



Challenges of Identity & Authentication in a Ubiquitous Environment – The Daidalos perspective

**Public Workshop on Security Issues
in Mobile and Wireless
Heterogenous Networks**

6th December 2004, Brussels

Stephen Butler

LAKE Communications





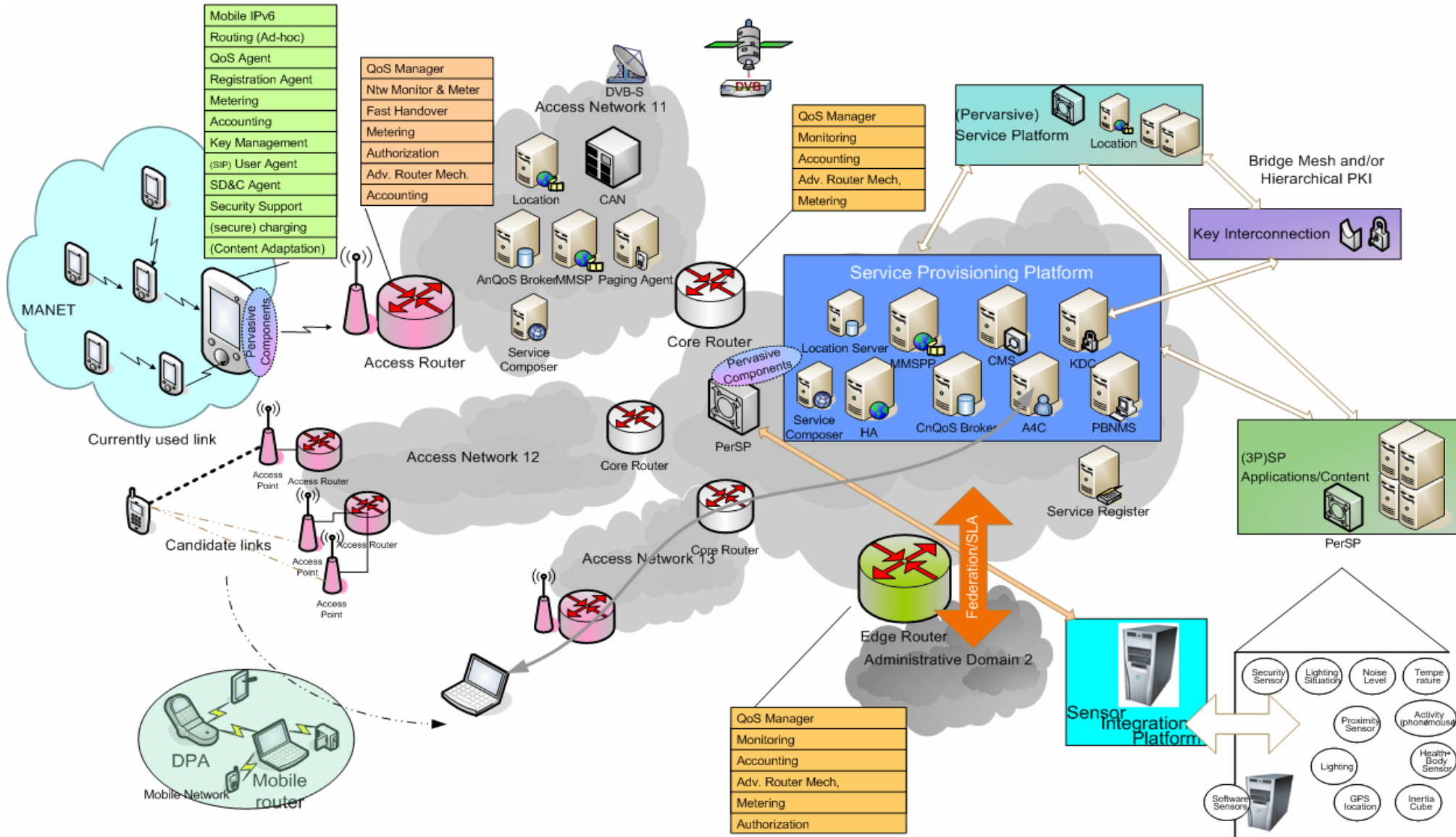
Daidalos technical context

Within the context of IPv6 and mobile IP, the technical goals of Daidalos are to:

- Design, prototype and validate the necessary infrastructure and components for efficient distribution of services over diverse network technologies beyond 3G,
- Integrate complementary network technologies to provide pervasive and user-centred access to these services,
- Develop an optimized signalling system for communication and management support in these networks,
- Demonstrate the results of the work through strong focus on user-centered and scenario-based development of technology.

