



International Telecommunication Union

Digital Identity Management Towards Ultimate Network Security

Jiwei Wei

**Security Architect, Huawei Technologies
Co., Ltd.**

ITU-T Workshop on "Digital Identity for NGN"
Geneva, 5 December 2006

- o Threats defined in X.800
 - Destruction of information and/or other resources
 - Corruption or modification of information
 - Theft, removal or loss of information and/or other resources
 - Disclosure of information
 - Interruption of services

- o Threats to NGN interfaces:
 - User-to-Network Interface (UNI): interception for user ID and/or other authentication information, session contents
 - Network-to-Network Interface (NNI): protocol transformation, protocol leak, Virus, DoS, interception, entity masquerading
 - Application-to-Network Interface (ANI): Illegal information and activity, third party service DoS;
 - Internal interfaces: entity masquerading, interception, connection broken



ITU-T

Security threats to NGN

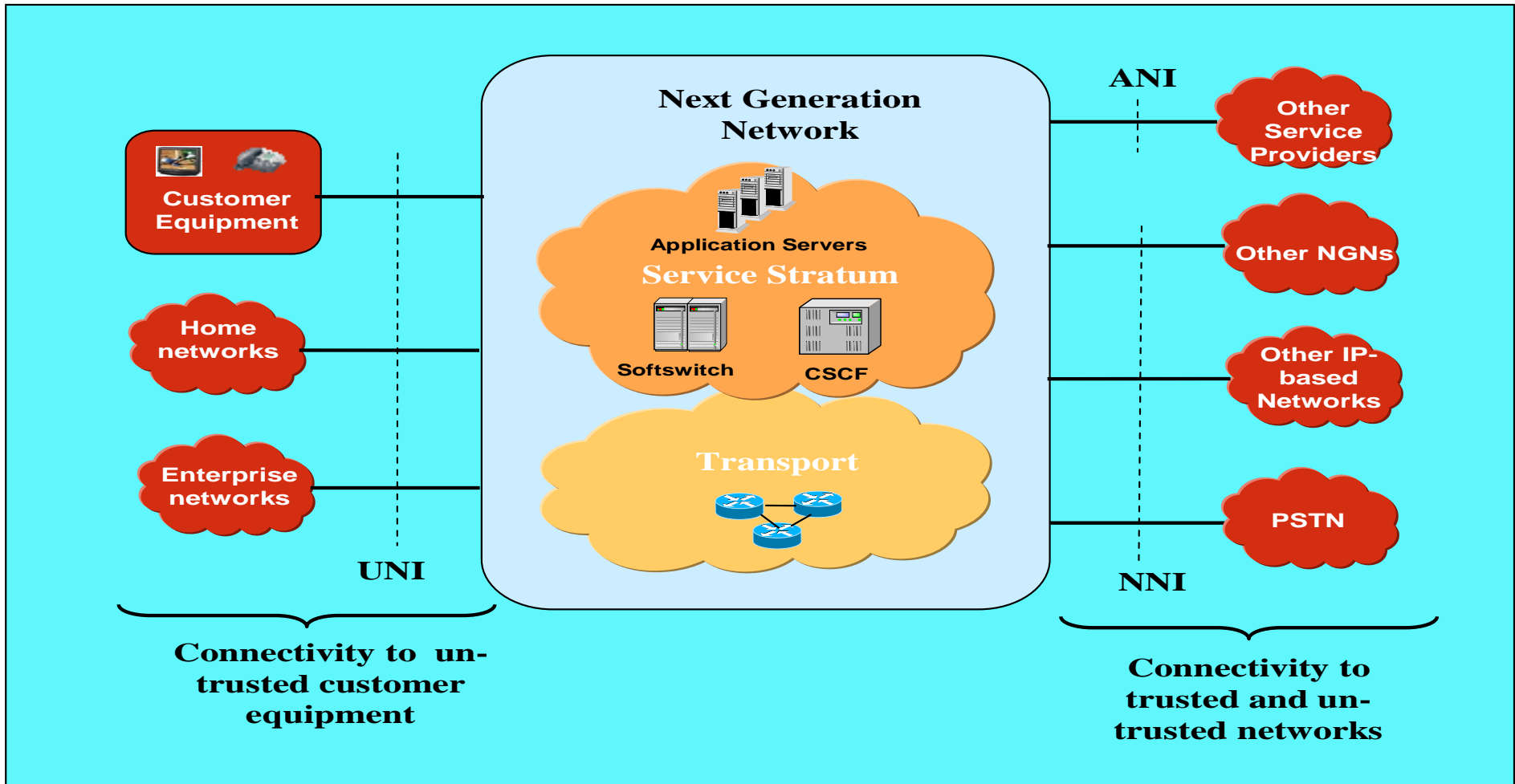


Figure – Connectivity to networks and users
(Source: Draft ITU-T Recommendation Y.2701)

