Digital (Virtual) Identities in Daidalos and beyond

Amardeo Sarma
NEC Laboratories Europe
Who wants to pay for more Bandwidth?

- More Access Bandwidth?
  - No one pays extra for volume or time
    - plain usage is a commodity
  - But they will pay for access services

Digital Identities: a potential breakthrough and convergence technology

Revenue Increase depends on Network Service (flat rate!) providing value, not volume

Pay for
- Pervasiveness & Ubiquity
- Seamless Mobility
- Comfort of use
- Trust & Reliability

Volume or Time
Basic fixed Charge
Overall Revenue
Challenges for Network Access

• Make network access everywhere possible
  – This is a more valuable service than more bits!

• Make your network available with the quality you need while on the move
  – Seamless user linked roaming and mobility independent of your device

• Simple billing and customer relationship
  – Your trusted provider (operator, credit card company) should take care of everything

• Remove device limitation
  – Borrow a phone or laptop or use an embedded device in a hired car
  – Use multiple devices, share devices
Requires Change in Thinking

Whatever the network:
The user (you!) is at the centre!
Not your device (phone, laptop, ...)

Liberate User from Devices!
Daidalos Virtual Identities Approach

- VIDs correspond to *personae* and could relate to different roles.
- VIDs are used for both network and service access, as well as content.
  - May be extended to other domains, e.g., gaining entrance to building.
  - ID token that contains VID Identifier + encrypted artefact for A4C is used.
- Use VID to also enhance *privacy* of user.

VID Identifiers *may* be linked to digital certificate.

Registered ID

- Government ID (e.g., passport, drivers license)
- RegID of ID provider (Operator, Bank)

Physical Person (DNA, behaviour, Personal attributes)

User constructs VIDs for Access

VID Identifiers

User credentials

Official Document

Contract

Verify
Today: Identity Fragmentation

- Current identity info of a user is distributed & duplicated among different platforms resulting in
  - Multiple sign-on procedures for a wide range of services
  - Inability to make good use of user related data (trail, presence, geo-location) across different platforms
  - Difficulty for users to provide, retrieve and update all privacy info managed at each platform separately
Tomorrow: Identity Convergence

- **To solve identity fragmentation,**
  - Make a bridge between platforms
    - introduction of multi-personas per user
    - optimum deployment & life cycle mgt of them
  - Filter flow of identity info across the bridge
    - minimization of identity info disclosure from user’s viewpoint
    - making identity info obscure from operator’s viewpoint

---

![Diagram](Source: NEC Corporation)
Daidalos Virtual Identities Approach

- Growing numbers of communication services burden users with increasingly complex authentication effort
- Users want a limited number of operators enabling universal access to everything – ideally “single sign-on”
- Identity solutions need to support multiple (virtual) identities or personae for several profiles, roles and contexts … respecting privacy

- The trusted operator becomes a proxy for billing which is a business in itself.
- Improved security through VIDs acting as pseudonyms
  - the service provider delivers without knowing the user.
  - the trusted operator (e.g. operator or bank) knows the user, not the service.

Source: Daidalos
Daidalos Virtual Identity Concept

Technical Challenges
- Privacy
- Unified and Uniform Namespaces
- Access Control
- Billing and Charging
- Mobility

Objectives
- Link real and digital worlds
- User’s data should be under his control
- Service providers use of federation to enhance user experience

Source: Daidalos
Daidalos Virtual Identities and Privacy

• Services operate on privacy-sensitive data
• Dynamic business scenarios
  – Services offered by unknown (potentially untrusted) 3rd Party Providers
• Simple access to services for user’s required (Mobility support, SSO)

Source: Daidalos
Daidalos Virtual Identities and Privacy

- Service use based on Virtual Identities (VIDs)
- VID selected according to user’s privacy policies
- Mid-term: Make IP/MAC Address unlinkable

Source: Daidalos
Related Technology: Context Obfuscation

- **Context Obfuscation Technology**
  - supports privacy of context information based on user preferences
  - handles context exchange within and across domains uniformly

