



FOTnet Coordination Day

Frank Kargl | University of Twente | f.kargl@utwente.nl



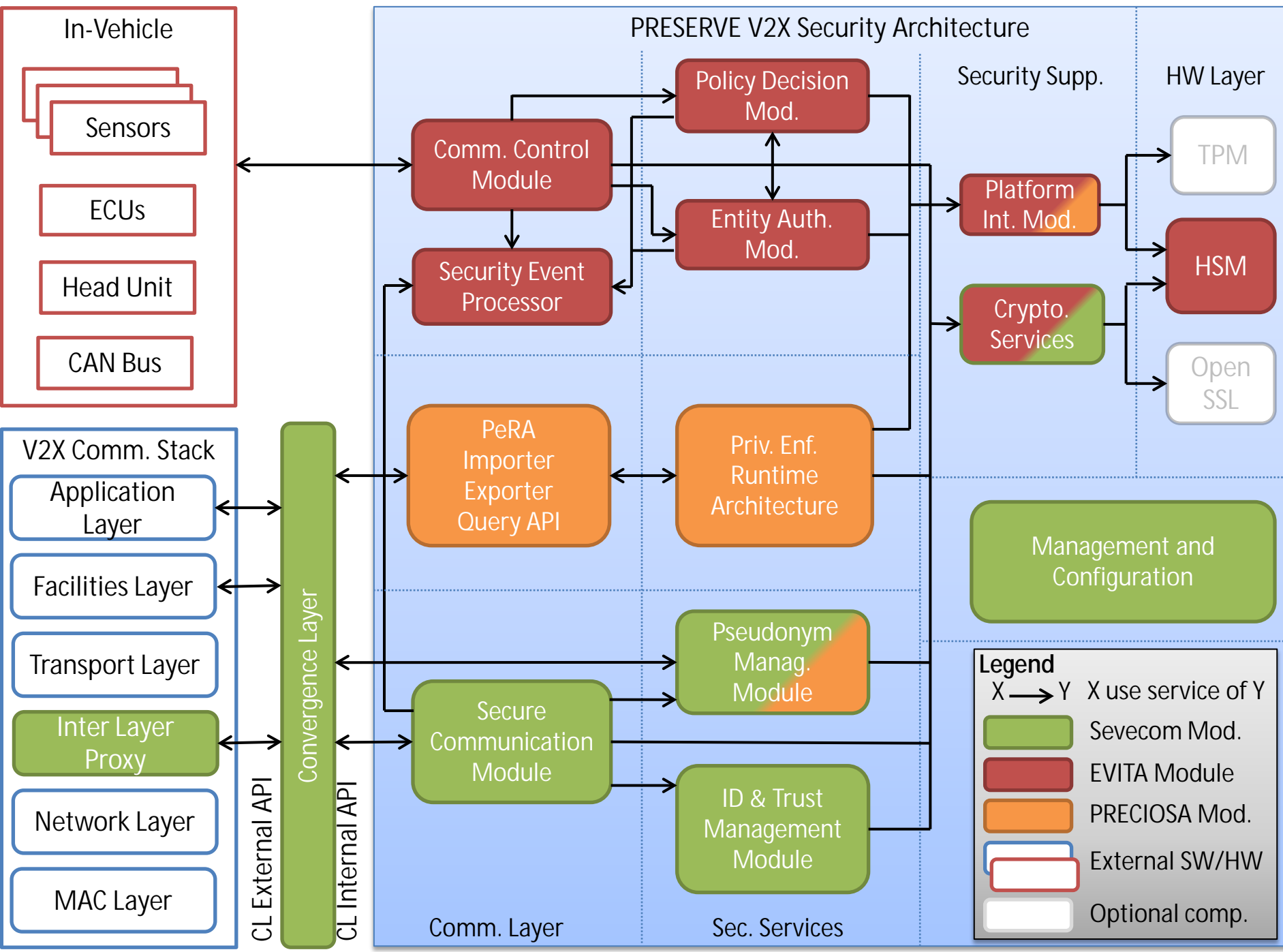
Session 1: Interoperability

of Cooperative Systems and feedback to standards

PRESERVE Status and Timeline

- V2X Security Subsystem
 - Modular Security Subsystem for ITS-S
 - Software Implementation, Convergence Layer, Hardware Security Module, Backend PKI
- VSS Kit 1: ready now (FPGA-HSM)
 - currently being integrated into Score@F platform
- VSS Kit 2:
ready mid 2013 (ASIC-HSM)

PRESERVE V2X Security Architecture



Activities to put in place?

- Searching partner for joint large scale test in 2nd half 2013
 - Integrate VSS with ASIC HSM into a fleet of vehicles
- Interoperability plugtest
 - Finalize ETSI norms
 - Testing interoperability of secured messages and PKIs
- Investigate potential integration of VSS into other ITS-S implementations

Req. Level of Interoperability?

- Interoperability of secured messages
 - Same security payload format
 - Same cryptosystems
 - Interoperable certificates
- Provide access to backend PKI via 3G or RSUs at all test-sites / in all vehicles
- Option to integrate HSM (currently USB)
- Interoperability of PKIs (optional)
 - Same ‘backend protocols’