- o Threats to Identities in NGN:
 - Embezzlement of user ID - similar to terminal users of traditional telecom networks, NGN user's ID relates to service provisioning and accounting. User identity authentication faces more challenges
 - Network entity masquerade - network or end users may suffer serious consequences when key network element such as Soft-switch or CSCF in core network is masqueraded. Entity Identity needs to be effectively managed.

Requirement for NGN Identity Management

- o Internet access
 - E.g. PPP Protocol over Ethernet (PPoE), based on password authentication, user/password as the identity
- o Telecom network access
 - Usually they require more restrict authentication, e.g. network access authentication for 3G user using IMEI (mobile equipment identifier) plus user identifier
 - E.g. 3GPP IMS AKA provides user and network mutual authentication

Requirement for NGN Identity Management

- o New Access Control protocols fit for NGN and jointly working with IdM system may be needed. IdM must supports diverse needs and types of identifiers of NGN
- o Other security mechanisms, e.g. privilege management, requires open interfaces through which IdM can provide identity services to them

Security focusing on identity management

- o Network access identity
 - User/password
 - IP address, MAC
 - IC card
- o Service access identity
 - User/password
 - Single Sign On (SSO)
- o Still way to go to meet the higher requirements for IdM of highly complicated telecom networks

Security focusing on identity management

- o NGN security focusing on IdM
 - IdM acts as a basic security platform to support network security functions and mechanisms, providing identity/identifier related security services
 - IdM service applied to multi-layer/multi-objects via open standard interfaces and APIs
 - IdM adapts to complicated network structure while keeps itself a simple, isomorphic model independent of heterogeneous network environment; it features dynamically homogeneity (behaving like Peer to Peer) while statically heterogeneity (constructing trust chain through authority identity)

Security focusing on identity management

- o IdM could be a powerful tool for trace back of attackers
- o A comment of TNC
 - For network access authentication of terminal, user identity (authentication) are binding with device identity profile (HW/SW integrity info)

- o Possible IdM mechanisms for NGN
 - Constructing association relationship between network access identity and service access identity, e.g. universal identity profile
 - Define ubiquitous identifiers including user/person and device/entity of NGN
 - Integrating privilege attributes info with identity profile, e.g. to support PMI applications

