

# **Daidalos Security B3G-SA and Security Clusters Joint Workshop**



**23<sup>rd</sup> September 2005**

**Brussels**

**Riccardo Pascotto (T-Systems)**

**Dirk Westhoff (NEC)**

**Stephen Butler (LAKE)**





# Daidalos contextual assumptions

- ▶ **Mobility Beyond 3G**
  - Heterogeneity: multi-access, multi-operator
  - Mobility: terminal, person, session
  - Separation: transport, service infrastructure
  - Integration: handover, routing, A4C, Security, QoS, Service Creation & Provisioning
- ▶ **Media Convergence**
  - All-IPv6 network infrastructure
  - Teleservices, Broadcast Services
  - Sensor Services, Device Services
- ▶ **Pervasive Systems and Services**
  - Pervasive Service Platform incl. Discovery
  - Privacy
  - Context-based adaptive reconfigurability
  - Personalization concepts



# Daidalos security research objectives



- ▶ Provision of **multilaterally** secure infrastructure for users and providers:
  - To securely operate networks and services
  - To use pervasive services without giving away privacy
  
- ▶ Holistic approach supported in all parts of the system
  
- ▶ Sample security functions:
  - Secure protocols
  - Advanced key management for use in network and services
  - Security in all network technologies, e.g., also in *ad hoc/sensor networks*
  - Privacy & Security management to support usability for user, e.g. *identity & privacy model*





# Daidalos architectural tiers

- ▶ **Daidalos infrastructure is a 3 tier system:**
  - Top Tier: Pervasive Service Platform (PSP)
  - Middle Tier: Service Provisioning Platform (SPP)
  - Bottom Tier: Access Networks (AN)
- ▶ **PSP:**
  - Platform for pervasive services
  - Sample enabling services: Context Management, personalisation, security and privacy
- ▶ **SPP:**
  - Core network
  - Network services
  - Multimedia services
- ▶ **AN:**
  - Integrated access to core network by different technologies, e.g., WLAN, UMTS, DVB-H



