**Consortium**

CASSIDIAN AN EADS COMPANY | ERNW Living Security. | Fraunhofer SIT | Hochschule Augsburg University of Applied Sciences | Nokia Siemens Networks | RWTH AACHEN UNIVERSITY

ASMONIA

*Attack analysis and Security concepts for MObile Network infastructures supported by collaborative Information exchAnge*

SPONSORED BY THE Federal Ministry of Education and Research

# ASMONIA Overview and Reference Architecture for Collaborative Information Exchange

ASMONIA Security Research Project

Hans Hofinger, Fraunhofer SIT

01.04.2011

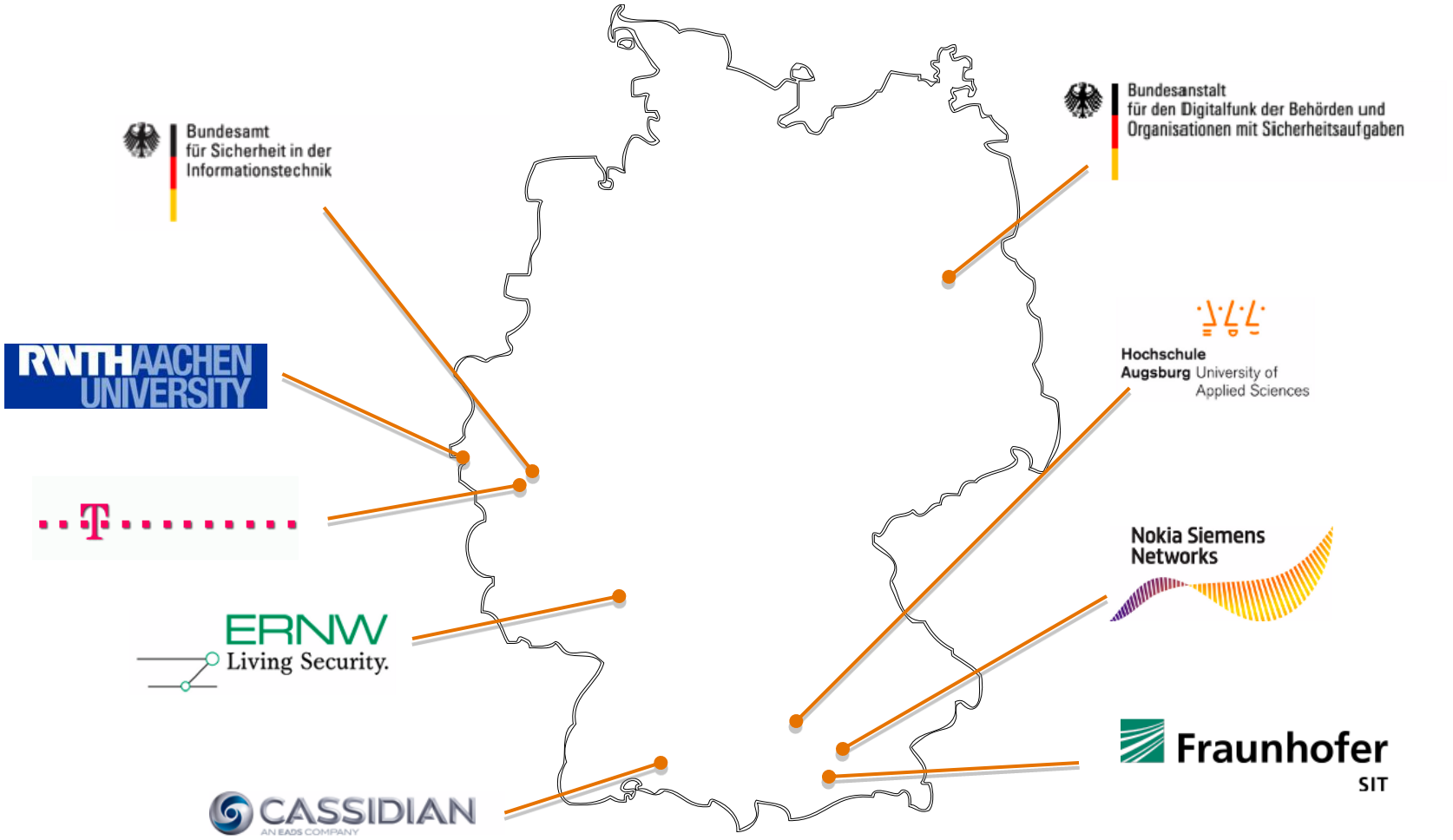
# Disclaimer

This document has been produced partially in the context of the ASMONIA project. The ASMONIA project is part of the BMBF program for research and as such is funded by the Federal Republic of Germany.

# Section: Project Overview

- Who we are
- Funding
- Status

# Project Consortium



# Project Consortium

## Partners

- CASSIDIAN
- ERNW GmbH
- FhG SIT
  Fraunhofer Institute for Secure Information Technology
- Nokia Siemens Networks
- RWTH
  Rheinisch-Westfälische Technische Hochschule Aachen
- University of Applied Sciences Augsburg (HSA)

## Associated Partners

- BDBOS
  Federal Agency for Digital Radio of Security Authorities and Organisations
- BSI
  Federal Office for Information Security
- DTAG
  Deutsche Telekom AG