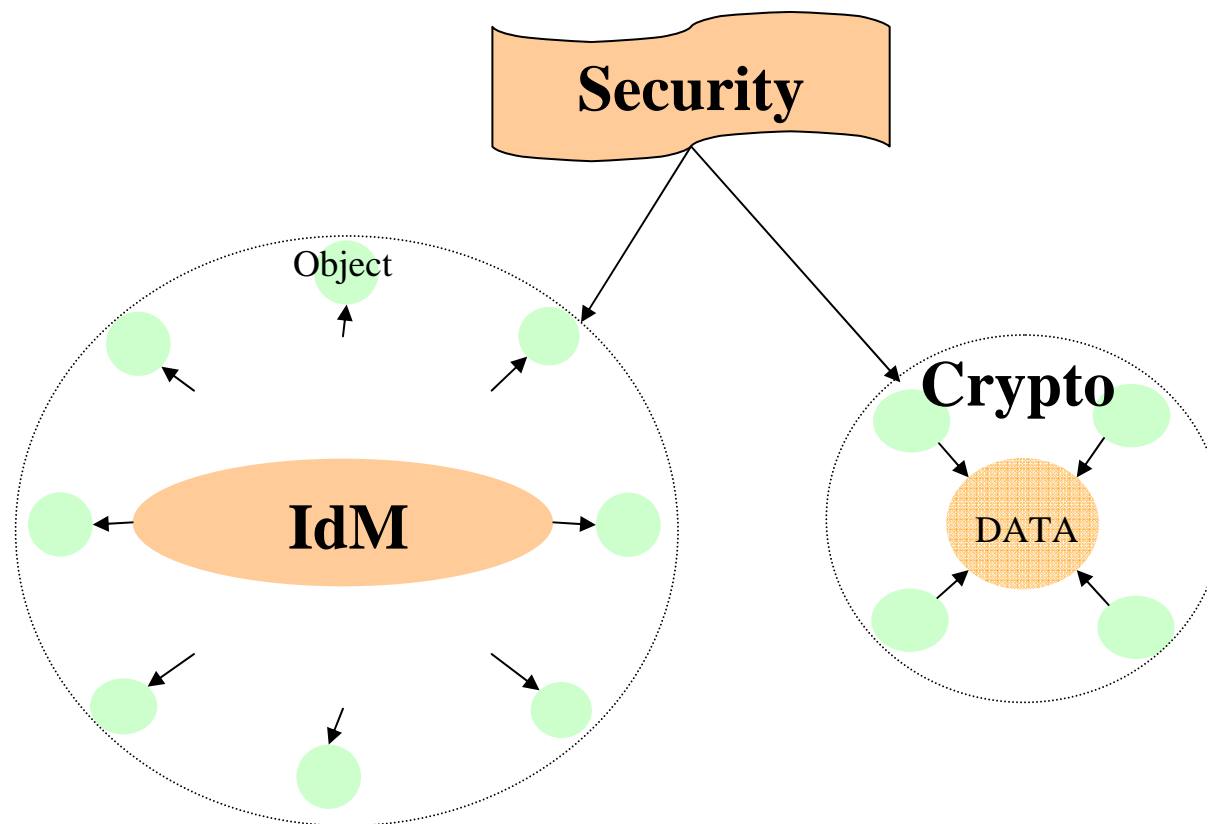


Figure 5 Understanding IdM: IdM for security

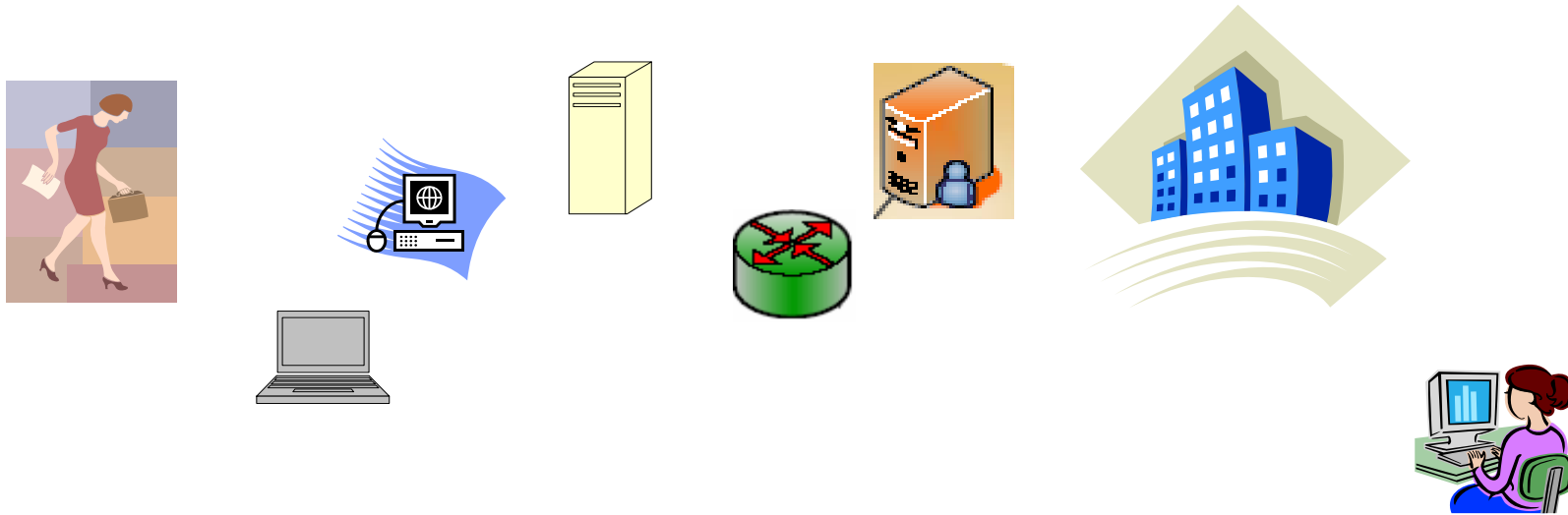


ITU-T

Requirements for IdM

- Source/root for all identifiers
- Authority of Id management in the network
- Provide open interfaces (Standardized protocols or APIs) to provide /support miscellaneous security services based on IdM, e.g. authentication, privacy control, privilege management, access control, tracing-back for originating attackers, etc.
- Efficiency: adoption of peer to peer basic model to save network computing resources
- Universal identities apply to universal objects (person/user/device/entity/domain...), with static identifiers (e.g. permanent Id) or dynamic ones (e.g. temporally Id with a short period of life time)
- Inherently constitute trust system among network identities
- Universal meta structure for IdM

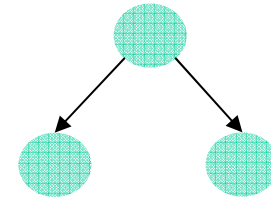
IdM scope



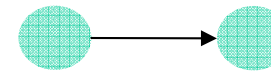
- IdM identifiers apply to various objects such as end users, terminals, servers, devices, network elements, network personnel, network or sub-network domains, and other entities that have the requirement of identity management
- The form of identifiers may be numbers, certificates /credentials, biometric features (person) or platform features (e.g. hash value) etc.
- IdM systems may be located any layer of a network, providing identity related functions or services

IdM Basic Models

