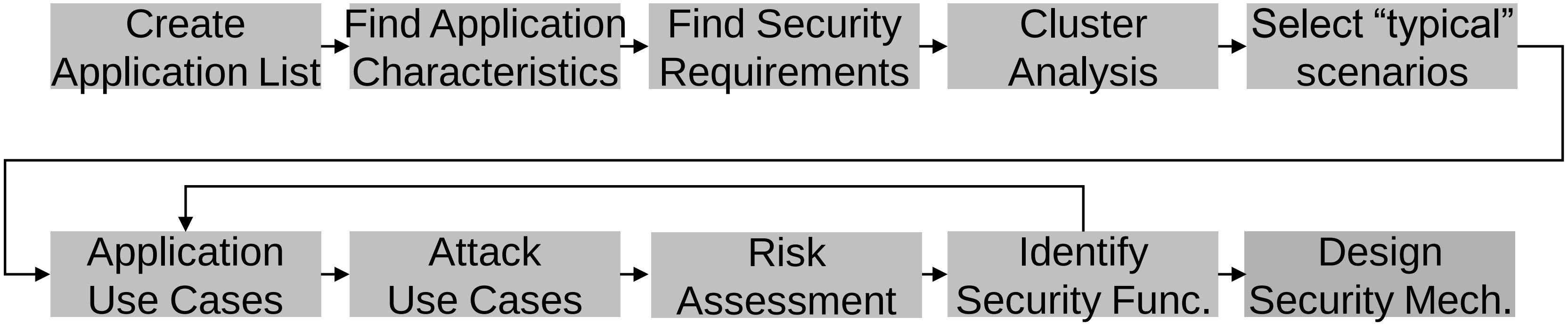
Secure Vehicle Communication

SeVeCom Baseline Architecture

Frank Kargl

17. October 2007

Security Requirements



Create Application List

Find Application Characteristics

Find Security Requirements

Cluster Analysis

Select “typical” scenarios

Application Use Cases

Attack Use Cases

Risk Assessment

Identify Security Func.

Design Security Mech.

- Starting with applications and general characteristics
  - Analyzed > 50 different applications
- Identified security requirements based on this understanding
- Cluster Analysis: 8 application clusters, selected 10 example applications
- Detailed application and attack use cases
- Identified 26 security functions
- SEVECOM Deliverable 1.1 “Threats and Requirements Analysis”
  http://www.sevecom.org/Deliverables/Sevecom_Deliverable_D1.1_v2.0.pdf
  Kargl, Ma, Schoch: *Security Engineering for VANETs*, Escar 2006

Security Requirements

- Authentication
  - Entity authentication
  - Attribute Authentication (e.g. IS_CAR property)
  - Geoauthentication (authenticate location of node)
- Integrity
- Confidentiality
- Privacy
  - ID privacy
  - Location privacy
  - … with revocation
- Non-repudiation / Liability issues
- Availability
- Access-Control

Security Functions

- Identification & Authentication Concepts
  - ***Identification***
  - ***Authentication of sender***
  - ***Authentication of receiver***
  - Attribute authentication
  - Authentication of intermediate nodes
- Privacy Concepts
  - ***Resolvable anonymity***
  - ***Total anonymity***
  - Location obfuscation
- Integrity Concepts
  - ***Integrity protection***
  - ***Encryption***
  - Detection of protocol violation
  - Consistency/context checking
  - Attestation of sensor data
  - Location verification
  - Tamper-resistant communication system
  - DRM
  - Replay protection
  - Jamming protection
- Access Control/Authorization Concepts
  - Access control
  - Closed user groups
  - Firewall/Checkpoint
  - Sandbox
  - Filtering
    (e.g. at intermediate nodes)