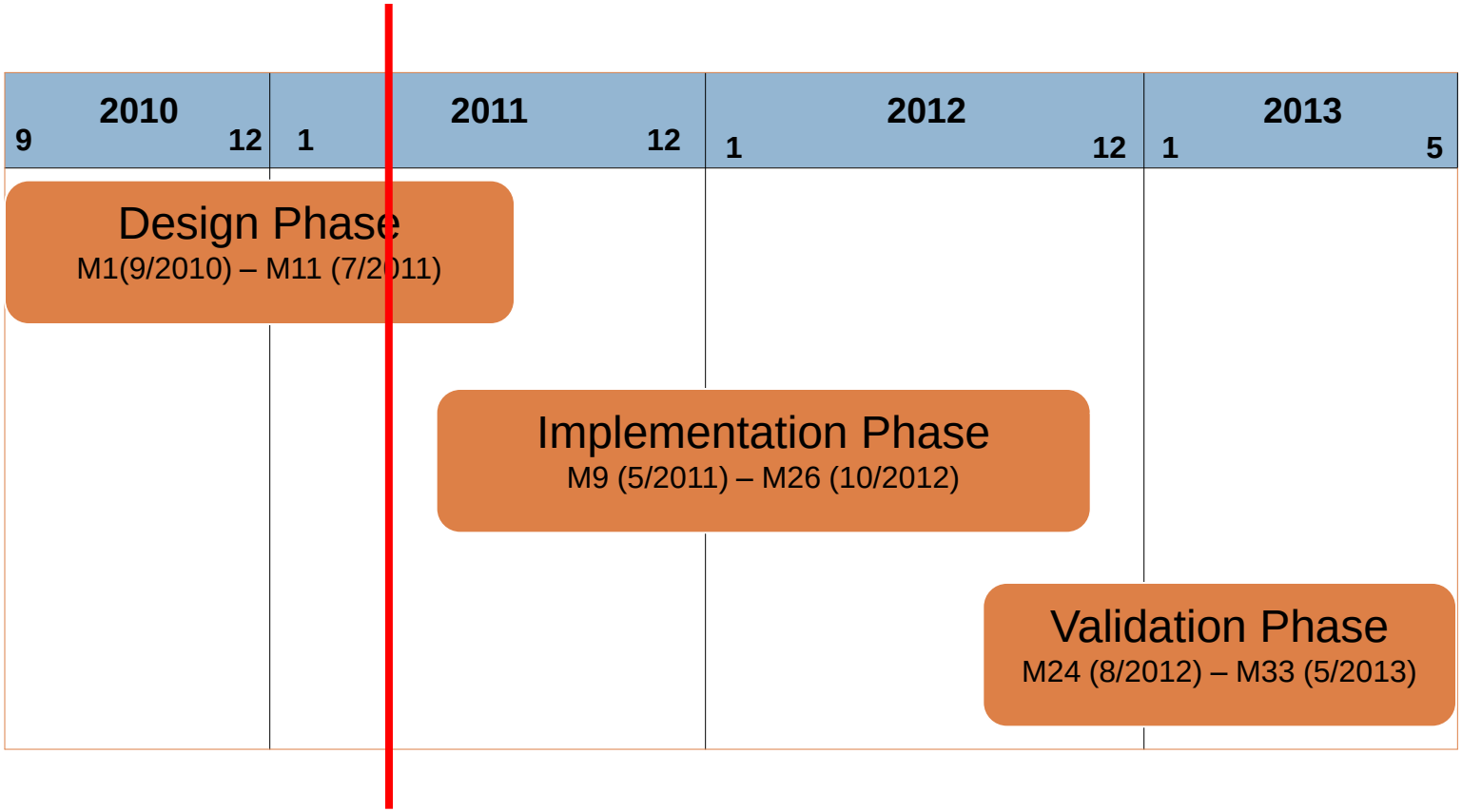
# Administrative Project Data

- BMBF sponsored project
- Start in September 2010 for 33 months (May 2013)
- More than 330 PM planned
- EUR 2.8 Mio funding

visit us at

**www.asmonia.de**

# Project status



# Project status

- Project is now in the Design phase

- First (intermediate) results
  - Initial threat and risk analysis finished
  - First assumptions manifested in reference architecture
  - Initial use cases identified

- Ambitious project objectives:
  - Improve terminal and NE integrity and security
  - Improve attack detection and mitigation
  - Enable collaboration across administrative domains

# Section: Motivation

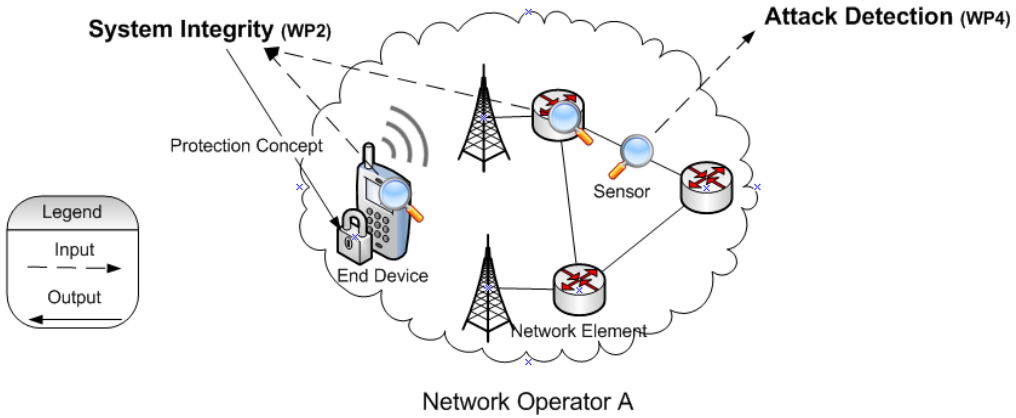
- Overall
- One Network Operator
- Across Network Operators
- Critical Infrastructure

# Overall Motivation

- Different Smartphone OSs and security architectures
  - Symbian, Android, iOS, RIM, Windows Mobile etc.
  - Distribution mechanisms of Smartphone Apps
- Business models of underground economy more and more applied on mobile platforms
  - From proof of concepts to automated broad scale attacks
- Changes in network infrastructure when migrating to 4G might lead to new threats that have to be addressed
- Collaborative data exchange advantageous to mitigate attacks

# Motivation:
# Single Network Operator

- **Network operator's motivation**
  - Improving terminal security by solutions that allow identifying system integrity problems
    - For terminals (open OS, Smartphones)
    - For NE of access network infrastructure
  - Improving malware and attack detection and handling



# Motivation: Multiple Network Operators

- **Network operators' motivation**
  - Improving terminal security by solutions that allow identifying system integrity problems
    - For terminals (open OS, Smartphones)
    - For NE of access network infrastructure
  - Improving malware and attack detection and handling
- **…with emphasis on several operators' infrastructure**
  - Sharing knowledge on vulnerabilites or attacks (situational information, reputation, fairness)
  - Evaluating use of elastic solutions for improving overall availability
  - Deriving assertions about „system health“ and situational awareness