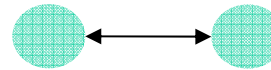
- o An IdM basic model is an elemental structure which forms the basis of IdM meta-structure
- o Simple protocol/mechanism for communications between Objects (each object equipped with an identifier) may apply
- o Universal objects
- o Trust inherent



a) Administration Model



b) Trust Model



c) Peer-to-Peer Model

Figure 2 IdM Basic Models



ITU-T

IdM design model

- Object Identifiers are basic object of IdM systems and they form the basis of IdM structure
- IdM Basic Models are integral components that build up the Meta IdM structure. Meta means that the structure is independent of network layer, environment, application scenarios, etc.
- An IdM System is heavily dependent on its network environment and application scenario, with customized interfaces to other security/non-security functionalities to providing ID related services.
- IdM network is comprised of multiple IdM systems between them communication protocols and mechanisms apply, e.g. SAML, SSO

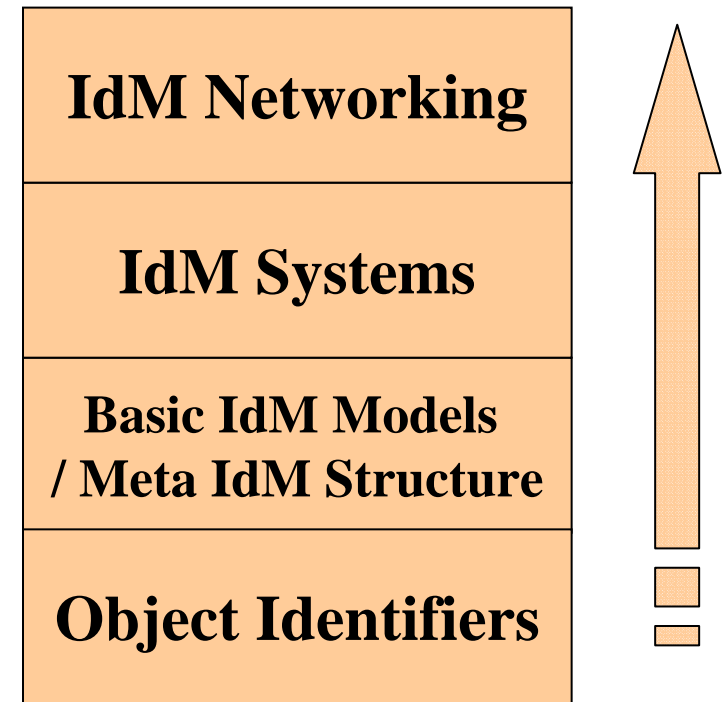


Figure 3 IdM design model



ITU-T

IdM Meta Structure

- IdM Meta Structure comprises of IdM core components centered by Object IDs
- For the Object IDs, they should have differentiated extensions to enable both local id functions and networked idM based functions
 - Basic ID Extensions enable the isolated IdM meta-structure
 - Advance Id Extensions enable IdM networking for security/efficiency, e.g. Federation ID