Baseline Security Architecture

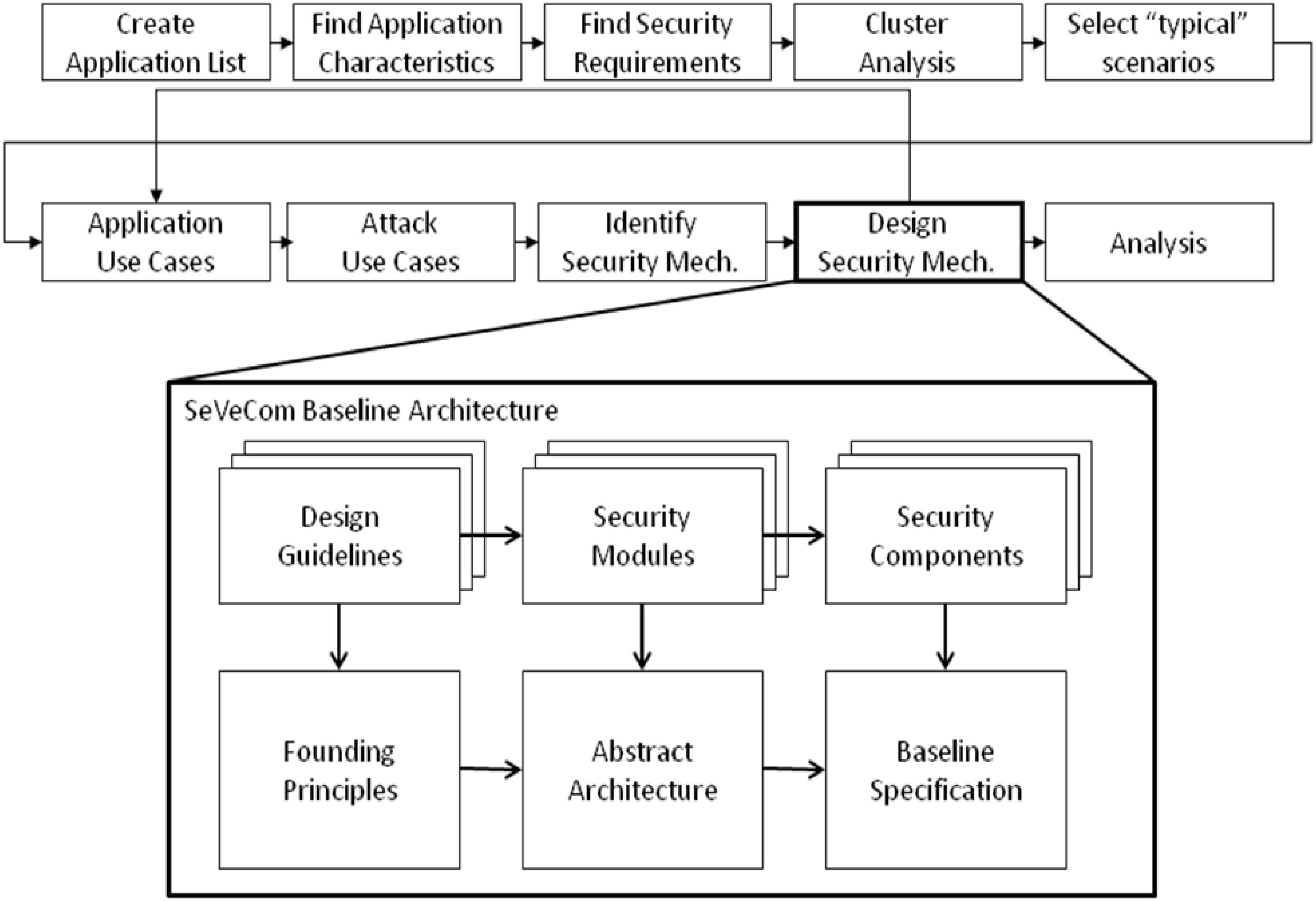
- Focus: Communication System

- Main objectives
  - Identity and Cryptographic Key Management
  - Privacy Enhancing Technologies (PET)