# Motivation: Critical Infrastructure (1/3)

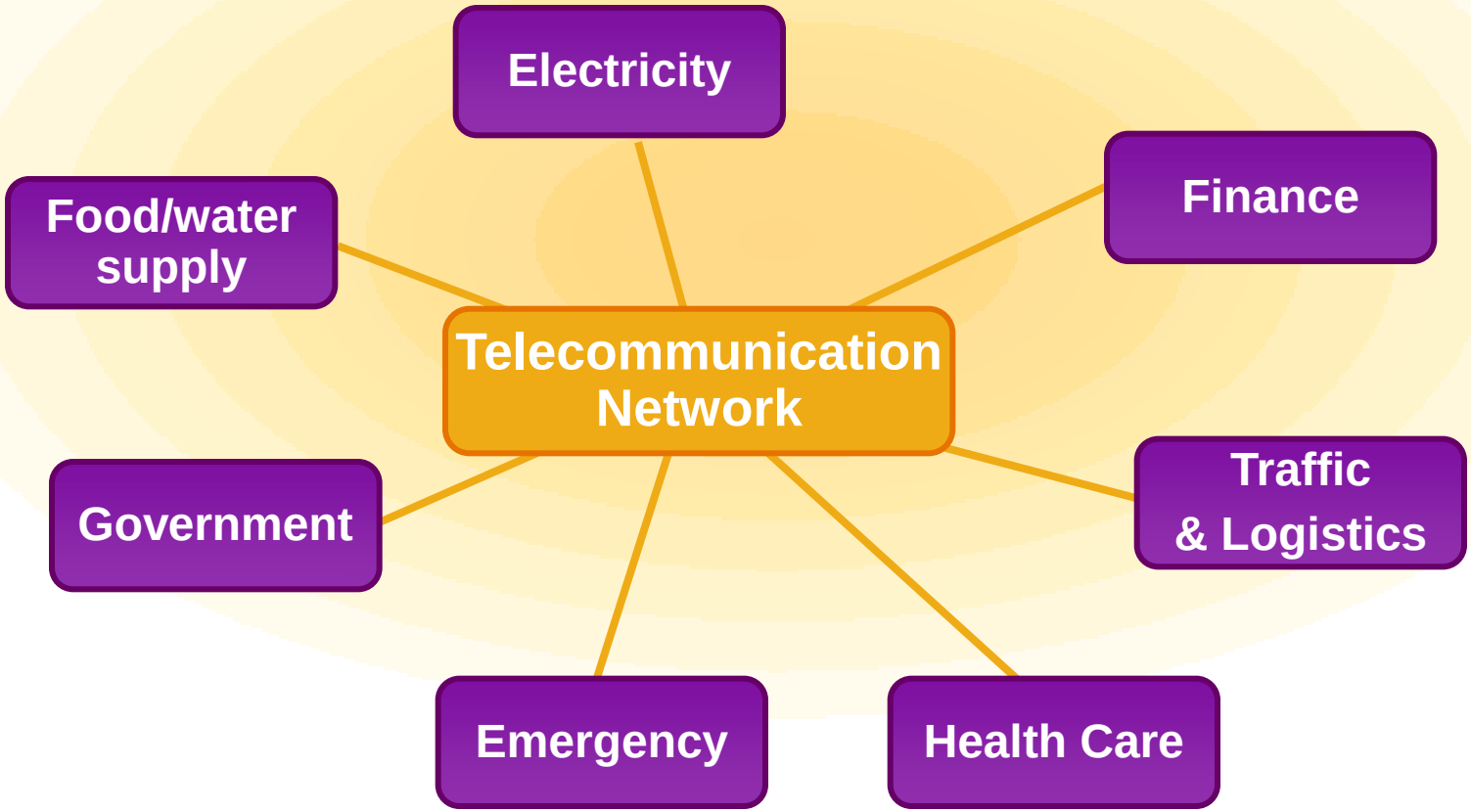
- **Telecommunication networks are part of critical infrastructures:**
  - More and more transactions, delivery processes, control procedures, business processes based on the use of telecommunication networks
  - Cross-relationships between telecommunications and critical infrastructure (electricity supply, transport, ...) reinforce

# Motivation: Critical Infrastructure (2/3)

- **At the same time, the exposure of telecommunication networks against attacks is growing:**
  - Global Internet connectivity
  - Increasing complexity and functionality of the networks
  - Worldwide availability and "trade" with attack tools and illegally obtained results (-> "criminal eco-system")
  - Increasing physical accessibility of telecommunications equipment
  - The achievable amount of damage increases the attractiveness of attacks, e.g., by ideologically motivated adversaries, or as a military threat potential

# Motivation: Critical Infrastructure (3/3)

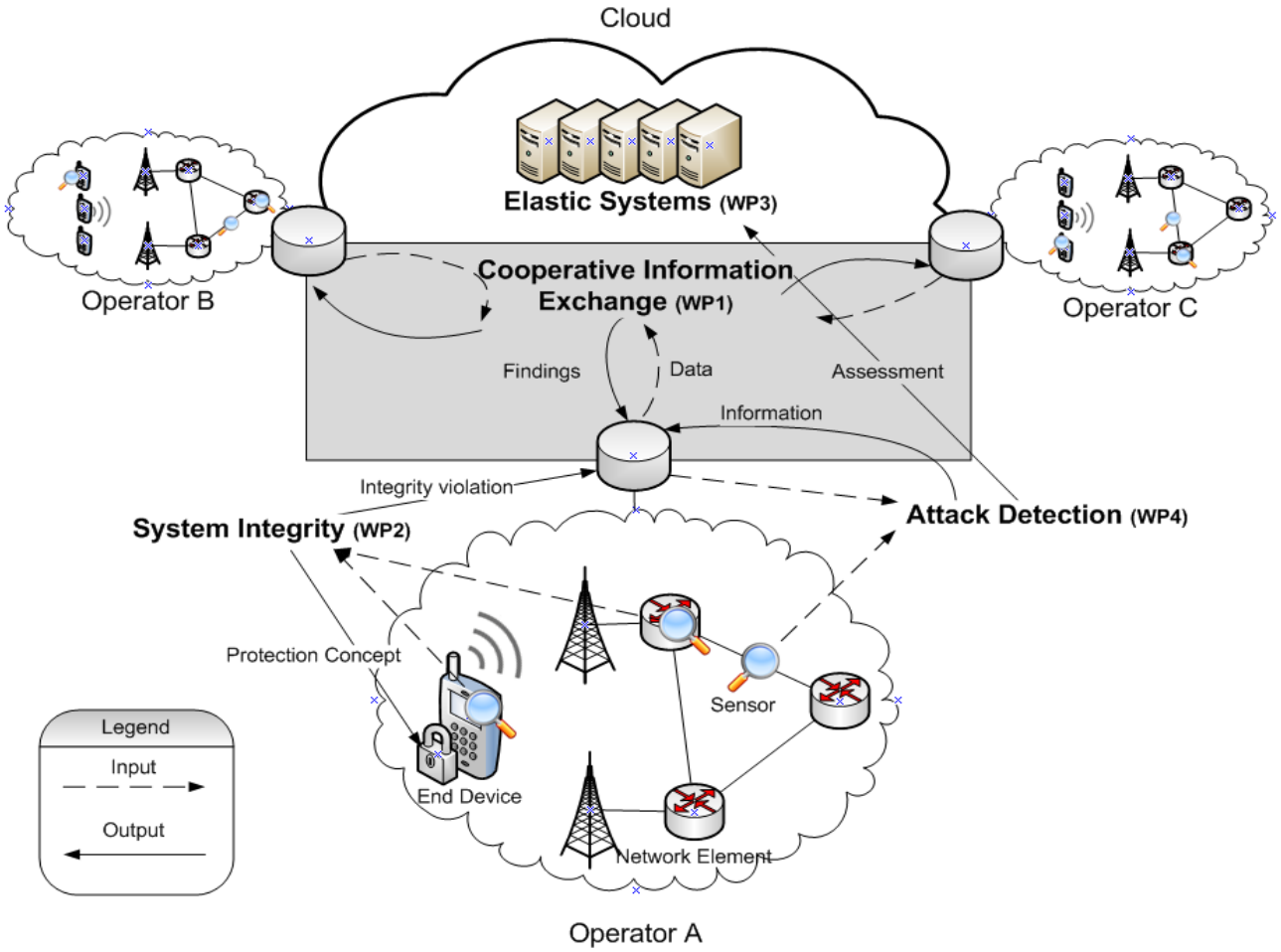
- Double role: critical infrastructure & connecting link