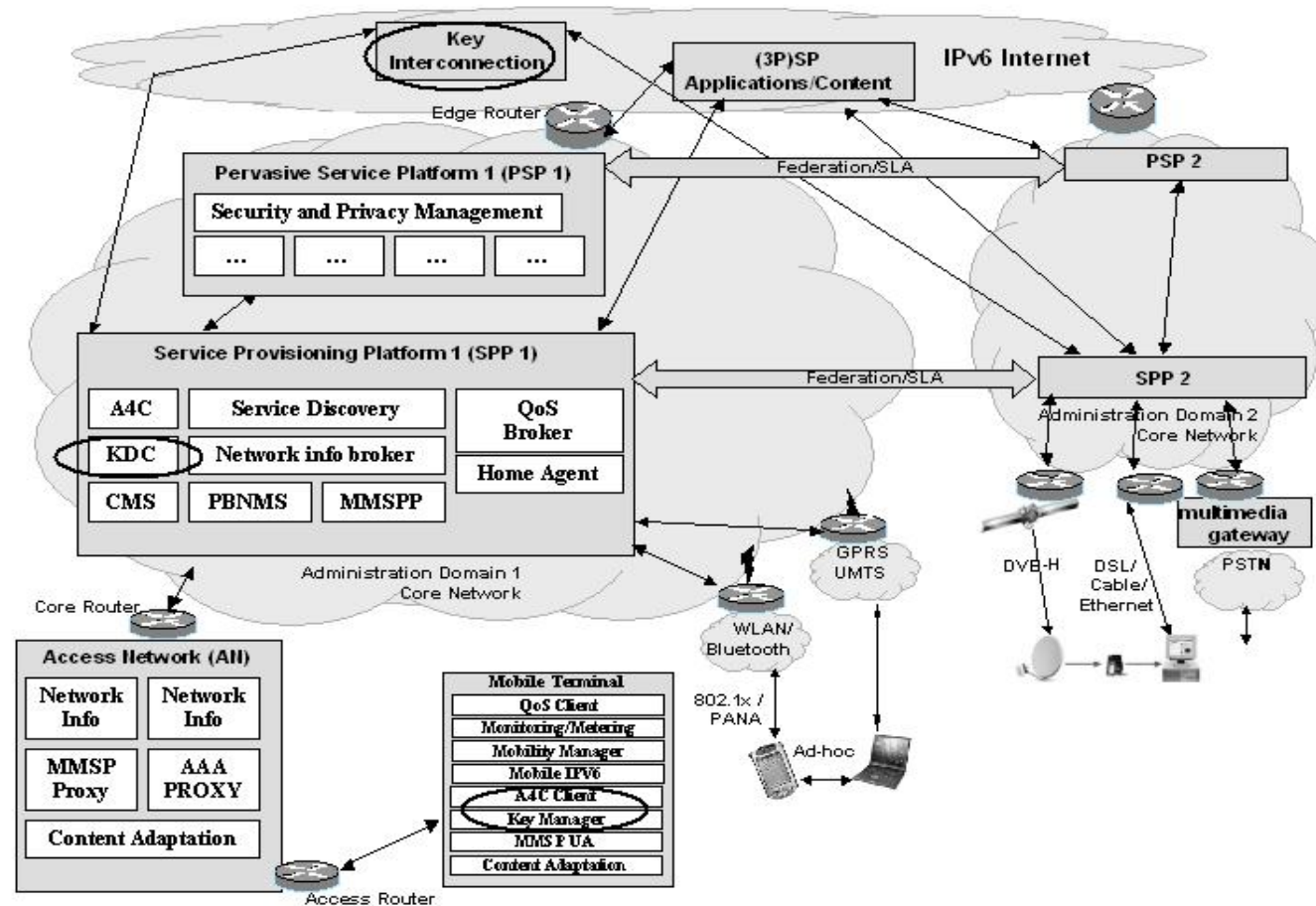


# Daidalos security architecture

Top Tier

Middle Tier

Bottom Tier



# Pervasive Service Platform Security



- ▶ **Pervasive Service Platform** collects, manages and distributes context data about users:
  - Context data typically very personal
  - Privacy protection is essential
- ▶ Integrated **security and privacy subsystem** based on a three step approach:
  - **Privacy Policy Negotiation:** Negotiates with a newly discovered service the terms of operation wrt privacy (e.g., context data to be disclosed)
  - **Identity Management:** Selects a suitable VID based on the negotiated privacy policy
  - **Credential Management & access control:**
    - Creates necessary authorizations for use of service and interfaces with the A4C for this
    - Verifies authorizations at time of context access by service



# Service provisioning platform security



- ▶ **Intra & Inter-domain key management**
  - Uses a common key manager to store certificates, key material, ID tokens etc.
- ▶ **Secure protocols:**
  - IPsec is deployed as the as the basic security protocol; hence, a means to distribute and manage cryptographic material not only within a single domain but also across domains is required.
  - Currently the KDC system is based on a Public Key Infrastructure (PKI) and its associated protocols.
- ▶ **Federated & Privacy enabled Access Control** based on SAML:
  - SAML used to integrate distributed authentication, authorisation and SSO.





# Access network security

- ▶ Cryptographically generated addresses (**CGA**) and secure neighbor discovery within the IPv6 access network.
- ▶ Integration of CGA and Mobile IPv6
- ▶ **SEND** and CGA integration for Ad Hoc networks.
- ▶ **PANA** as a bootstrapping protocol:
  - Provide the transport for independent access network and for EAP contents exchange
  - Network and associated services
- ▶ **SAODV** secure ad hoc routing.
- ▶ **SICP** derivate for secure incentive based charging in ad hoc networks
- ▶ **CDA** concealed data aggregation for end-to-end encryption in WSNs