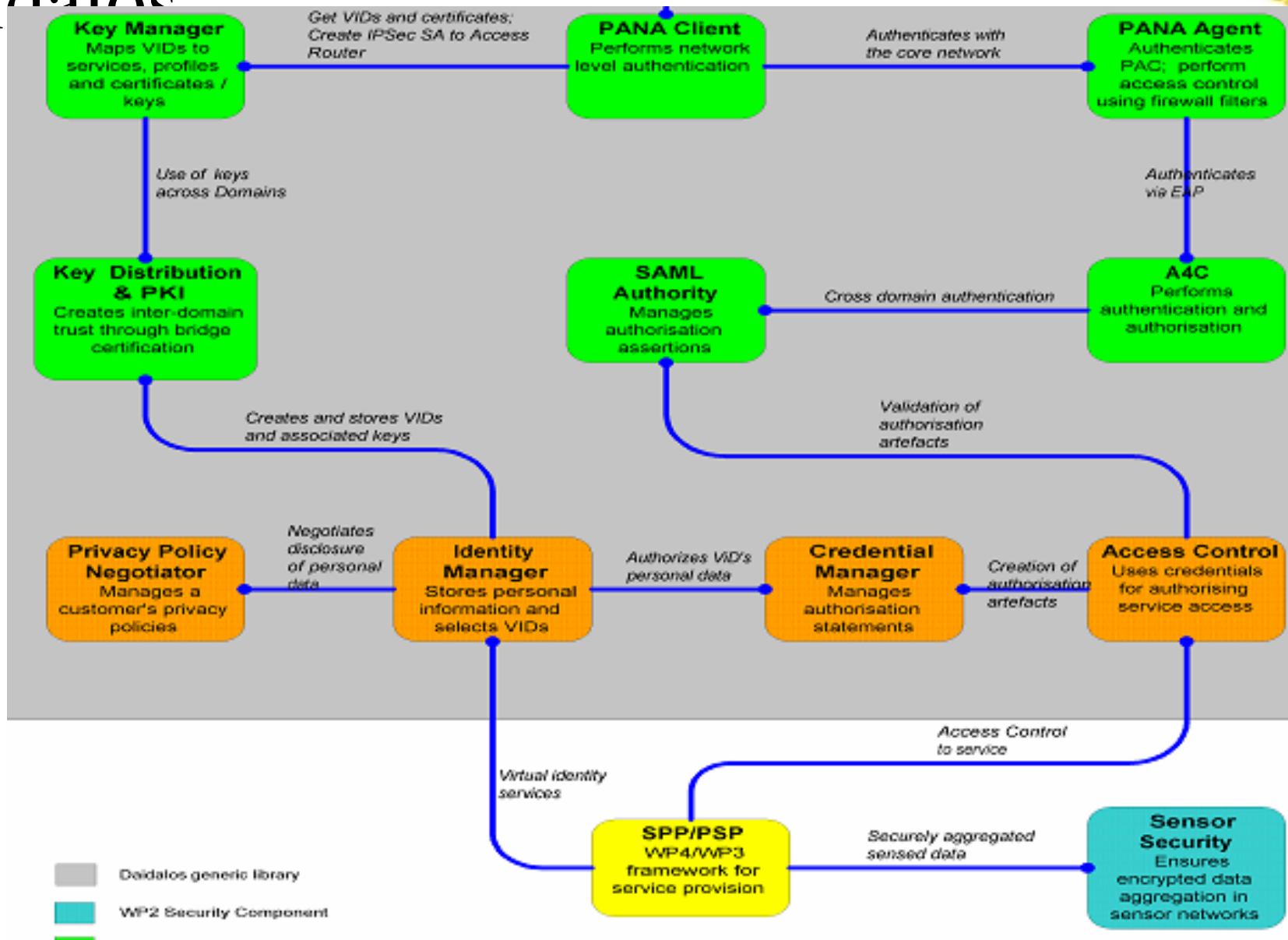


Daidalos Architecture



Security Components of

Daidalos





Daidalos goals related to Identity

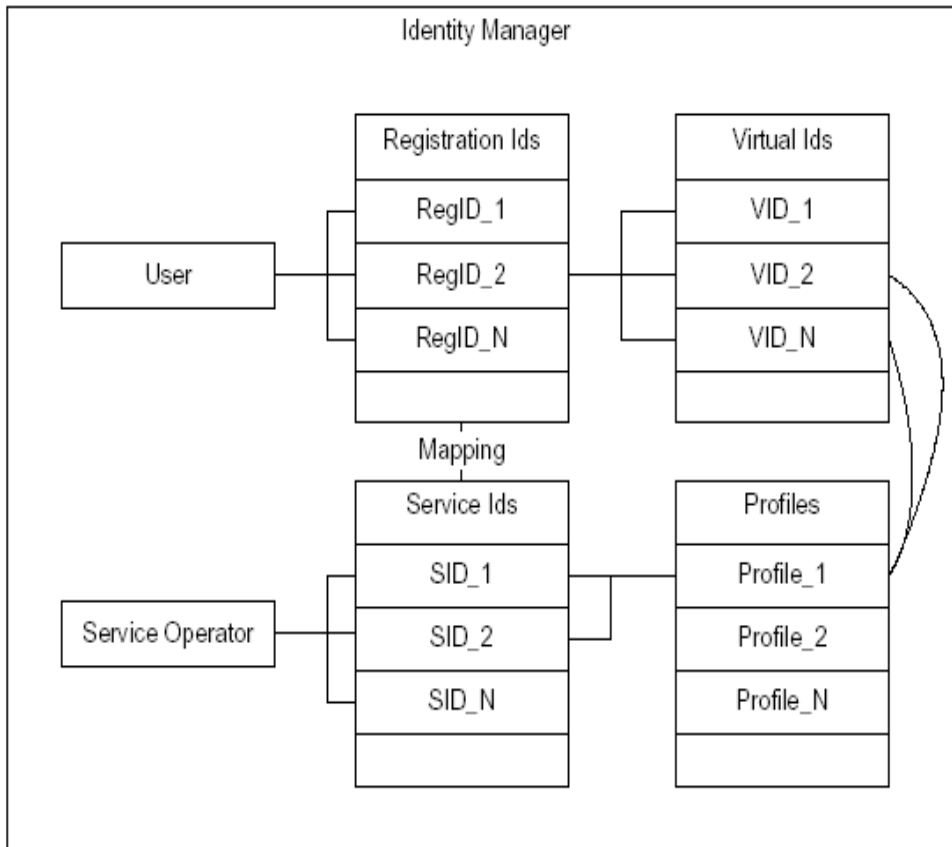
- ▶ Fine-grained user controlled privacy through profiles.
- ▶ User confidence in privacy
- ▶ Enhanced levels of privacy through privacy tokens
- ▶ Inter-work with a heterogeneous set of service discovery protocols.
- ▶ Service discovery must scale from simple peer to peer to an enterprise services.
- ▶ Context aware discovery - facilities and location will determine service availability and levels.



Types of identity

- ▶ Layer 1: Physical or Corporeal identity
- ▶ Layer 2: Layer 1 + full attributes of a person - mood, history location etc.
- ▶ Layer 3: Relational ID - ID which implies a (social) contract. E.g. Driving licence or mobile phone number.
- ▶ Layer 4: Virtual Identity - an artifice by which a person can control the privacy of their Layer 3 identities.