# Section: Approach

- ASMONIA Big Picture
- Tasks overview
- Technology components

# ASMONIA Big Picture



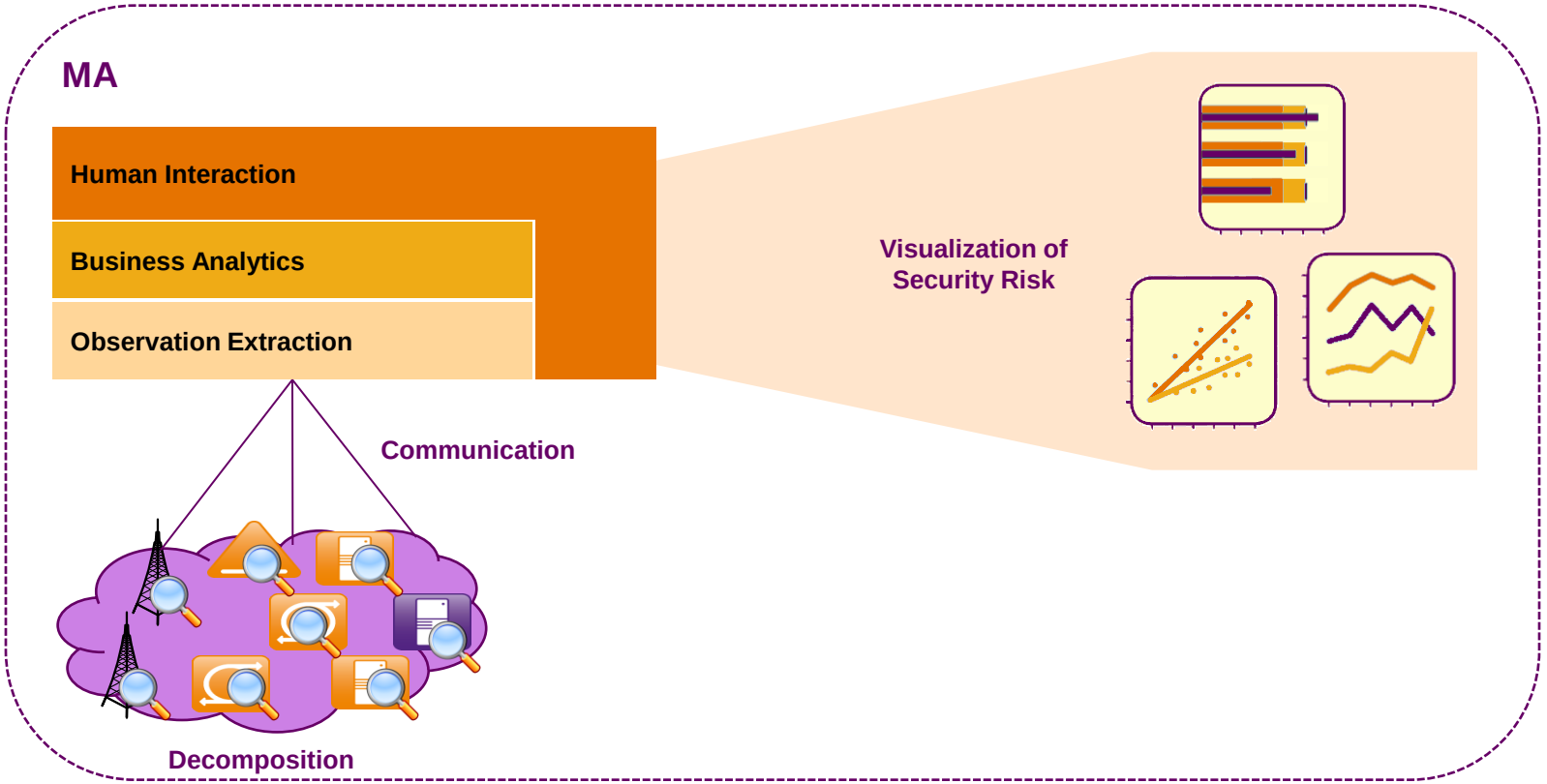
# Integrity Protection & Attack Detection

- On network elements in access network
  - SW-Integrity protection as a priority protection measure
- On terminals
  - OS hardening concepts (L4 µkernel, Open Kernel Labs OKL4, TrustZone …)
  - ligthweight attestation as runtime validation measure
- Malware
  - honeypot based malware detection methods