  - Secure Communication

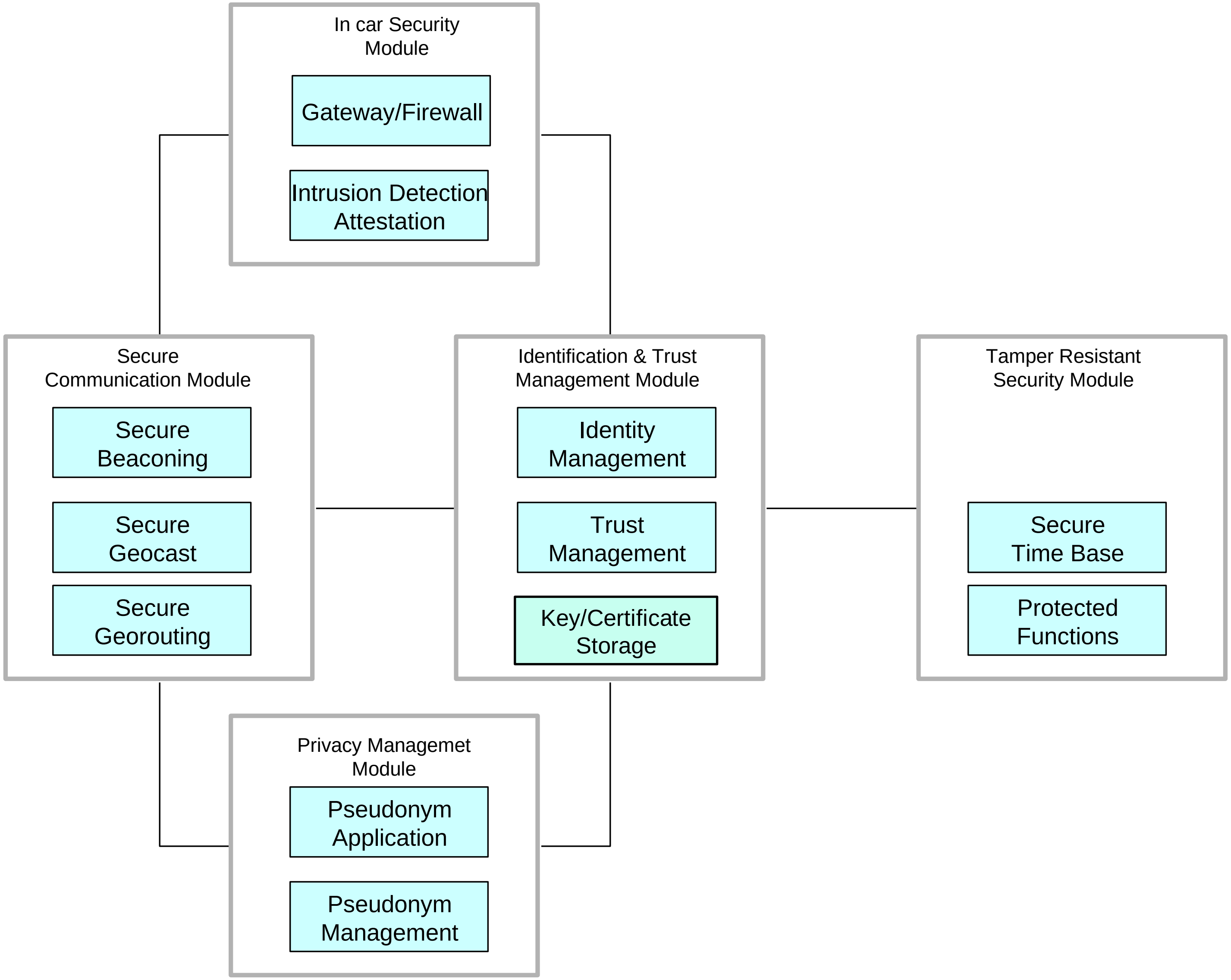
- Baseline solution design approach
  - Standardized cryptographic primitives
  - Easy-to-implement
  - Low overhead
  - Adaptable protection