Entity mappings in ID management



- User 1<->* RegID
- RegID 1<->* VID
- Service Operator 1<->* SID
- VID *<->1 Profile *<->1 SID
- A profile may lead to a number of VIDs being created for the use with different services.
- One profile may apply to a number of services from the same service provider:
- What can a user do in their profile manager:
 - Control exposure of private information - e.g. location or bank account details.
 - Specify how and when VIDs are to be created.
 - ViD = RegID reference plus “right to use” certain private data.
 - Associate profiles with services to which they have subscribed. E.g . “My buddyfinder service may expose my location service to my buddies but not my QoS preferences...”

Profile and policy in VID negotiation



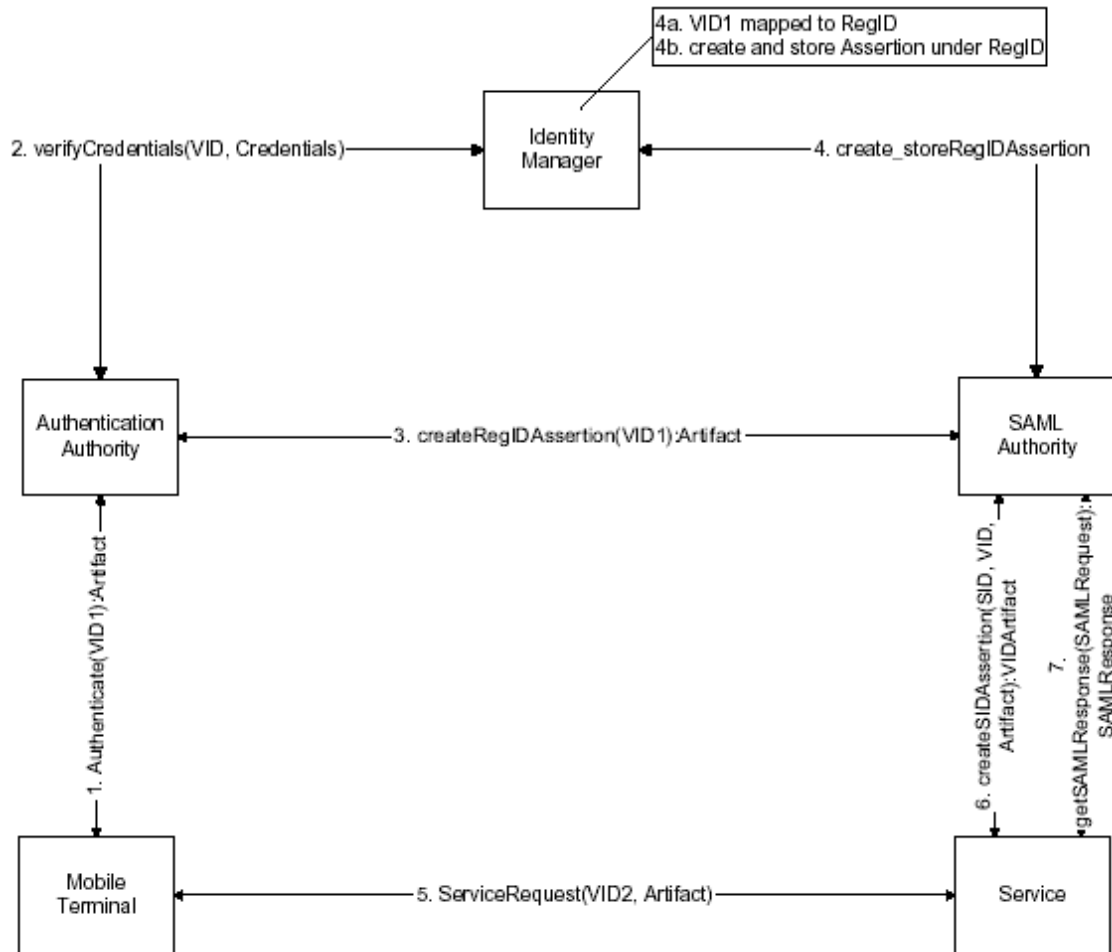
- Identity Manager, Privacy Policy Manager and Context Manager interact in the user's Mobile Terminal and on the Service Provisioning Platform.
- Privacy policies define rules for exposure of private data. Other policies (e.g. QoS specifications, appearance) exist.
- Services require the use of contextual information and the Context Manager mediates these.
- A Privacy Policy and Context negotiation takes place between the user's PPM and the service provider to either:
 - a) Choose an existing VID or
 - b) Create a new VID for this session.