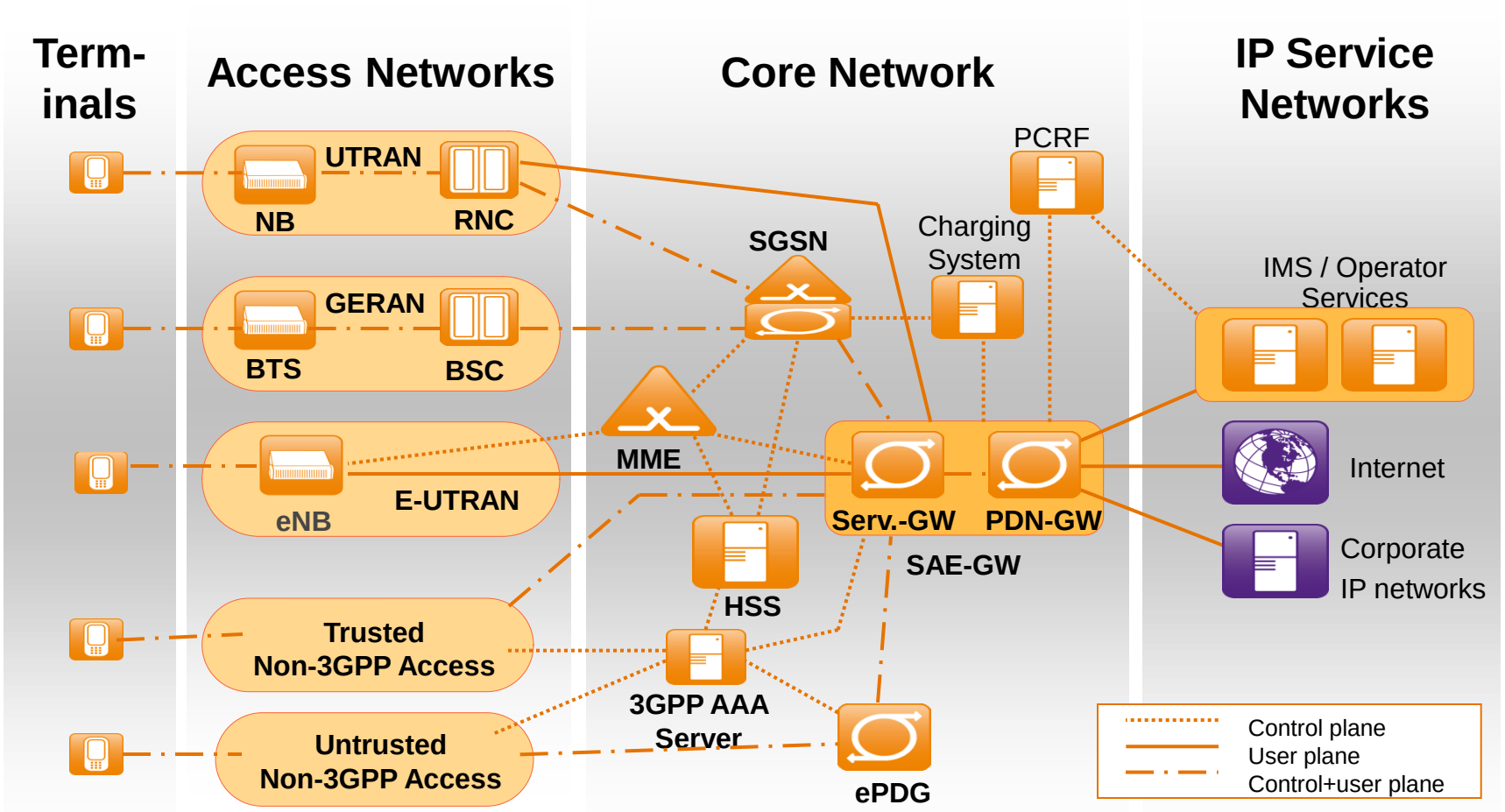
# Cloud Computing Scenarios Considered

- Cloud as a means to store and evaluate messages
  - Integration of messages about events and warnings with different origins
- Cloud as a means to enhance availability and security in overload and outage situations
  - Instantiate telecommunication system capabilities in elastic systems to improve failure situation and reconfiguration handling
- Management of shared cloud resources
  - Aspects of cloud management including scalability and instantiation of components in the cloud

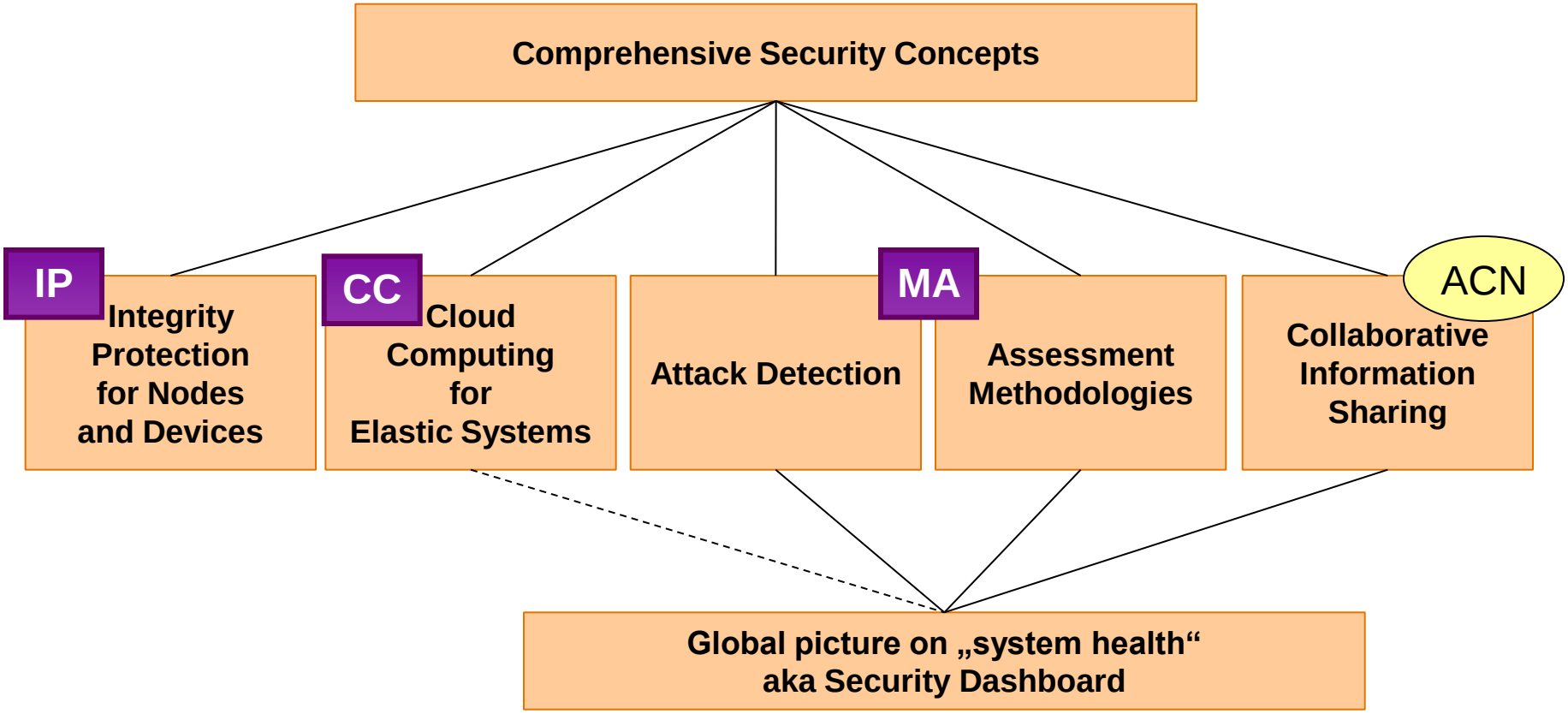
# Single/Multiple Network Operator System Health



