On Security in All-IP Networks

◀BROADEN YOUR LIFE▶

Alcatel SEL AG
Matthias Duspiva

Agenda

> On wireless security

> What is AAA?

> AAA in All-IP networks

> Identity management

> Selected solutions

- IP-VPNs for end-to-end security
- Context transfer for fast handover

The scenario

- All terminals and services will be Internet compatible
- Services in All-IP networks:
  - **Internet Services** operated by Internet Service Providers (ISP),
  - **Application Services** operated by Application Service Providers (ASP) e.g. in banking and commerce,
  - **Communication Services** such as Unified Messaging or VoIP by Communication Providers and
  - **Media Services** by Content Providers.
- Revenue models develop from the pay-per-minute bill model in second generation networks to application and content based bill in third and fourth generation networks
- The revenue models for personal applications are:
  1. Fixed access fee based on the limited access resources.
  2. Minute or kByte bill model used in mobile telephony by mobile operators.
  3. Application licensing or upgrade model, also possible as Application Service Provider (ASP) model. Microsoft has been one dominant player here.
  4. Content delivery model, used in games and in audio or video distribution.

Source: Necsom Ltd, Finland

What security is about

> **Prevention** – before it happened
  - Authentication – are they who they claim to be?
  - Authorization – do they have permission to do it?
  - Accounting – a log or history of what happened

> **Detection** – when it happens
  - Intrusion detection
  - Intrusion tolerance (new research area)

> **Reaction** – after it happened
  - Damage assessment
  - Recovery
  - Forensics

Basic wireless security requirements

> **Confidentiality** of exchanges –
make sure that nobody can listen in.

> **Authentication** –
Certify the identities of the parties involved.

> **Data Integrity** –
assurance that data is not tampered with on its journey.

> **Non-repudiation** of transactions –
assure agreements are legally binding.

> **Availability** –
make sure that services are available anytime.

Specific wireless security risks

> In all-IP networks all of the Internet risks

- Identity theft, masquerade
- Theft of service
- DoS attacks (TCP, UDP, ICMP, GTP-U/C flood, HTTP request…)
- Viruses, worms, trojan horses
- Modification (Control flow – GTP-C…; Management flow – SNMP…, User data flow), replay, …

> Especially eavesdropping (passive attacks from a distance): violation of privacy and confidentiality

> Hardware limitations, such as low network bandwidth and limited battery power, also increases denial-of-service risk (a.k.a. resource depletion/exhaustion attacks)

Source, partly: Kai Hwang, University of Southern California

Some Security Requirements of the IMS

- User identity confidentiality (private ID not sent in clear)
- Mutual authentication between the user and the network or service provider
- Confidentiality protection of SIP messages (for payload on underlying layers)
- Data integrity protection for SIP signaling
- Visibility and configurability of security features (e.g. accept/reject non-ciphered sessions)
- Protection of location information (external service providers)

IMS: IP Multimedia Subsystem

Assumption

> Extremely vulnerable interfaces are:

- Interface to the external Packet Data Network (Gi)
  - Can be used to easily flood NEs
  - Masquerade as NEs
  - Integrity, Privacy violation of user traffic
- Interface to another PLMN (Gp)
  - Can be used to masquerade and perform DoS attacks
  - Flooding is also a concern but not very critical

Increasing Security Demand in M-Commerce and Pervasive Applications

- LANs, clusters, Intranets, WANs, Grids, and the Internet all demand security protection hacker-proof operations, crucial to the acceptance of a trust-based digital society
- Innovative mobile wireless services, E-transactions, telemedicine, and digital government; all demand high security, privacy protection, and data integrity.

