ETSI

World Class Standards

# ETSI TC ITS WG5
# SECURITY STANDARDIZATION

SCOTT CADZOW (WG5 CHAIR)

ETSI Presentation to ISO SC27, April 26th 2014

*What is ITS security and why can we say with confidence that we can provide a secure ITS?*

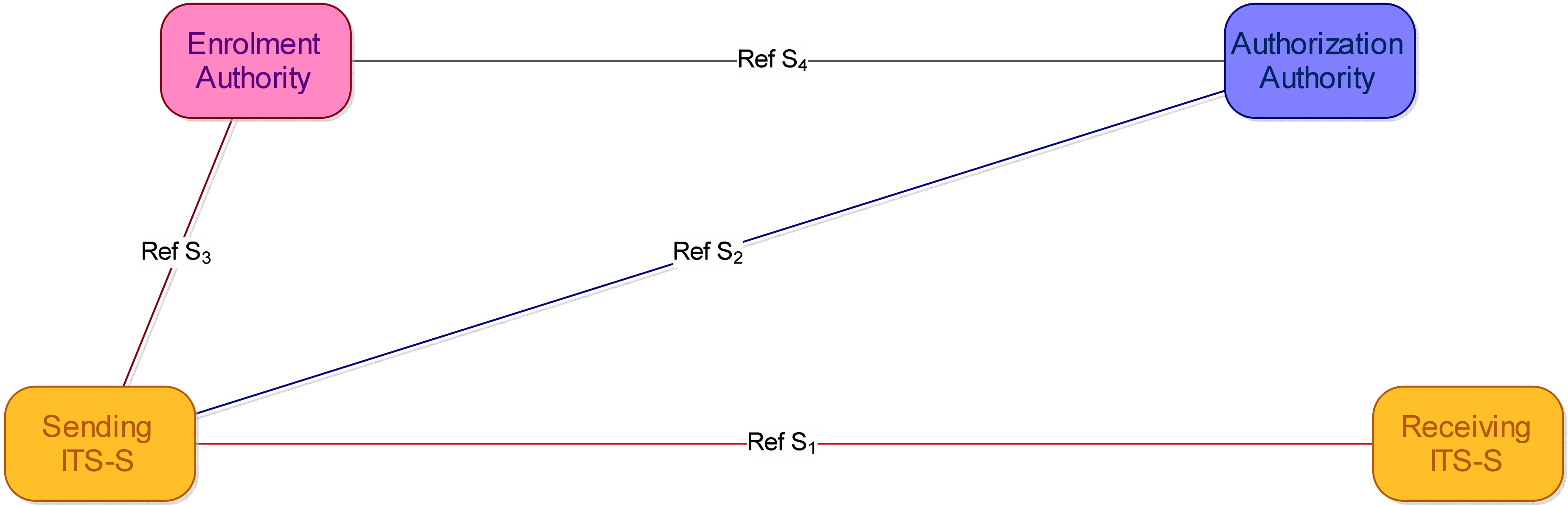
© 2010 – Proprietary Information of ETSI

# ETSI's security model

- Simple model of differentiated authorities
  - Enrolment authority
    - Used as authentication root for the ITS-S identity based on asymmetric cryptography
  - Authorisation authority
    - Authorises individual services pseudonymously based on asymmetric cryptography
  - Consent authority
    - For our extension to enable support of non-repudiation of consent service in DP&P framework working in concert with smart city projects in the EU

# Simplified security architecture

- ComSec architecture
  - Assures support of risk analysed capabilities for CIA model with privacy extensions



# Roles in ITS Security

| Functional element | Role |
|---|---|
| **Enrolment Authority** | Authenticates an ITS-S and grants it access to ITS communications |
| **Authorization Authority** | Provides an ITS-S with authoritative proof that it may use specific ITS services |
| **Sending ITS-S** | Acquires rights to access ITS communications from Enrolment Authority<br>Negotiates rights to invoke ITS services from Authorization Authority<br>Sends single-hop and relayed broadcast messages |
| **Receiving ITS-S** | Receives broadcast messages from the sending or relaying ITS-S |

# Who are the authorities?

- An authority needs to be identified for each application and in some cases the setting of attributes for an application
  - Who do you trust to act as authority for a service?
  - One authority is not a workable model (public safety vehicle versus private vehicle)