# Threat & Risk Analysis



# Dependencies of Technology Components



# Section: Collaboration

- Collaborative Information Exchange
- Use Case
- Challenges & Requirements
- Proposed Components

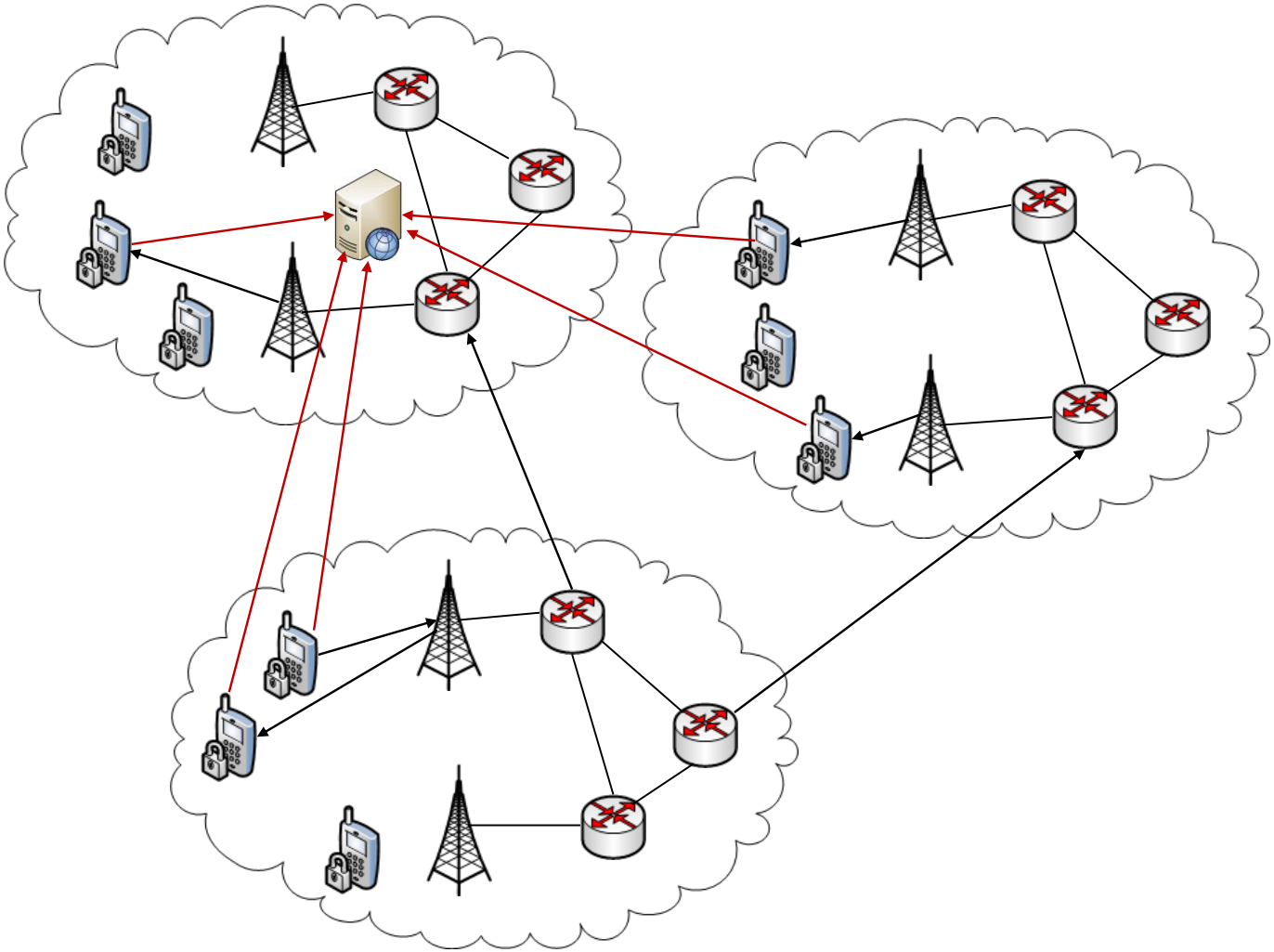
# Collaborative Information Exchange

- Objective
  - Attack mitigation by exchanging signatures and warnings
- Methodology
  - Information sharing of incident related data between mobile operator networks
  - Exploitation of heterogeneous environments
- Requirements
  - Taking into account privacy and security considerations
  - Interfaces to existing Early Warning Systems

# Use Case Example

- Unknown mobile malware (worm) infects specific Smartphones depending on their OS in multiple operator networks
- Botnet is formed and used for a DDoS attack on a service of an operator or third party
- Attack is detected and local and global system health states are created and exchanged
- Cloud computing systems are used to provide additional resources and handle overload situation
- Incident related data is exchanged between operators to mitigate attack impact and restore infected devices to a trustworthy configuration

# Use Case:
# Unknown Smartphone worm



# Challenges & Requirements

- Incident related data might include sensitive information of operators, e.g. network infrastructure details, vulnerable services etc.
  - Loss of reputation must be prevented
    - Anonymizing and sanitizing information before sharing is essential
    - However, data must contain enough information to be useful for recipient
- ASMONIA Collaboration Network (ACN) needs to be highly available
  - Single points of failure must be avoided
    - Usage of a distributed, completely decentralized infrastructure