- SEVECOM Deliverable 2.1: Security Architecture and Mechanisms for V2V/V2I V2.0
- Papadimitratos, Buttyan, Hubaux, Kargl, Kung, Raya, M.: *Architecture for Secure and Private Vehicular Communications*, ITST 2007

Architecture Model



Base. Arch.: Conceptual View



In car Security Module

Gateway/Firewall

Intrusion Detection Attestation

Secure Communication Module

Secure Beaconing

Secure Geocast

Secure Georouting

Identification & Trust Management Module

Identity Management

Trust Management

Key/Certificate Storage

Tamper Resistant Security Module

Secure Time Base

Protected Functions

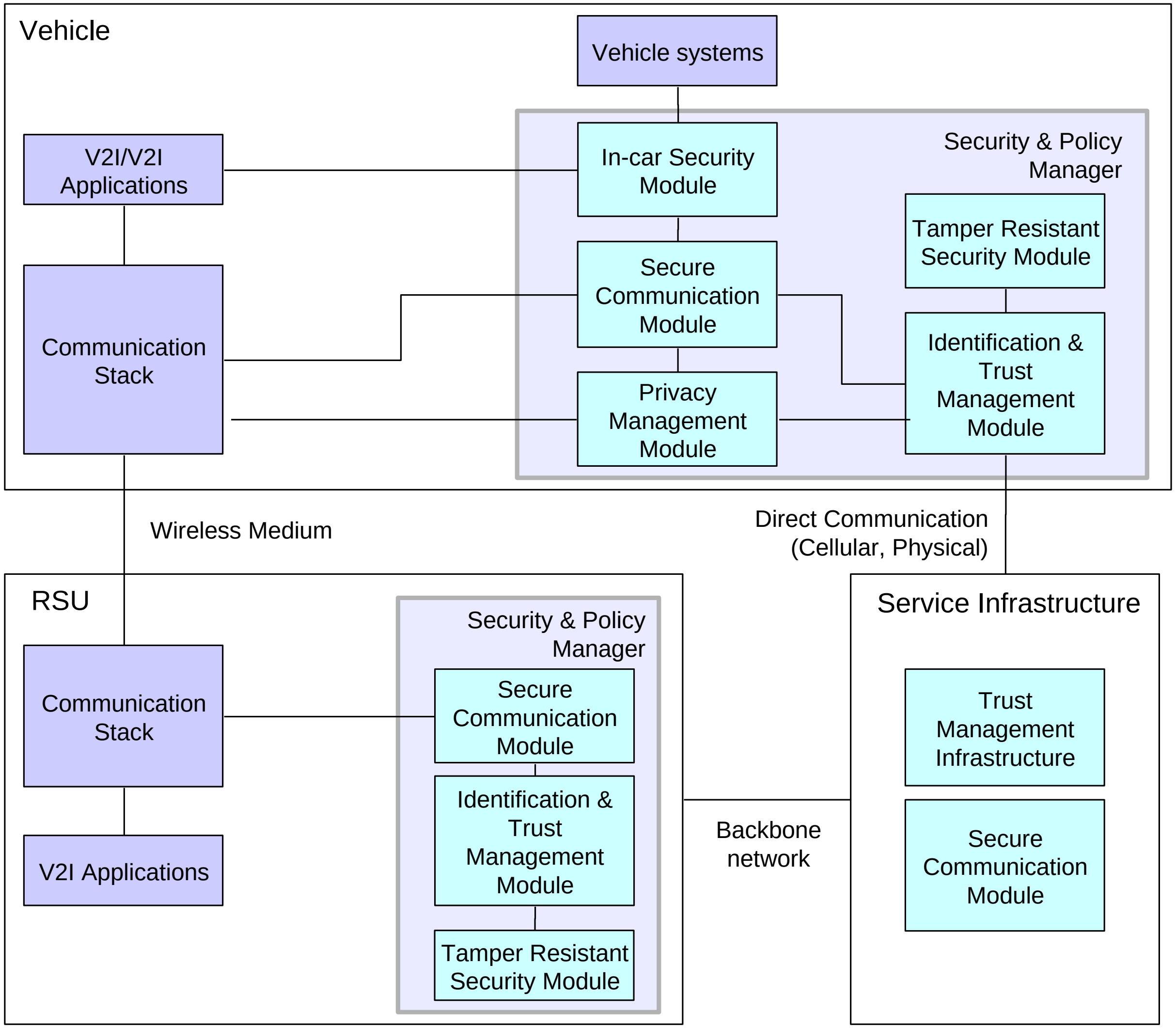
Privacy Managemet Module

Pseudonym Application

Pseudonym Management

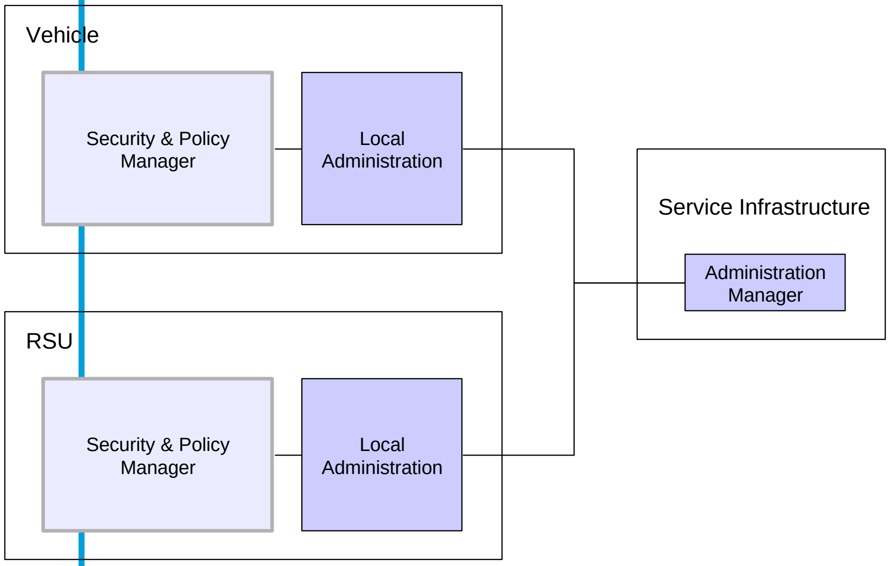
Modules	Comp.	Mechanisms
ID Management	Identification	**Identifiers, Certificates**, …
	Trust Manag. Infrastructure	**PKI**, Policies, …
	Revocation	**Verifier Revoc., RCCRL**, …
Privacy	Pseudonym Management	**Pseudonym pool**, …
	Pseudonym Application	Pseudonym Selection Proc.
	MIPv6/NEMO Privacy	BS Loc. Obfuscation, …
Secure Communication	Secure Beaconing	**Sec. Beaconing Prot., …**
	Secure Flooding	Secure Geocast Prot., …
	Secure Routing	Secure CGGC, …
Data Consistency	Position Verification	**Pos. Ver. System**, …
	Appl. Data Consistency	Data Consistency Checking
	Secure Aggregation	Secure Aggregation

SEVECOM Base. Arch.: Deployment View


Vehicle
Vehicle systems
V2I/V2I Applications
In-car Security Module
Security & Policy Manager
Tamper Resistant Security Module
Secure Communication Module
Communication Stack
Identification & Trust Management Module
Privacy Management Module
Wireless Medium
Direct Communication (Cellular, Physical)
RSU
Security & Policy Manager
Secure Communication Module
Communication Stack
Identification & Trust Management Module
V2I Applications
Tamper Resistant Security Module
Backbone network
Service Infrastructure
Trust Management Infrastructure
Secure Communication Module

SEVECOM Base. Arch.