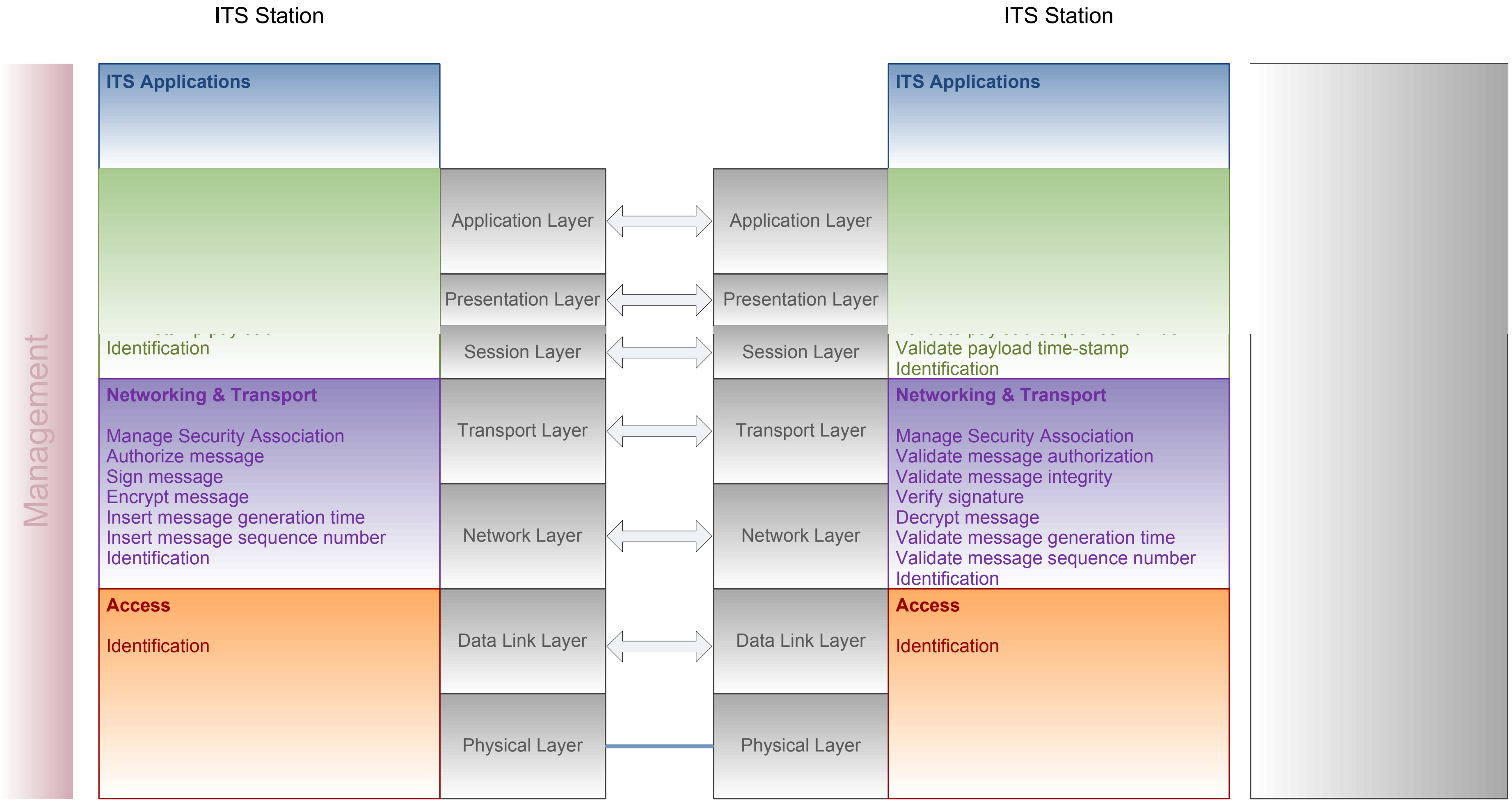
# Which ETSI standards?

- TR 102 892: Risk analysis (TVRA)
- TS 102 940: Security Architecture
- TS 102 941: PKI enrolment and authorisation management protocols
- TS 102 942: Confidentiality
- TS 102 943: Integrity
- TS 103 097: Data model and data definitions

# What the standards allow

- PKI management over reference points $S_3$, $S_2$ and $S_4$
- Secured message transfer over reference point $S_1$
- Underpinned by use of IEEE 1609.2 certificates and key management messages adapted for ITS application in ETSI’s architecture
- Taking input from a wide set of EU projects

# Protocol stacks (from TS 102 940)



# Where to secure a message?

- Proof of source authenticity and authority
  - At source of message
    - CAM for CAM (assertion of state)
    - DENM for DENM (assertion of event)
    - Application to peer application (facility or application layer)
- Digital signature
  - Offers integrity, source authenticity, source authority validated by 3rd party

# The common questions

- Where do I sign a message?
  - Security answer: Where the message is completed
  - Consequence of security answer: same information may be signed many times as it goes up and down the stack as Layer n’s message is relevant only to Layer n
- Purpose of signing  is to assert authority/authenticity/integrity to peer and for the peer to verify the assertion is true

# Other problems to be solved

- Who specifies the PKI?
  - ETSI as an SDO defines the protocols to manage the keys (certificates) that make up the PKI
  - Industry, government, user bodies (i.e. the stakeholders) should do the core definition and building of the infrastructure

# Our workplan and future

- Continuous risk assessment
- Refinement of data model
  - Internationally harmonised with IEEE 1609.2 and intent is to expand harmonisation with ISO, CEN, ITU-T to use ASN.1 modules
- Expansion of PKI model in TS 102 940 (architecture) and TS 102 941 (protocols)
  - Taking input from PRESERVE and others
- Intend to ensure that all security of ITS is only described in the TS 102 94x suite of documents
  - This needs co-operation of all WGs and participant SDOs to succeed