RegIDs and VIDs

- Each operator assigns one RegID to each customer. This RegID is unique in the operators domain. The RegID is operator confidential.
- Services are accessed with a VID. All customers will have to use at least one predefined VID. Additional VID can be defined by the user.
- The operators authentication and charging unit are the only components allowed to do the mapping from VID to RegID.
- Each VID is associated with a RSA key pair issued by the operator. This key pair is used to sign the authentication assertion artefact and to build the IPsec tunnel.
- Single Sign On over multiple operator domains will require either a globally defined name space guaranteeing ID uniqueness or "identity mappings" (e.g. mapping/federation of VIDs) between operators.
- In the case of Single Sign On over multiple operator domains, the RSA key pairs associated with the VID must be generated and certified by a trusted third party.

Authorisation using SAML artefacts



- Negotiation agrees a specific VID for authenticating at the authentication authority (1).
- The Identity Manager verifies the credentials provided and indexes these under the VID in use(2).
- The authentication authority requests the generation of an authentication assertion based on the successful authentication of the user with his VID (3).
- The SAML authority maps the VID to the RegID via the Identity Manager, creates an authentication assertion and artefact and stores it (4).
- The artefact is sent to the Mobile Terminal, where it is stored for further service requests. A user can choose a certain VID for accessing a service. The SAML artefact is included in the request (5). This is encapsulated in a Privacy Token.
- The policy enforcement point of the service requests information on the users successful authentication and authorizations from the SAML authority (6).
- Because the service is not allowed to obtain the authentication assertion directly related to the RegID, it requests to create an assertion for the actual used VID which can be obtained via the respective artefact (7).



Privacy Token Structure

SAML Authority Identifier	Artifact	Virtual Identity	Timestamp / Sequence Number
Not encrypted	Encrypt (SAML_Authority_Public_Key/Symmetric Key)	Sign(VID_Private_Key)	
Sign(SAML_Authority_Private_Key)			
Not encrypted	Encrypt(SAML_Authority_Public_Key)		

- ▶ First part (dark Grey) issued by SAML authority.
- ▶ SAML authority ID never encrypted - so we know where to go to for verification.
- ▶ Authorisation Artifact is encrypted so authorisation is private to reading outside the SAML authority.
- ▶ MT adds ViD (could be for session, could be one-off per transaction - increased anonymity).
- ▶ MT also adds timestamp / sequence number to prevent replay attacks and data mining. This can be used to limit the lifetime of Privacy Tokens.
- ▶ MT signs with the ViD private key - only really valuable where ViD manufactured in the MT.
- ▶ Whole thing is encrypted with the Public Key of the SAML authority to prevent intercepted reading between the MT and the SAML authority.
- ▶ Traffic analysis limited to “some parties/party on MT X have used service Y”.
- ▶ Problems - more encryption work in the MT and the SAML authority.

Data hiding within the Service Provisioning Platform and the Access



Network

- ▶ Access network traffic analysis further frustrated by the use of IPSec tunnels between Mobile Terminal and Access Router
- ▶ The only information a service provider sees in an authorisation artefact is a SAML authority identifier. At the point of authorisation a service provider does not know who is being serviced.
- ▶ If an adequate separation exists within the federated A4C infrastructure, only the anchor service providers ID manager need know the linkage between VIDs and RegIDs.
- ▶ It is possible to hide (depending on policy) this information from billing authority providing only aggregated service charges depending on user's privacy policy.
- ▶ Hooks exist in the IDM for exceptional law enforcement contingencies.