Administration View



Vehicle

Security & Policy Manager

Local Administration

RSU

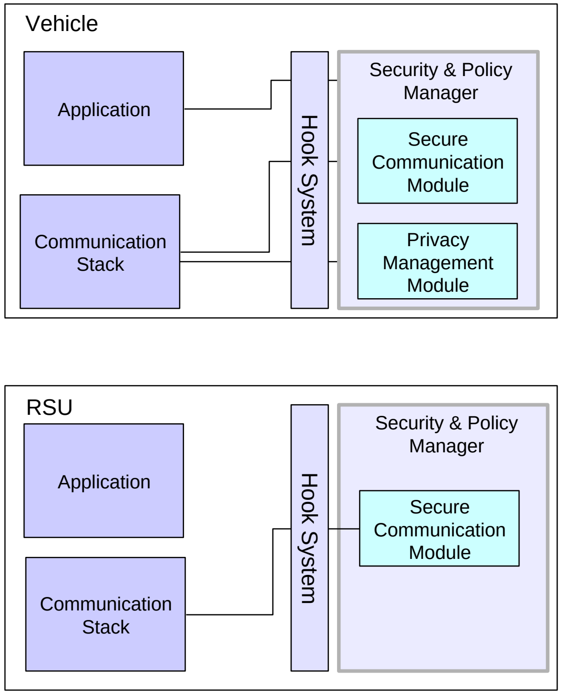
Security & Policy Manager

Local Administration

Service Infrastructure

Administration Manager

Integration View



Vehicle

Application

Communication Stack

Hook System

Security & Policy Manager

Secure Communication Module

Privacy Management Module

RSU

Application

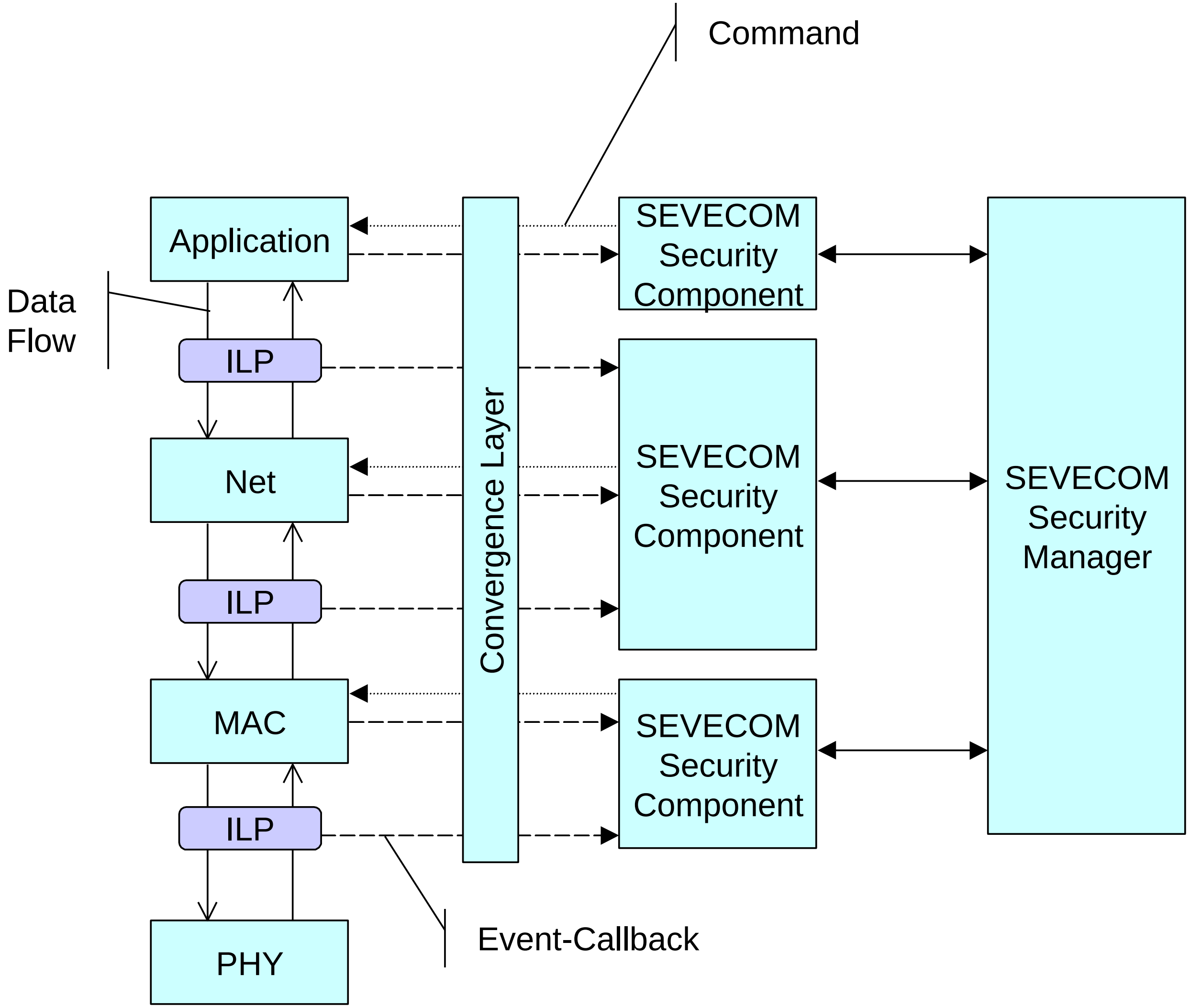