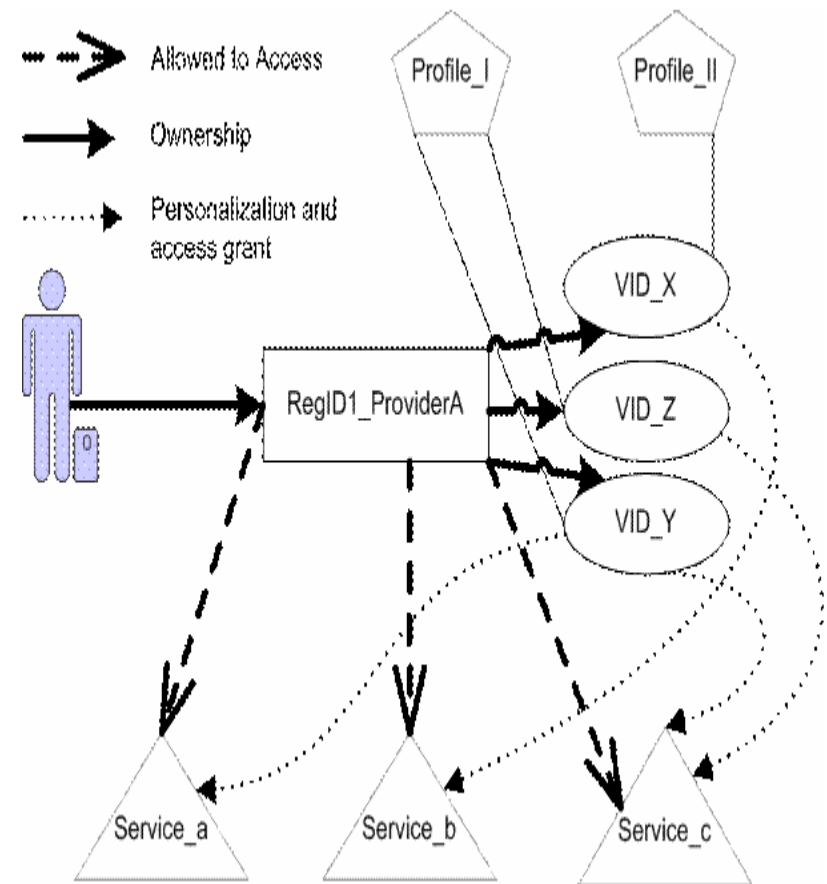


# Identity and Privacy model

- **Main paradigm - User control:**
  - Of disclosed personal information
  - Of trade-off: privacy vs. functionality, performance.
- **Basis:** Several virtual identities per user while still allowing for accounting etc.
- **Two level identity model:**
  - **RegID (*Registration Identity*)**
    - Assigned by a Daidalos operator
    - Holding conditions of contract and account info
    - Operator confidential and not transmitted over the network
  - **VID (*Virtual Identity*)**
    - Bound to a RegID
    - Mapping only on operator's subsystems
    - Share defined granularity of attributes and profiles
    - Provides different levels of privacy
- **Virtually unlimited set of "Virtual IDs" or Roles:**
  - **Mapping of VIDs to (contracted) user done in**

**A4C\_home**

Daidalos Security B3G-SA and Security Clusters Joint Workshop





# ID Tokens

- ▶ Introduction of an 'ID Token', residing on MT:
  - "Pointer" to current registration context in A4C\_home
  - "Identity Proof" of user
  - Small in size, time-limited validity
  - *Encrypted (with random) in each Request*
  - *Supports privacy and identity model using VIDs*
  - *Sequence-number to avoid replay-attacks*
  - *Digital signature over entire ID-token*
  - *Sensitive data encrypted with receiver's public key*

IDToken

Random Number	Serial Number	Artifact
Digital Signature (by using client's private key)		
VID = string@realm		



Clear text



Encrypted (with receiver's public key)