Source: Kai Hwang, University of Southern California

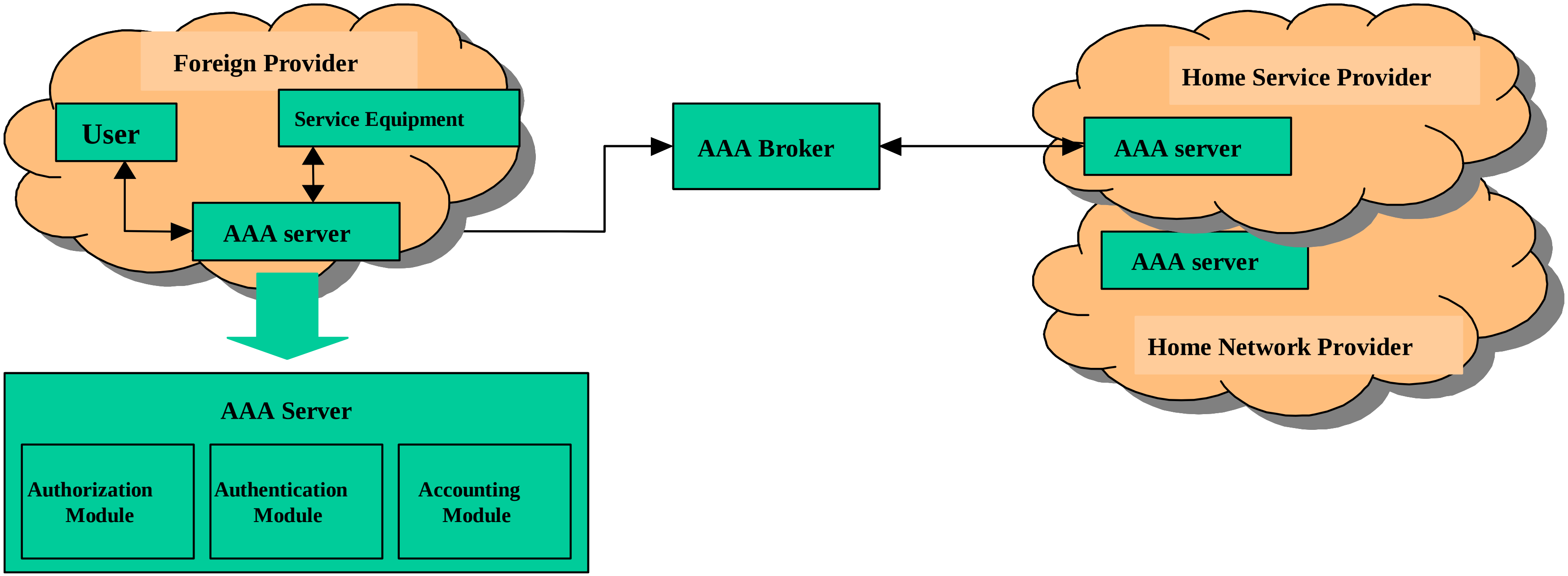
What is AAA?

> **Authentication**	who is who?
> **Authorization**	profile, permissions
> **Accounting**	who pays for what?

> AAA servers:

- Home AAA Server
  AAA server in the home network.
- Visited AAA Server
  AAA server in the network providing service when user is roaming outside home network.
- Broker AAA Server
  Intermediate AAA server(s) having security associations with Home and Visited AAA Servers.

AAA architecture



AAa

- RADIUS is the dominating AAA protocol in IP networks today, while Diameter is the successor of this well-known protocol. Diameter is currently standardized within the IETF AAA working group. Both RADIUS and Diameter are flexible and extensible protocols. Additionally, Diameter is built to be interoperable (backwards compatible) with RADIUS. Both the Diameter and the RADIUS protocols are and will be used for the fixed PSTN, cellular PPP kinds of dial-up users as well as roaming Mobile IP users.
- AAA provides Internet roaming services – i.e. the user is entitled the use of various access networks around the world, while keeping the users Internet service agreements with a “home Internet service provider”.

aaA

- The aaA function acts as storage buffer for near real-time charging data collection from the IMS nodes.
- Session Charging Function (SCF)
- Bearer Charging Function (BCF)
- Event Charging Function (ECF)
  - Subscriber Content Charging Function (SCCF)
  - Content Provider Charging Function (CPCF)

PN-4935.7 (TIA-873.7):
All-IP Core Network Multimedia Domain IP Multimedia Subsystem – Accounting Architecture

Authentication

- Online **identity**: IP address, phone no., Email address, IMSI, IMUI, … ?
- Credentials used to prove the identity and role (have, know, be)
- IP Multimedia Subsystem (IMS): strong user authentication in addition to network authentication makes it possible to access IMS from different access networks;
  SIP requires authentication at session level
- Approach: Layered authentication for network and service access; 802.1x, EAP-SIM, Radius, Diameter, WIM/WTLS
- EAP method used: the User Identity field carries the user identity composed by the Public User Identity and a Home Network Domain Name

Authorization

> Authorization is a MMCS function, it aligns service requests with the service agreement (subscription profile)

> Profile: subscriptions
>
> → Network/Service Access control
>
> → authorization for QoS

> Policy-based Authorization:

- Dynamic Home IP Address Allocation (DHCP).
- Network Access Control (time-of-day controls).
- Differentiated Service Delivery.