Communication Stack

Hook System

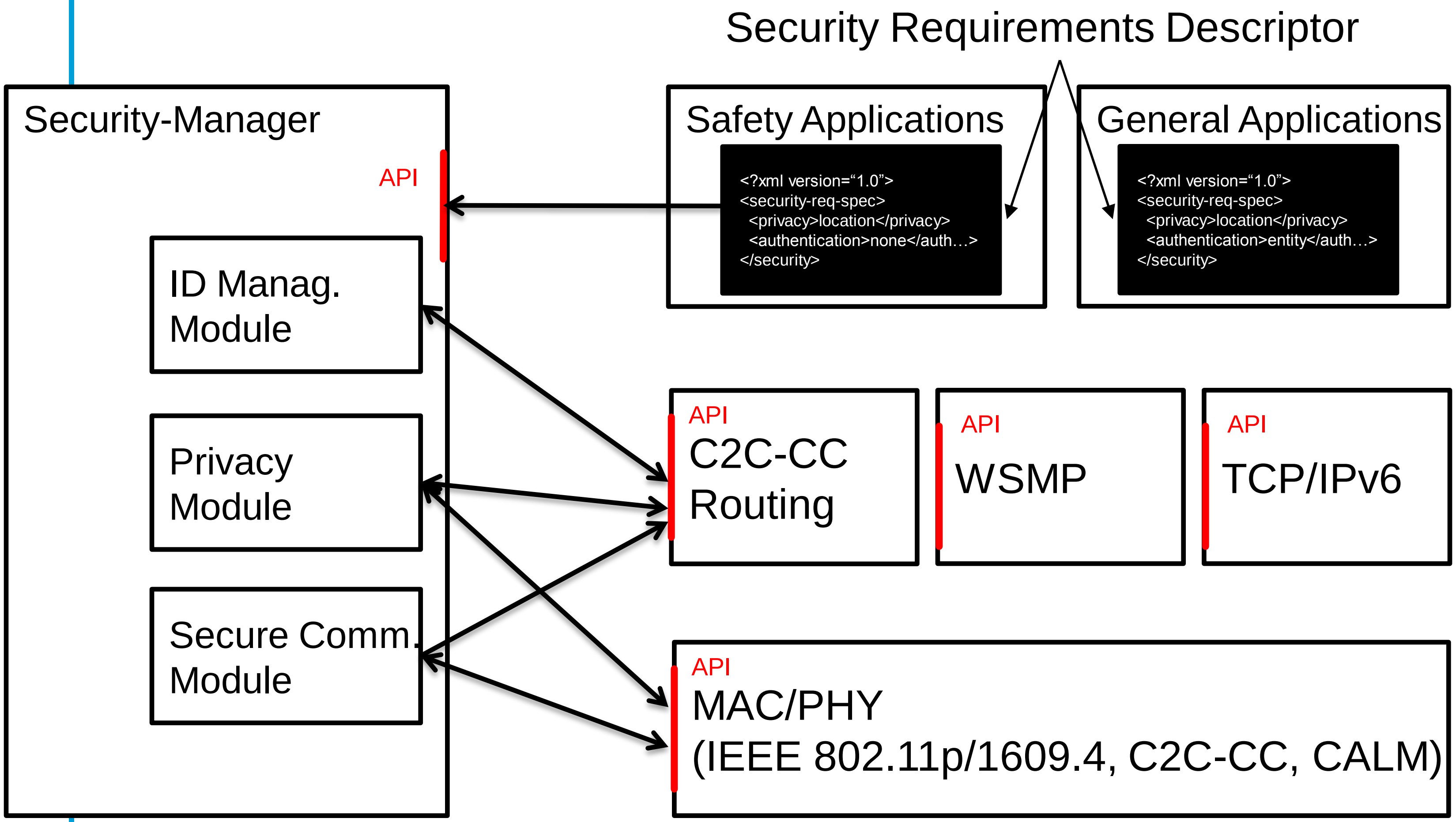
Security & Policy Manager

Secure Communication Module

Base. Arch.: Hooking Arch.



Impl. Architecture Concept



```
<?xml version="1.0">
<security-req-spec>
  <privacy>location</privacy>
  <authentication>none</auth…>
</security>
```

```
<?xml version="1.0">
<security-req-spec>
  <privacy>location</privacy>
  <authentication>entity</auth…>
</security>
```