# Challenges & Requirements

- Information shared between operators must not be modified by attackers
  - The integrity and confidentiality of messages in the ACN must be guaranteed
    - Shared information must be encrypted and signed by sender
- External attackers must not be able to inject falsified messages into the ACN
  - A closed user group for authorized participants must be established
    - The authenticity of messages must be guaranteed, e.g., by using certificates

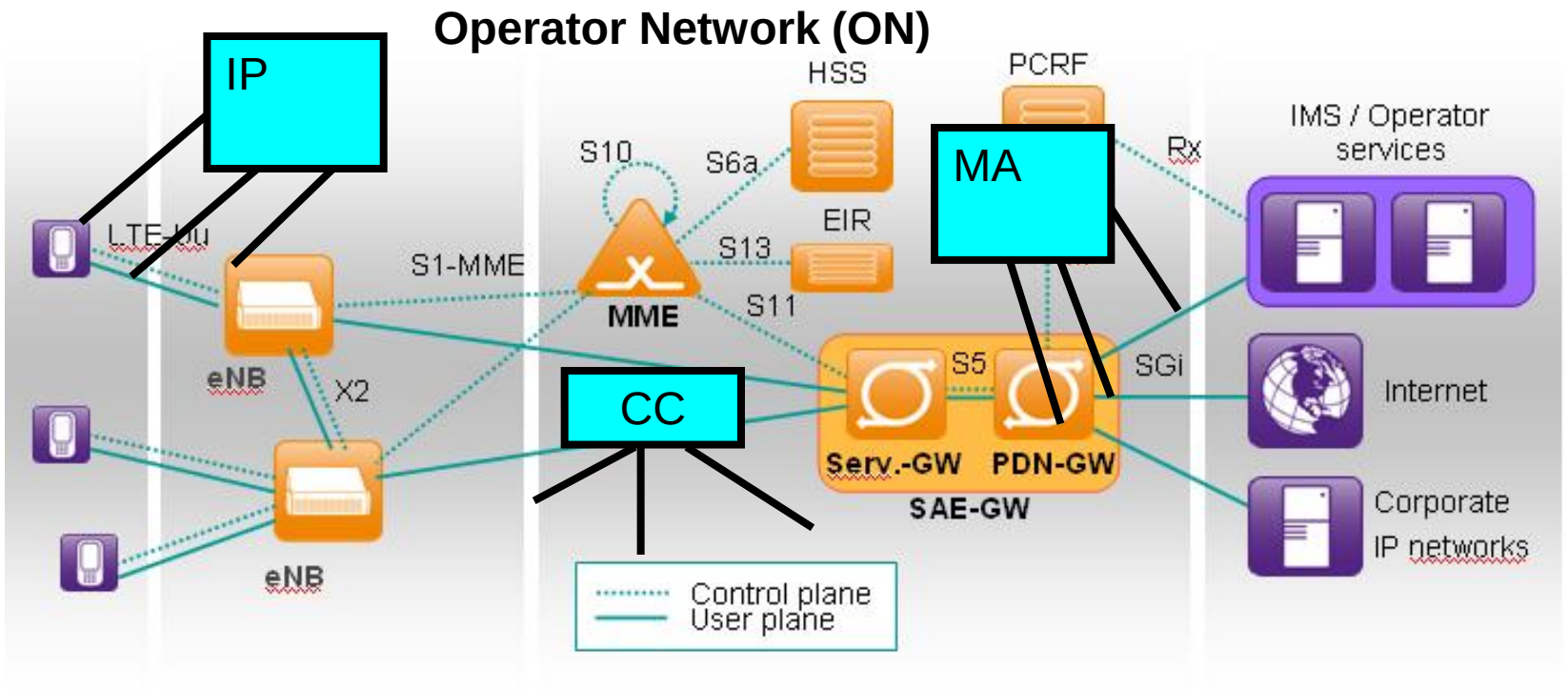
# Proposed Components

- Traceable Anonymous Certificates (TAC) [1]
  - Traceable Anonymous Certificates (TAC) provide key material to en-/decrypt and sign exchanged information without revealing a participant's real identity
- P2P Overlay Networks (GNUnet [2], GAP [3])
  - P2P Overlay Networks (e.g., GNUnet) improve resilience and anonymity of the data exchange channels itself by using redundant and indirect routes
- Secure MultiParty Computation [4]
  - Secure Multiparty Computation (MPC) enables participants to share security incident related data in a privacy preserving way to enhance detection and mitigation of attacks