MMCS: Multimedia Call Server

Accounting

- Variety of services (aaA in SGSN for bearer, in S-MMCS for call control):
  - Communications (voice and data)
  - Transactions (m-commerce, micro-payment)
  - Value-added content (location based services, gaming, …)
- Customer billing on a usage or flat rate basis:
  convert all usage/charging records into mobile format and maintain relation to IMSI
- Wholesale billing between the network operator and content aggregators (portals, …), branding of the aggregator on the bill issued by the network operator
- Goal: unified bill for all services, predictable charging mechanism for usage per transaction / flat rate / volume / duration
- Problem: many subscriptions and connections to value-added service providers and content providers

Accounting, cont.

> Billing challenge:

- In 2G networks are all services provided by the operator and billing is based on the service usage
- 2.5G architecture made 3rd party services possible
- In all-IP 3G everybody can offer services to mobile users

- Amount of billing tickets increased: challenge to billing servers
- New billing model needed for 3G operators,
  not to end up just selling bandwidth

Source: WFI

Charging in an All-IP network

- The purpose of charging is to collect data on the network resource usage and services to enable the billing of the subscriber
- Charging layers
  - Access Layer: The charging for the usage of bearer resources (e.g. GPRS access services)
  - IP Multimedia Layer: The charging of services provided by the IMS (e.g. multimedia sessions)
  - Service and Application Layer: The charging of services provided by the service subsystem (e.g. games, location)

Source: Kati Lehtinen

Charging in an All-IP network, cont'd.

> Two separate charging architectures:
off-line and on-line charging architecture

- Off-line charging architecture provides a charging process where charging information does not affect, in real-time, the service rendered

- On-line charging architecture provides a charging process where charging information can affect, in real-time, the service rendered and therefore directly interacts with the session/service control

Source: Kati Lehtinen

3GPP AAA server

> The 3GPP AAA server is located within the 3GPP network.

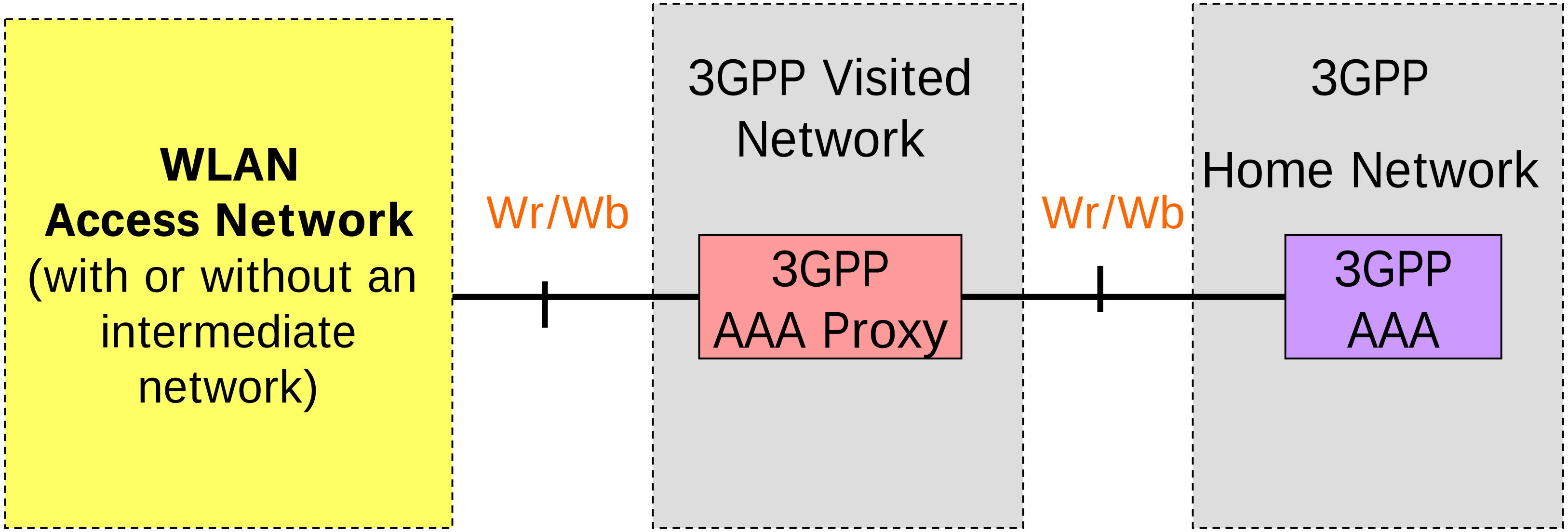
> The 3GPP AAA server :