Security Req. Specification

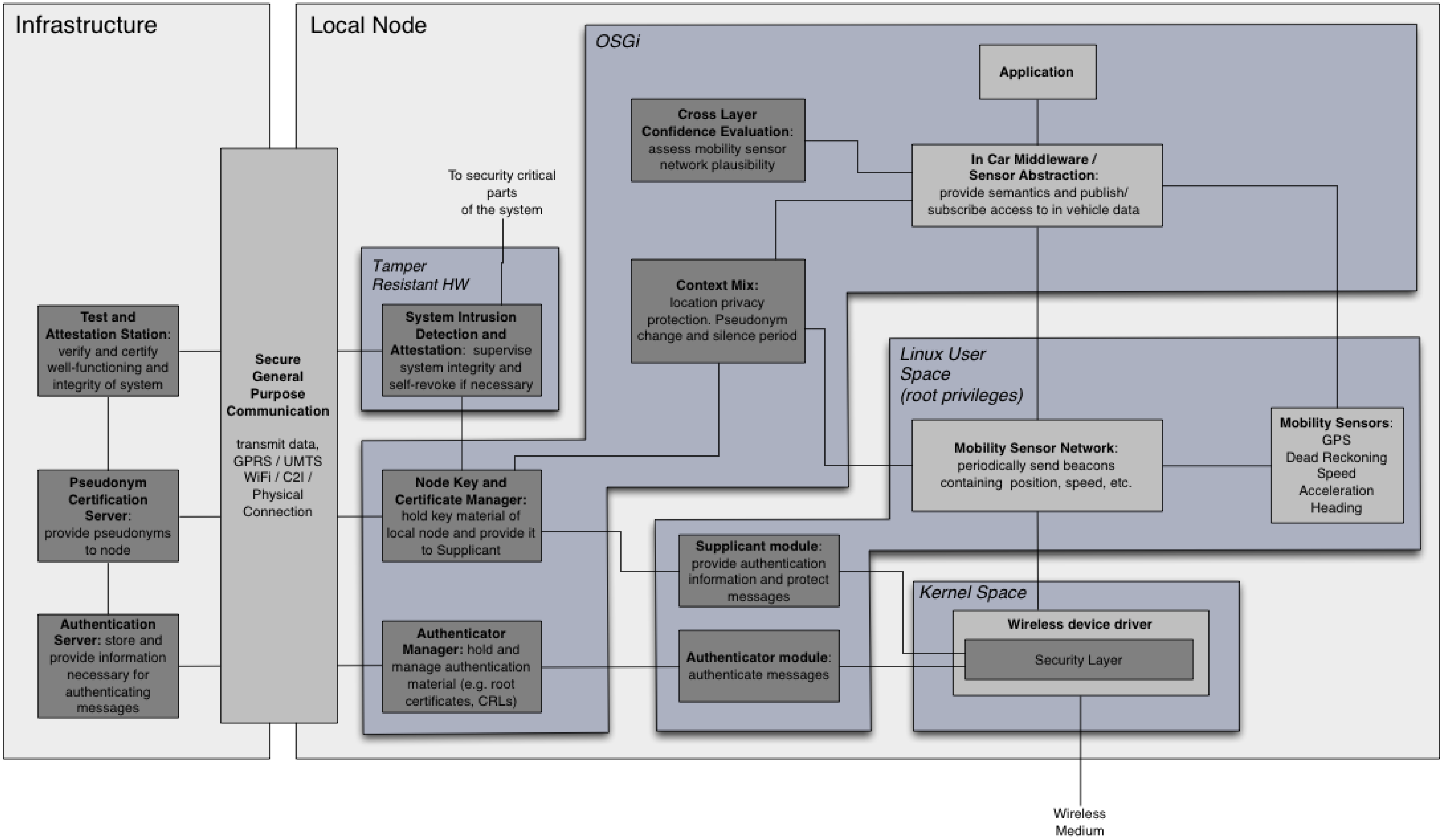
- Syntax
  - XML-based
  - Resource Description Framework / RDF
- Example

```
<?xml version="1.0"?>
 <rdf:RDF xmlns:rdf="..." xmlns:sv="http://www.sevecom.org/schema#">
  <rdf:Description rdf:about="http://www.c2c-cc.org/vehicle-based_road_cond_warning">
   <rdf:type rdf:resource="esafetyApplication"/>
    <sv:requires>
     <sv:SecurityRequirement module="PropertyAuthentication">
      <sv:nodeType>Vehicle</sv:nodeType>
     </sv:SecurityRequirement>
    </requires>
    <requires>
     <sv:SecurityRequirement module="Privacy">
      <sv:idPrivacy changeInterval="5s"/>
     </sv:SecurityRequirement>
    </sv:requires>
  </rdf:Description>
</rdf:RDF>
```

Opportunities

- Dynamic security and privacy configuration allows
  - Configure priorities in case of contradicting security requirements
  - Extend security / privacy configuration during operation, e.g. when new applications get installed
  - Personal security and privacy profiles
    - User empowerment
    - How to create/edit profiles? Security User Interface
  - Adapt security / privacy to national regulations
    - Even during use, e.g. when crossing borders
  - …

SeVeCom and NoW/Fokus



Infrastructure

Local Node

OSGi

Application

Cross Layer Confidence Evaluation: assess mobility sensor network plausibility

In Car Middleware / Sensor Abstraction: provide semantics and publish/ subscribe access to in vehicle data

To security critical parts of the system

Tamper Resistant HW

System Intrusion Detection and Attestation: supervise system integrity and self-revoke if necessary

Context Mix: location privacy protection. Pseudonym change and silence period

Linux User Space (root privileges)

Mobility Sensor Network: periodically send beacons containing position, speed, etc.

Mobility Sensors: GPS Dead Reckoning Speed Acceleration Heading

Test and Attestation Station: verify and certify well-functioning and integrity of system

Secure General Purpose Communication

transmit data, GPRS / UMTS WiFi / C2I / Physical Connection

Pseudonym Certification Server: provide pseudonyms to node

Authentication Server: store and provide information necessary for authenticating messages

Node Key and Certificate Manager: hold key material of local node and provide it to Supplicant