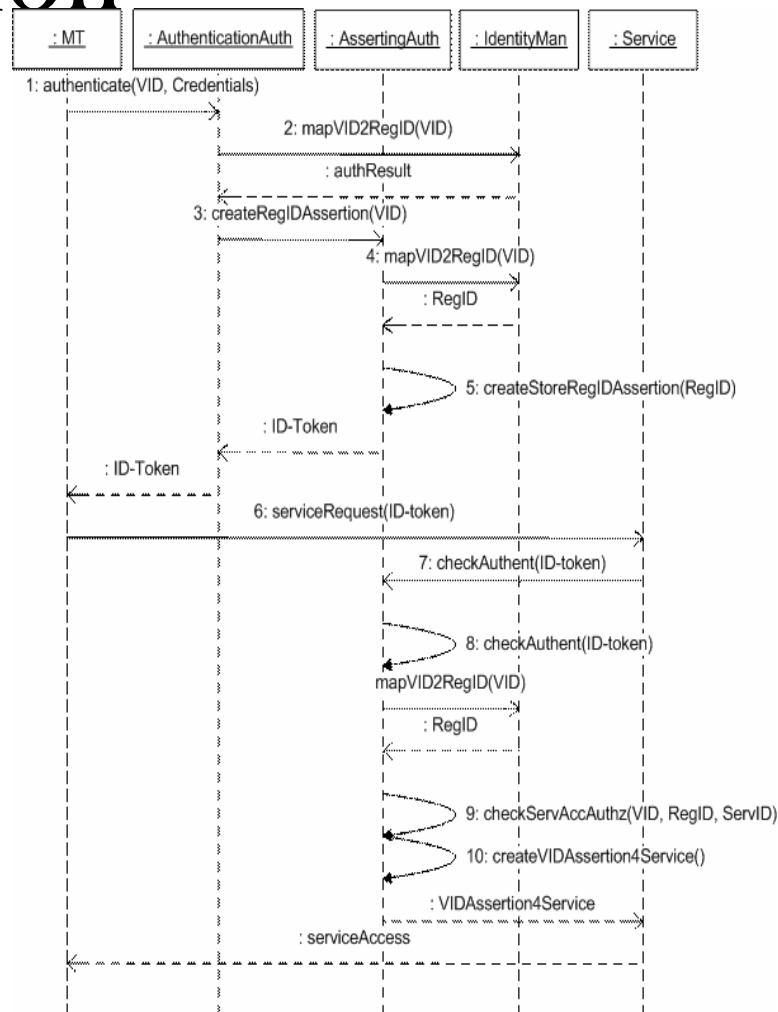
# IDs and authentication

## •Authentication phase & ID-token delivery:

- Selection of a VID depending on privacy level
- Verification of credentials
- Generation of assertion and ID-token related to RegID
- ID-token sent to MT and stored for further service requests

## •SSO and service-authorization:

- Selection of a VID and update of ID-token
- ID-token is sent to service
- AA information is requested from Asserting Authority
- Verification of ID-token
- Authorization check related to VID-specific profile
- Generate VID-specific service assertion to conceal RegID
- Transfer assertion to service



# Case Study: Sensor network



## security

### CDA: Concealed Data Aggregation

- merging data aggregation and E2E-encryption
- data need to be aggregated on its way to the sink node -> saves energy
- data aggregation function is context sensitive

**Currently:** data aggregation + hop-by-hop encryption, e.g. RC5 (single group key)

**Our proposal:** data aggregation + E2E-Enc.

### Pros:

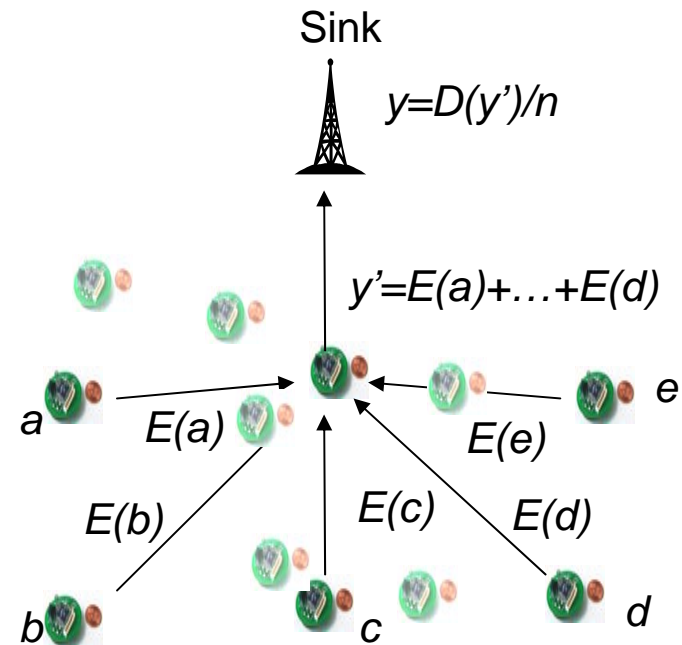
- saves energy consuming encryption operations in the backbone
- no lack of security at aggregating backbone nodes
- most flexible for aggregator node election process over different epochs