- Retrieves authentication information and subscriber profile (including subscriber's authorisation information) from the HLR/HSS of the 3GPP subscriber's home 3GPP network;
- Authenticates the 3GPP subscriber based on the authentication information retrieved from HLR/HSS.
  - The authentication signalling may pass through AAA proxies.
- Communicates authorisation information to the WLAN potentially via AAA proxies.
- Registers its (the 3GPP AAA server) address or name with the HLR/HSS for each authenticated and authorised 3GPP subscriber.
- May act also as a AAA proxy (see next slide).

Source: WFI

3GPP AAA proxy (1)

- The 3GPP proxy AAA functionality can reside in a separate physical network node
- It may reside in the 3GPP AAA server or any other physical network node
- It represents a Diameter proxying and filtering function that resides in the visited 3GPP network.



Source: WFI

3GPP AAA proxy (2)

> The 3GPP proxy AAA functions include:

- Relaying the AAA information between WLAN and the 3GPP AAA Server
- Enforcing policies derived from roaming agreements between 3GPP operators and between WLAN operator and 3GPP operator
- Reporting charging/accounting information to local Charging Collection Function(CCF)/Charging Gateway (CGw) for roaming users
- Service termination (O&M initiated termination from visited NW operator)
- Receiving authorisation information (Subscriber information)
- Forwarding authorisation information to WLAN