Supplicant module: provide authentication information and protect messages

Kernel Space

Wireless device driver

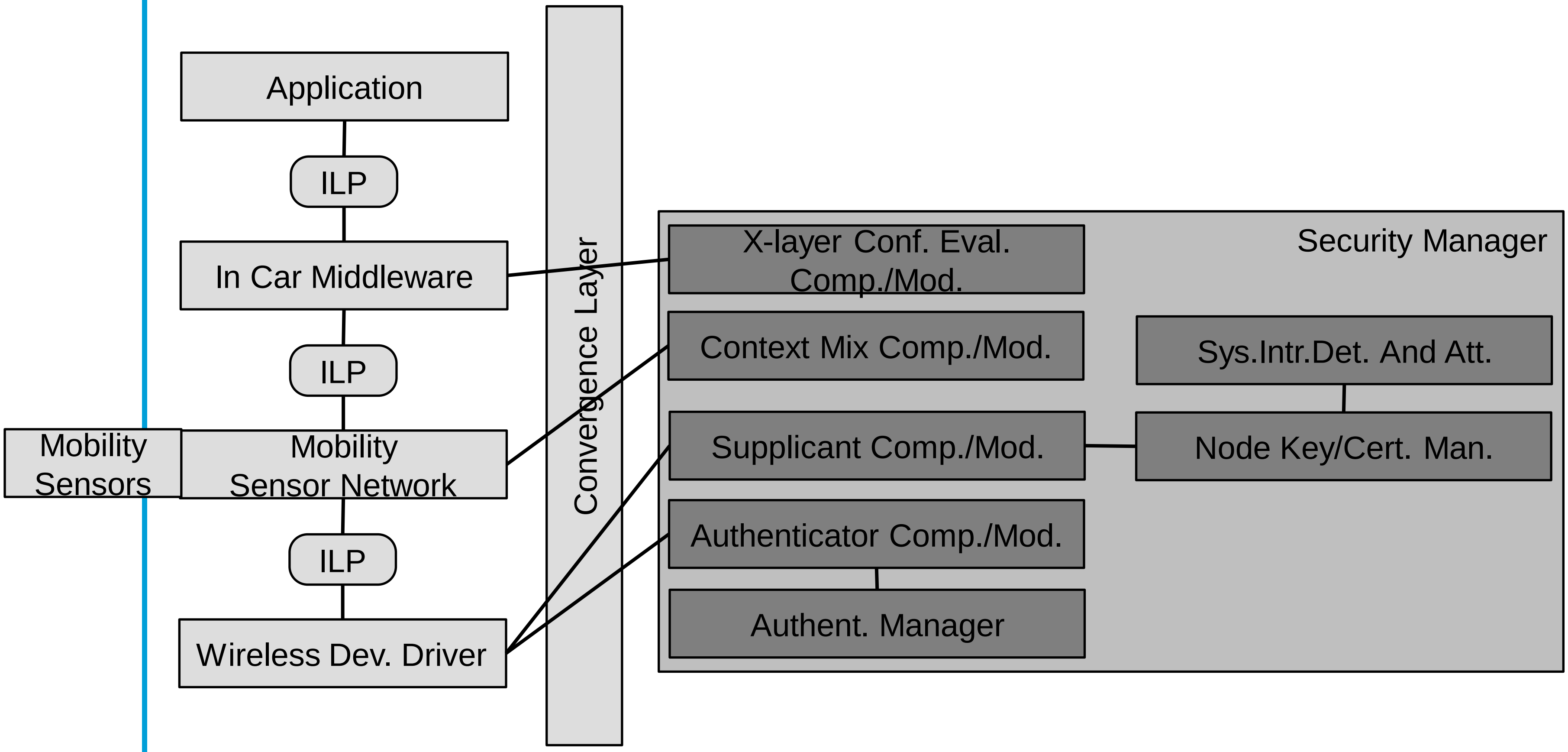
Security Layer

Authenticator Manager: hold and manage authentication material (e.g. root certificates, CRLs)

Authenticator module: authenticate messages

Wireless Medium

SeVeCom and NoW/Fokus



Next Steps

- Baseline Component Specification
- Status
  - Standardized component description including
    - Purpose of component
    - Prerequisites for component
    - Interfaces and services provided by component
    - Description of component
    - Performance aspects
    - Related Work
  - Work has started for the following components
    - Identification
    - Trust Management Infrastructure
    - Pseudonym Management
    - Pseudonym Application
    - Secure Beaconing
    - Secure Flooding
    - Secure Routing
  - Should reach a somehow mature state until end of the year

ID Management

- Need to prevent unauthorized network access and Sybil attacks
- Identification of a vehicle or RSU needs to be protected
- Solution: PKI-based approach
  - Public key cryptography, certificates, CAs, message signing
  - Issued at construction, extended later automatically
  - Stored in tamper-resistant hardware
  - Crypto-based addresses:
    derive MACs, IPs, … from public key
- Privacy Problem: nodes get traceable when using fixed identifiers

Changing Pseudonyms

- Privacy Enhancing Technologies (PET)
  - Temporary Pseudonyms
    - Remove all identifying information from certificate
    - Equip vehicles with multiple pseudonyms from pseudonym providers
    - Alternate among pseudonyms over time (and space)
    - Pseudonym provider can resolve pseudonyms e.g. in legal disputes

PSNYM_3_2
PSNYM_1_3
PSNYM_2_2
PSNYM_1_1
PSNYM_2_3
PSNYM_1_2
PSNYM_3_1
PSNYM_2_1

Discussion?