermeasures that may be considered for implementation in:
  - Certificate Practice Statements
  - Other Security Policy and Procedures documents applicable to PKI implementers
- Why?
  - Coverage in the C-ITS Certificate Policy is broad and has gaps in terms of actual procedures and practices typically included in Certificate Practice Statements or other organizational controls

Summary of the 21186-3 Certificate Policy Material (Section 8) (cont.)

- Material also addresses current inflexibility of the C-ITS certificate policy to accommodate a range of ITS applications of varying sensitivity
  - E.g., Section 1.6.2 [forbidding use of certificates for anything that could lead directly to death]
  - E.g., Section 6.1.5.2 [mandate for Protection Profiles that may require higher security unneeded for low-sensitivity applications]
  - Recommendation is to provide additional policy requirements that accommodate both higher and lower sensitivity device/applications
- **Rationale for recommended C-ITS certificate policy changes:** If the European C-ITS certificate policy stratified security/privacy/assurance requirements based on application and device sensitivity, MANY C-ITS devices could potentially be less complex and less expensive

Agenda webinar #1

- **Session 1**: 13:10 – 13:25
  C-ITS standardization landscape (TR 21186-1)
- **Session 2**: 13:25 – 14:00
  Hybrid communications for C-ITS service deployment (TR 21186-2, TS 17496)
- **Session 3**: 14:00 – 14:15
  Generic position, velocity and time information for C-ITS services (TS 21176)
- **Break**: 14:15 – 14:30
- **Session 4**: 14:30 – 15:15
  Generic access to sensor and control data for C-ITS services (TS 21184)
- **Session 5**: 15:15 – 16:00
  Cybersecurity for C-ITS services (TS 21177, TR 21186-3)
- Questions and discussions: 16:00 – 17:00

Subsequent webinars will present in more detail these technologies.