Source: WFI

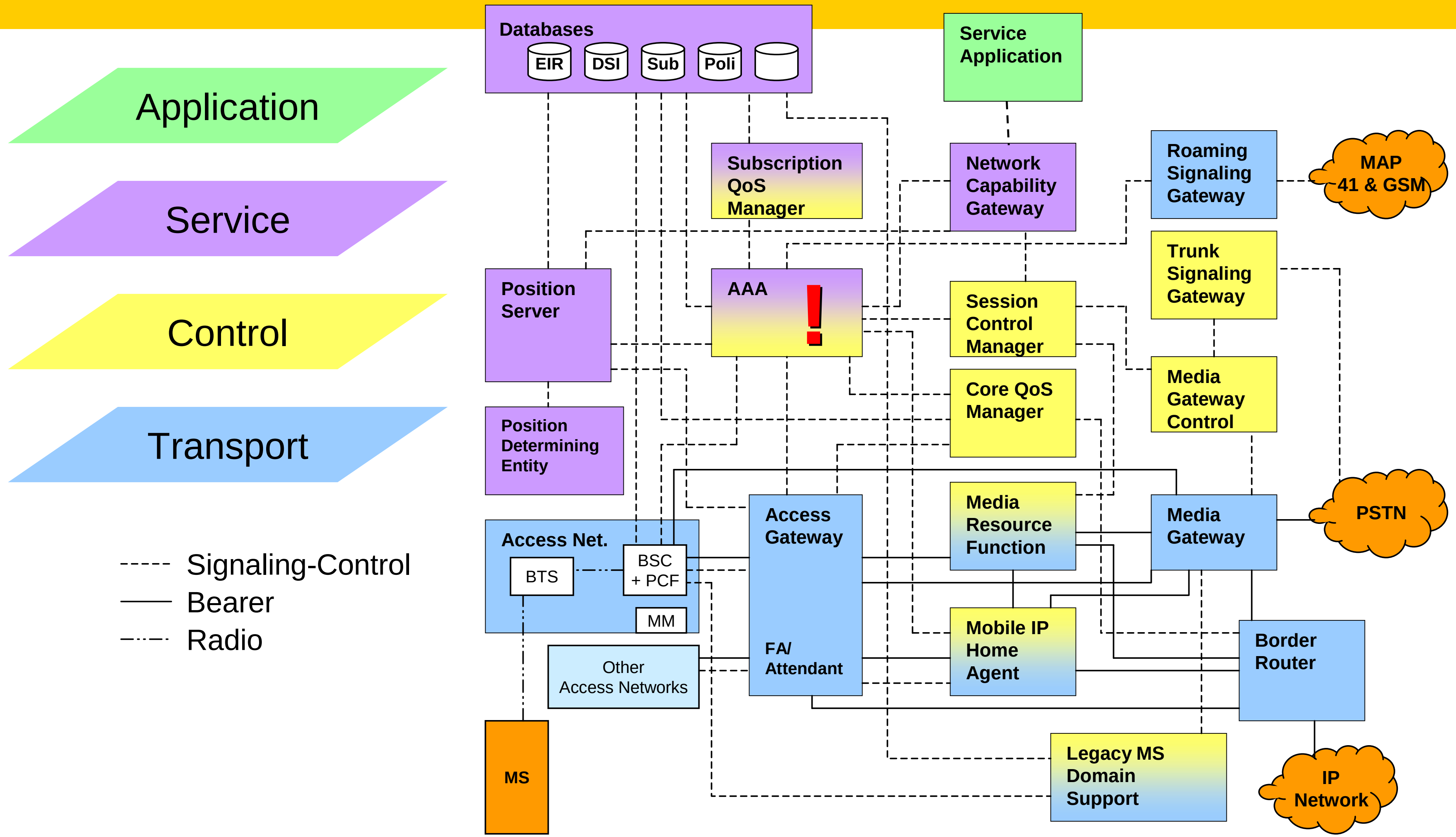
3GPP, 3GPP2

- **3GPP** uses GGSN, SGSN nodes.
- 3GPP does not allow heterogeneous access.
- The HLR is likely to be used by the SGSN for authenticating data users. Thus, access and data network authentication are integrated.

- **3GPP2** uses mobile IP and PSDN as FA/HA .
- It allows heterogeneous access.
- The PSDN uses an AAA infrastructure to authenticate data users. Access and data network authentication are separate.

Source: Sridhar Machiraju, University of California at Berkeley

3GPP2 All-IP Network Architecture Model



Source: Sridhar Machiraju, University of California at Berkeley

Interfaces of the border gateway

> The interfaces between the network elements are referred to in the specifications as **reference points**. They are:

- ~~Wr: Connects WLAN AN to the 3GGP AAA server~~
- ~~Wx: Located between the 3GPP AAA server and the HSS~~
- ~~D'/Gr': Located between the 3GPP AAA server and the HLR~~
- ~~Wb: Located between the WLAN AN and the 3GPP network~~
- ~~Wo: Used by a 3GPP server to communicate with the OCS~~
- ~~Wf: Located between the 3GPP AAA server and the CCF/CGw~~
- ~~Wn: Tunnels WLAN user data towards the 3GPP system~~
- ~~Wi: Connects the PDGW and a Packet Data Network~~

And what about end-to-end security?

> IMS mainly relies on PS network physical security:
> for more security use application security on top of IP

> Use IPSec to establish end-to-end security associations, e.g. for corporate access; policies for

- Access control (access for trusted traffic only)
- Security coverage (nodes, domains, areas)
- Content access (for trusted Proxy, Intrusion Detection System)

> Use SSL/TLS for point-to-point transactions

> Authentication by shared keys (IKE) or PKI Digital Certificates

> Use Intrusion Detection Systems, antivirus software, etc.

Security Model

> The mobile networks implement with AAA the classical model of restricted access systems

> SIP requires more mechanisms,
> e.g. phone or instant messaging spam control
> (black list / white list), in order not to end up like Email,
> or to help increase data privacy

> Several stages of access control and access mobility require a lot of identities and credentials for