### How to achieve E2E-Enc. With CDA:

- additive (multiplicative) PHs

$$a+b=D_k(E_k(a)+E_k(b))$$

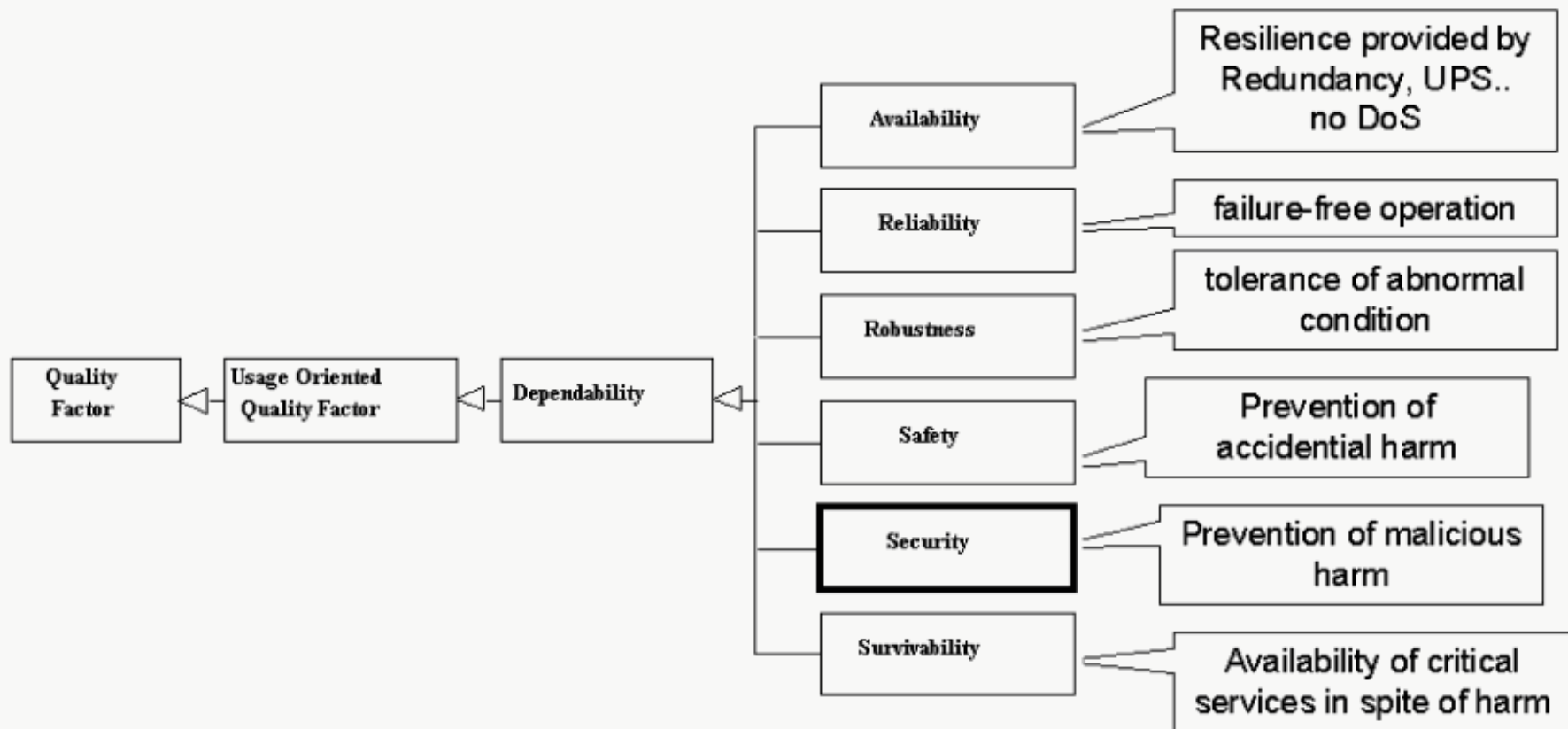
$$a*b=D_k(E_k(a)*E_k(b))$$



aggregation function "average"  
of n sensor nodes



# Activity 1.6 - Security Evaluation Criteria





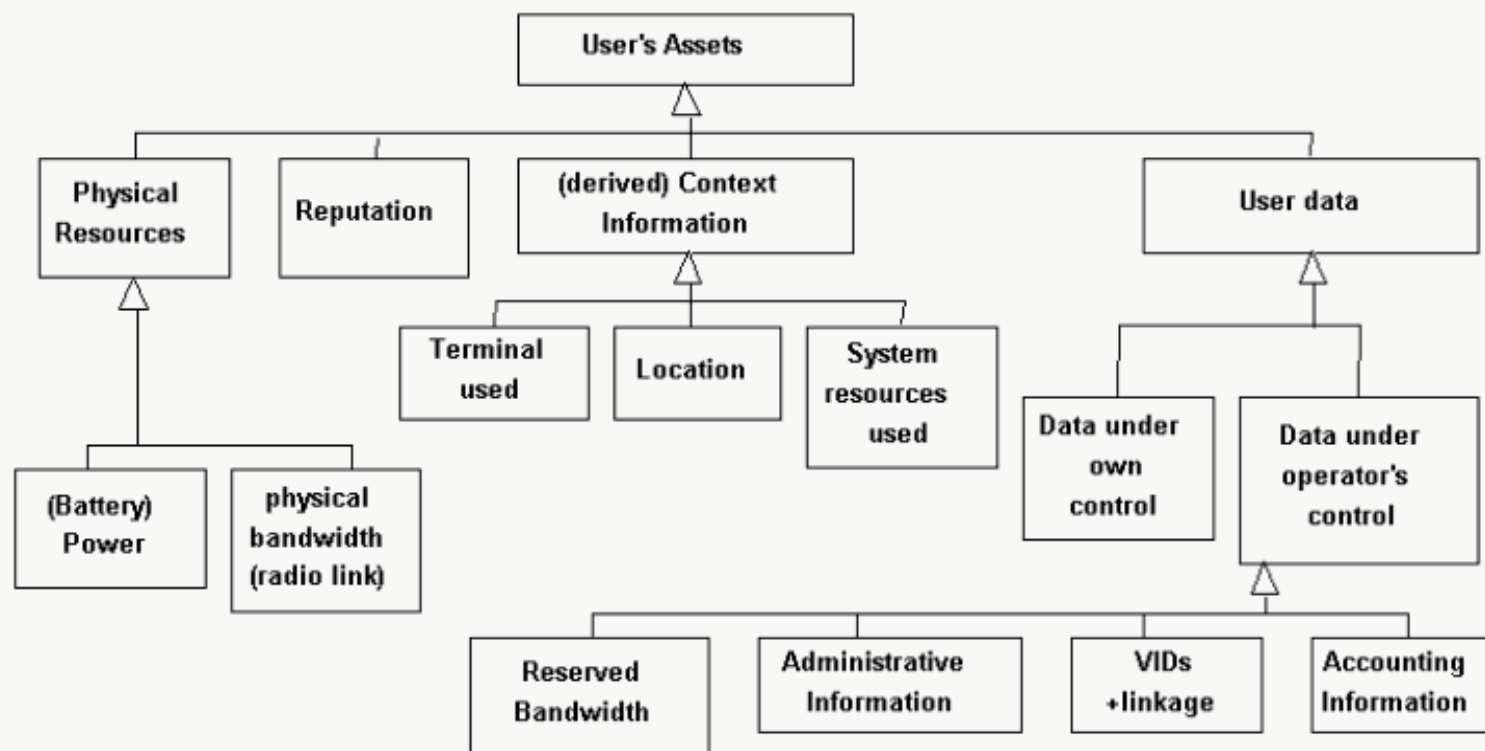
# Assumptions and methodology

- ▶ We evaluate a platform specification!  
(We do not know what components will be used for a production platform)
- ▶ we do not care for:
  - Implementation weaknesses
  - Protocol flaws
  - Demonstrators/prototypes
- ▶ Methodology
  - Collect assets of stakeholders
  - Define security policies
  - Define attacker models
  - check whether assets are protected against attackers by security policies
  - Go through each component and evaluate whether policies are fulfilled





# Example - user assets to be secured





# Conclusion

- ▶ A high performance and cost efficient converged multi-technology (broadcast/wireless/ mobile) seamless access network with overarching support of:
  - mobility (personal and device mobility)
  - **SA4C, QoS, Network Management...**
- ▶ Implement basic concepts in a compatible and consistent way **across all layers** (from the network up to the enabling services):
  - VID (Virtual Identity) separates the user from a device and enables privacy and personalization at all system levels.
- ▶ Include sensor networks also in phase II via cooperation with UbiSec&Sens