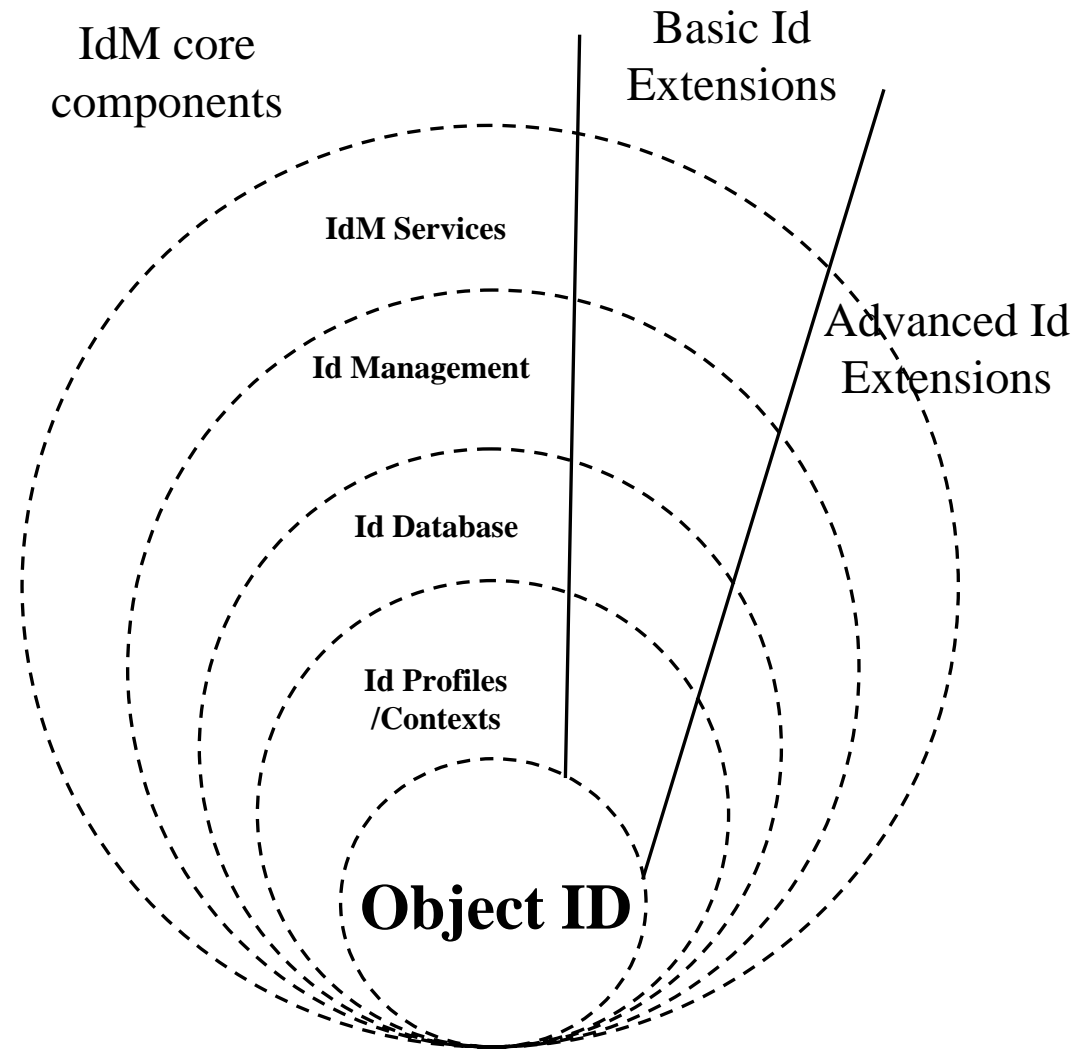


Figure 4 IdM Meta structure



Thanks for Your Attention!

谢谢!

jiwei.wei@huawei.com