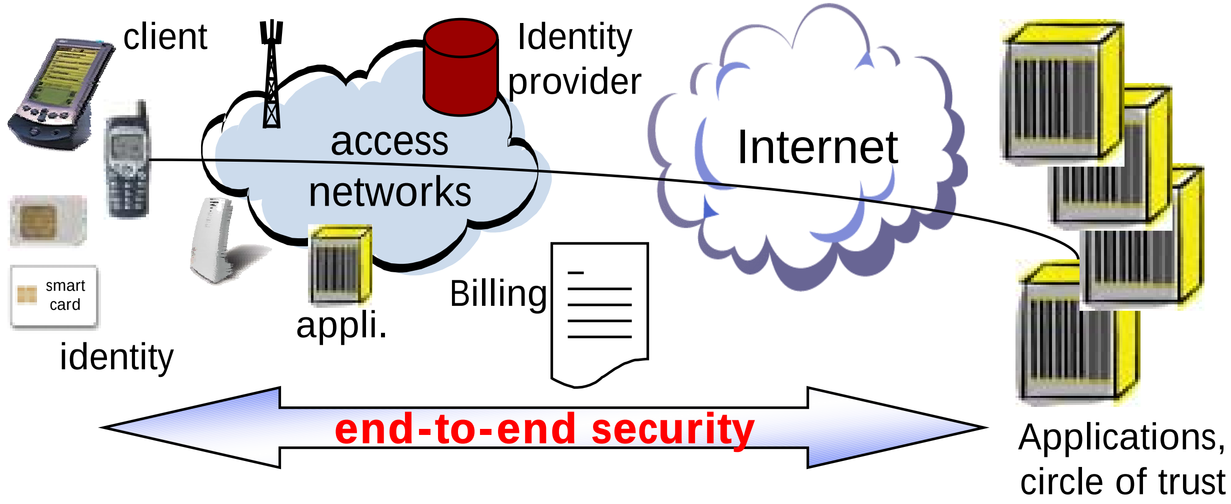
- Mobile network access, wireless network access
- MNO service access
- ISP network access
- Internet service access

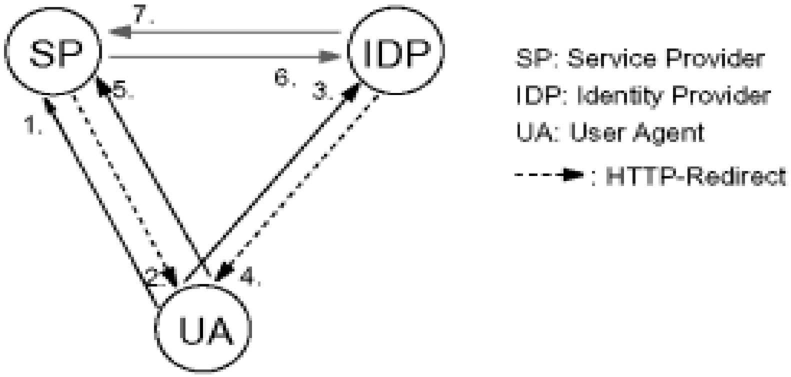
Approaches for (user) identity management

> Network access

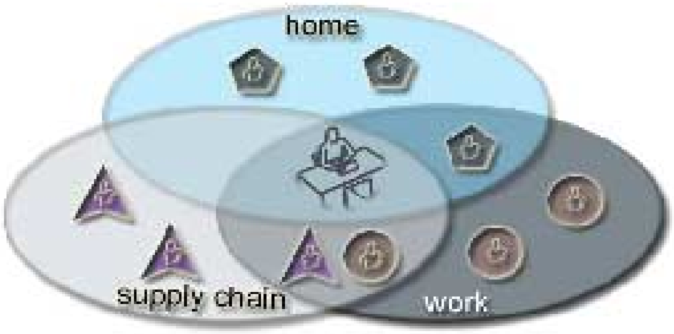
> Service access

> Identity federation (Liberty Alliance): single sign-on, etc.