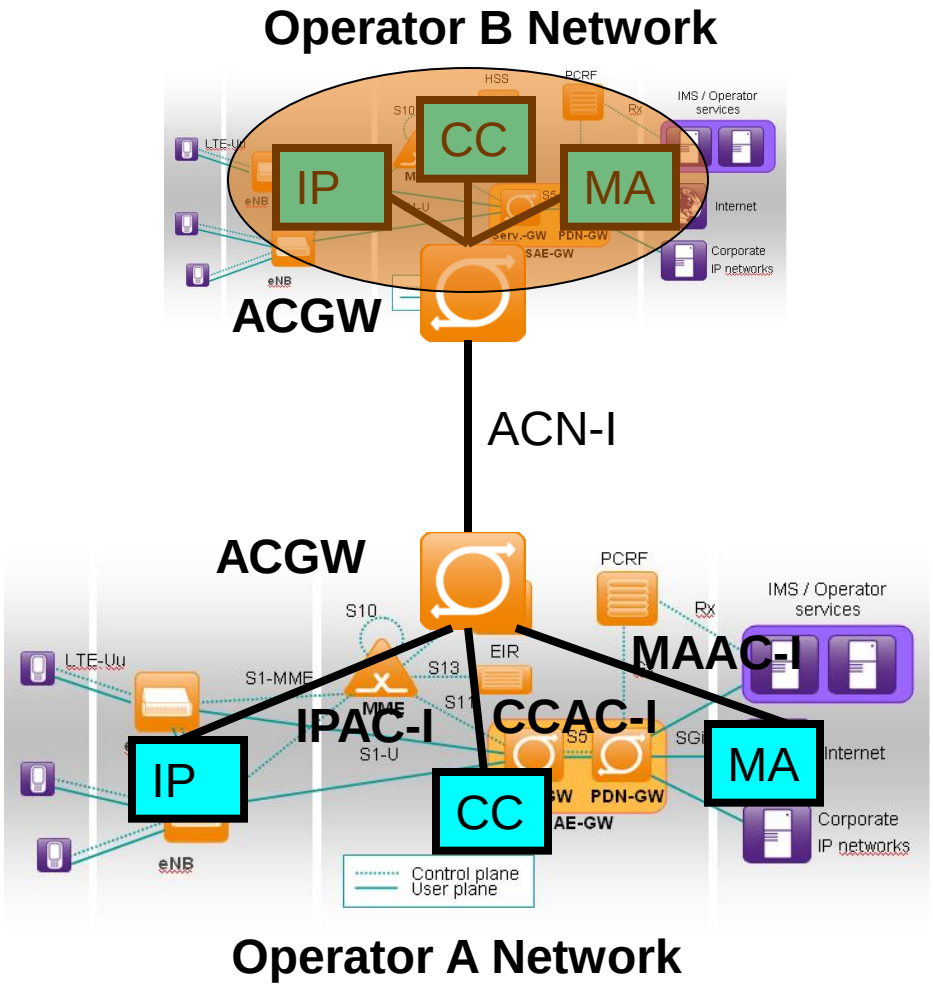
# Section: Reference Architecture

- Mobile Operator Network Infrastructure
- Functional Clusters
- ASMONIA Collaboration Gateway (ACGW)
- ASMONIA Collaboration Network (ACN)

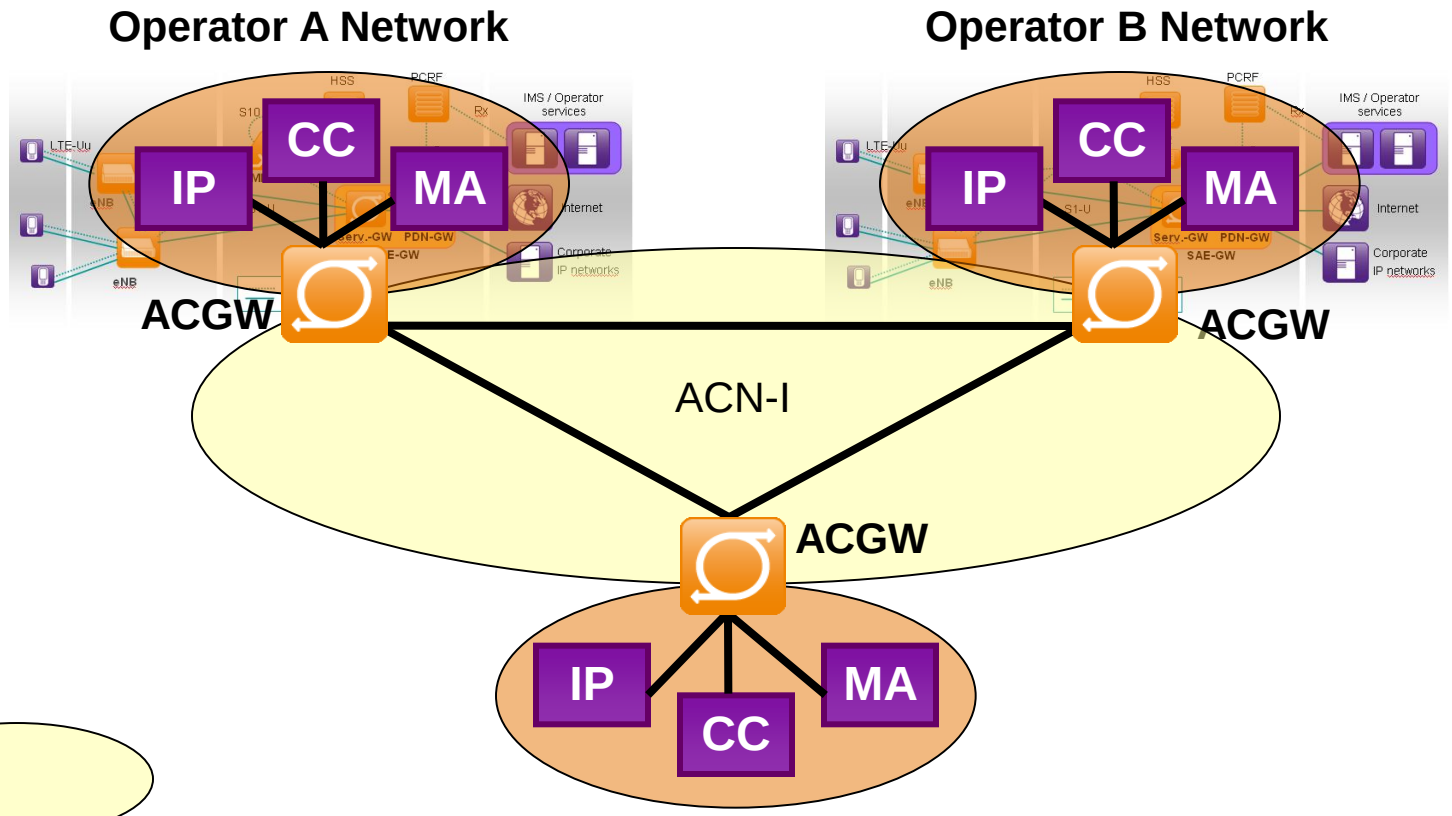
# Reference Architecture – Functional Clusters (FC)



# Reference Architecture – ACGW



# Reference Architecture – ACN



# Section: Conclusion

- Objectives
- Future Work

# Project Objectives

- Improve terminal and NE integrity and security
- Improve attack detection and mitigation techniques
- Evaluate usage of cloud systems to support ASMONIA tasks
- Enable collaboration across administrative domains
- Definition of protection concepts to improve security of mobile network infrastructures

# Future Work

- Detailed specification of functional and security requirements of the introduced elements
- Evaluation if proposed components meet the defined requirements
- Definition of a flexible architecture for future modules and integration of interfaces to existing Early Warning Systems
- Simulation of proposed system architecture to validate practicability and performance of our approach

# References


[1] RFC 5636, Aug. 2009

[2] K. Bennett, C. Grothoff, T. Horozov, I. Patrascu, and T. Stef. Gnunet—a truly anonymous networking infrastructure. In *Proc. Privacy Enhancing Technologies Workshop (PET).(Mar. 2002).*

[3] K. Bennett and C. Grothoff. Gap practical anonymous networking. *Lecture notes in computer science, pages 141–160, 2003.*

[4] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos. Sepia: Security through private information aggregation. Technical report, Computer Engineering and Networks Laboratory, ETH Zurich, Switzerland, October 2009.