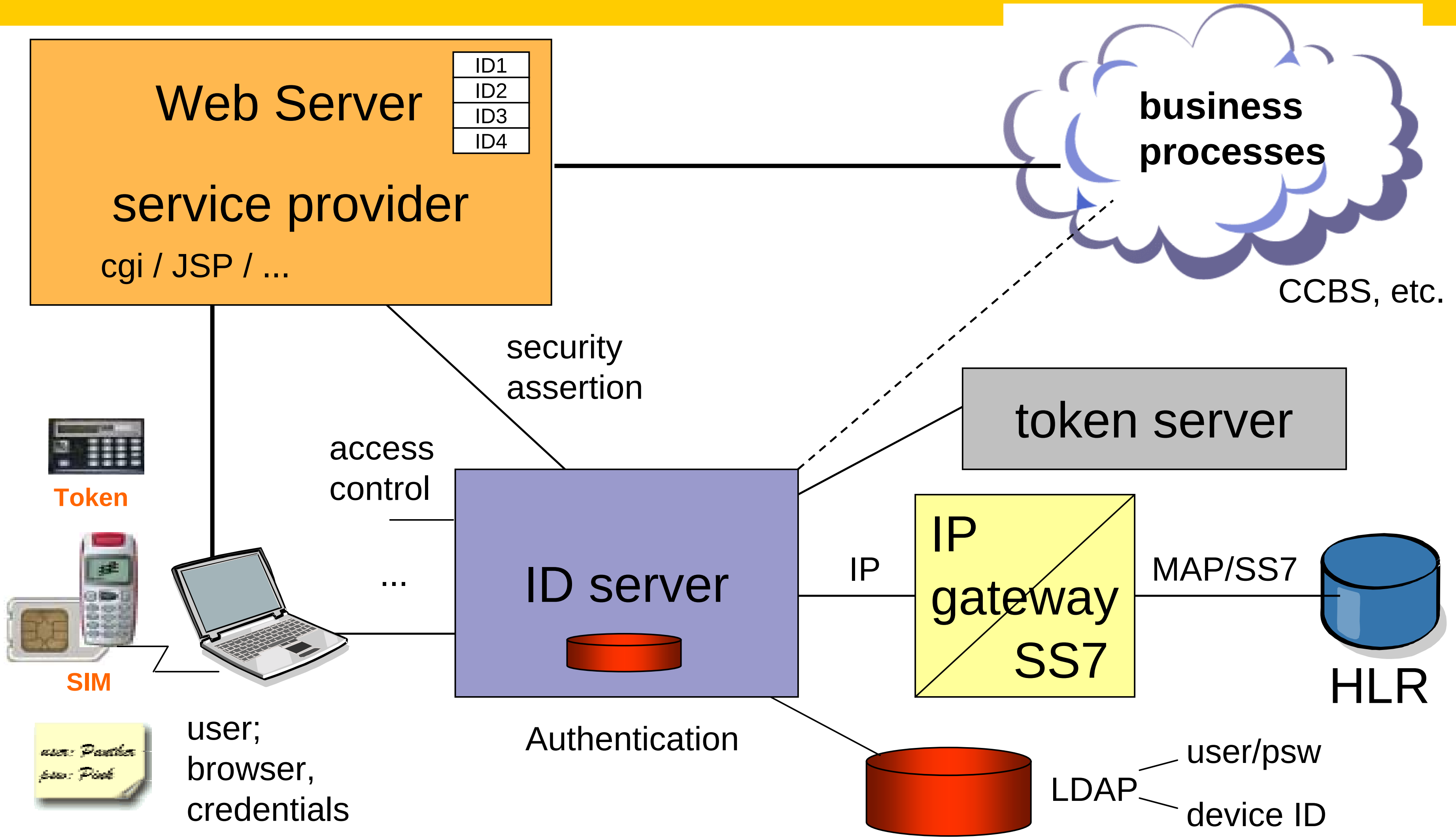


Authentication



Circles of trust

Identity Federation



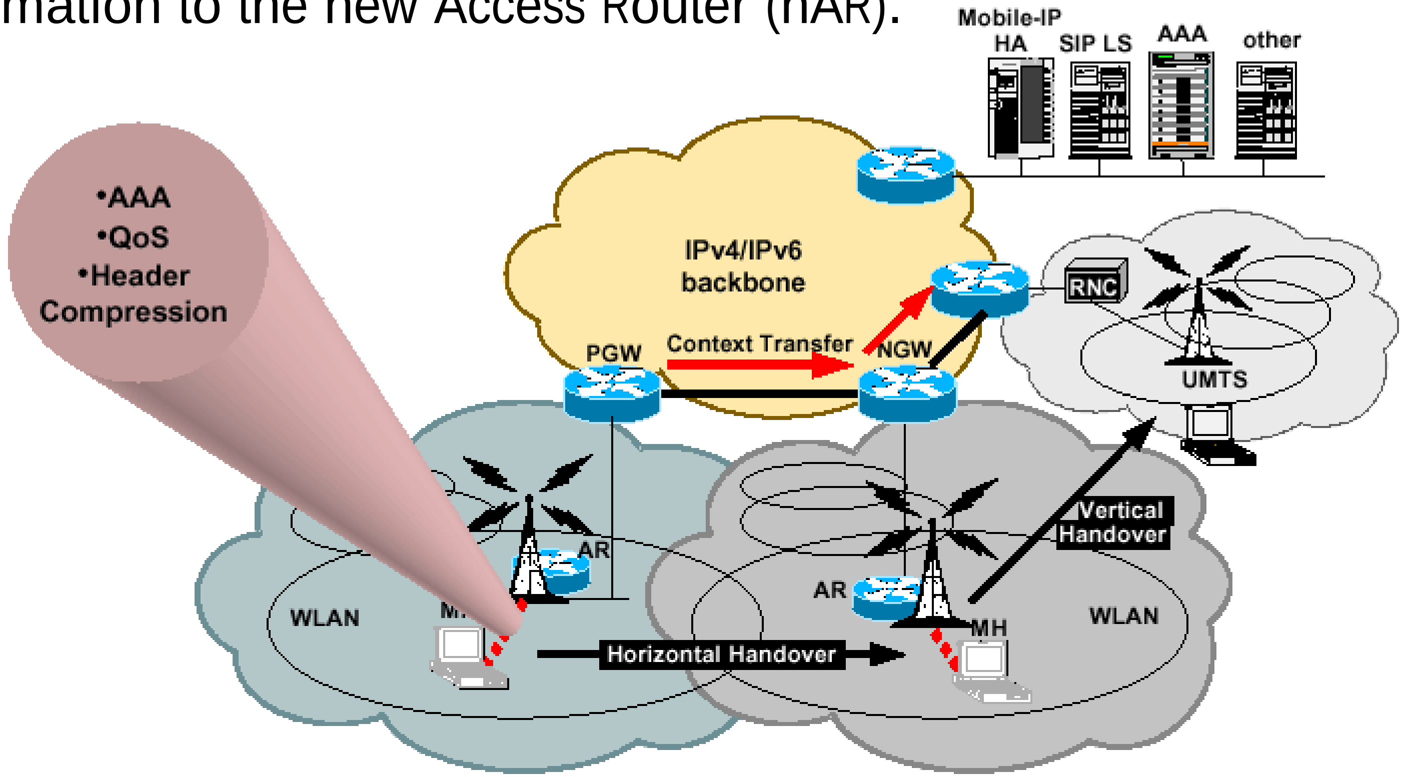
Issues

- Fast and secure: the mobility scheme should support different levels of security requirements such as data encryption and user authentication, while limiting the traffic and time of security process e.g. key exchange.
- From a handoff performance perspective, one of the key issues in the development of a multilayer mobility management scheme is minimizing the handoff delay while a mobile host is roaming across the homogeneous/heterogeneous networks.
- AAA adds an undesired delay component.

Example of an Approach for fast HO

> IST Evolute (FP5) proposes a context transfer mechanism to minimize and if possible eliminate the additional delay introduced due to AAA security provisioning. Context transfer forwards the AAA pre-established information to the new Access Router (nAR).

“Context Transfer” aims to contribute to the enhancement in handover performance. When a mobile node (MN) moves to a new subnet it needs to continue certain transport- or routing-related services that have already been established at the previous subnet. Such services are known as ‘context transfer candidate services’, and examples include header compression, QoS policy, AAA profile and IPsec state.



Conclusion

> Extremely complex architecture (Access, Core, IMS, Internet)

> Not all domains under control of the Mobile Network Operator

> Mobility follows AAA; fast horizontal and vertical HO

> Limited bandwidth and requirements on spectrum efficiency influence the choice of the security protocols

> Many research projects and standardization work ongoing to find solutions

References

- IST-2001-32449 Evolute project
- Nokia OMA, http://www.openmobilealliance.org/
- Microsoft .NET, http://www.microsoft.com/net/
- GRID Forum, http://www.gridforum.org/
- Liberty Alliance http://www.projectliberty.org/
- draft-kroeselberg-sip-3g-security-req-00.txt