- **Context Obfuscation Challenges**
  - Context requires a structure that translates naturally to a blurring mechanism
  - Semantics for context blurring need to be defined
  - Adequate context distortion filters are required
  - User interface must be simple and support decisions in a dynamic environment
  - User must trust obfuscation behaviour

Source: Daidalos
Cross-layer design becomes Imperative

- Uniform namespaces (one ID for all purposes)
  - For network identification
  - To obtain information about a user/service/group
  - Under which to authenticate to the network and to the services

- To maintain pseudonimity at a higher level, a top-down protocol design is required

- ID must be independent of the application, service, interface and even terminal

Source: Daidalos
Mobility Support for Digital Identities

Source: Daidalos
Daidalos Virtual Identity Data Model

- **Entity**: individual, company, provider, etc able to make legal binding
- **Entity Profile Part (EPP)**: Coherent piece entity’s data e.g. at provider
- **Entity Profile (EP)**: The union of all EPPs plus entity’s knowledge
- **Entity Profile View (EPV) or Virtual Identity**: Entity’s aggregation of EPPs
- **Filtered EPV** used for access (to not reveal more than needed)

Source: Daidalos
Scenario:
- Alice uses a service offered by Bob
- Alice interacts as VIDID “X” with Bob

Bob requests attribute from Alice via the ID Broker
The next Step: SWIFT (01/08 – 06/10)

Identity Management Systems

Stratum

Today

Societal/ legal

Several IdM concepts

Several digital IdM-based concepts

Some digital IdM-based concepts

Future – i2010/eldM

Service

Several digital IdM-based concepts

Several eIdM-based concepts

Several eIdM-based concepts

Transport

Serala eIdM-based concepts

Scope

eldM: electronic Identification Management

ITU-T/ISO/FIDIS Workshop, Lucerne, Switzerland © NEC Corporation 2007 30 September 2007 Empowered by innovation
EU IST FP7 Project SWIFT

• Target: *Leverage identity technology to integrate service and transport infrastructures by extending identity functions and federation to the network and addressing usability and privacy concerns*

• Partners: Fraunhofer SIT (Project Co-ordinator), NEC (Technical Leader), Alcatel-Lucent, Deutshe Telekom, Portugal Telecom, Dracotic (SME), University of Murcia, IT Aveiro, University Stuttgart

• Time Frame: January 2008 – June 2010

• Overall Budget: 5.3 Million €

• EU Contribution: 3.5 Million €

• Description of Work approved by the Commission on 27th September 2007
  – Currently in the final overall Commission-internal processing and approval stage

• Acronym SWIFT: Secure Widespread Identities for Federated Telecommunications
Key SWIFT Technology Objectives (1/2)

• Vertical integration of identity, privacy, trust and security across layers: Protocols, addressing and inter-layer interfaces with controlled privacy

• New identity-centric user schemes supporting different levels of information access control, with well-defined privacy rules about who can change or even knows the data handled.

• Methods and techniques on how users are identified and located, but may remain pseudonymous at all layers based on user preferences.

• Identity-based mobility solution: Adaptation of mobility protocols to the user’s “moving identities” across devices, services and networks.

• Semantic interoperability of eIdM systems – legacy and different national instances.
Key SWIFT Technology Objectives (2/2)

- Meta data model to deal with IdM data sets to support interoperability.
- An Identity Management Platform providing a common framework and APIs for controlled access of identity attributes across services and networks with user privacy mechanisms including specific APIs, such as for an Identity Broker.
- Mapping new identity techniques to existing technology (SIM cards, etc), and eIdM and AAA solutions to accommodate Identity Management.
- Name and identifier resolution across heterogeneous namespaces.
- Contribution to standardization to include the SWIFT identity approach at the different layers to go beyond the existing solutions.
Relation of SWIFT with the Rest of the World

EU FP6/7 Projects
e.g. PRIME, Daidalos, FIDIS
and possible follow-ups

Key Standards Organizations*
e.g. Liberty Alliance,
ITU-T FGIdM, ETSI TISPAN

* Subject to modification during the project lifetime if environment changes

Other initiatives, such as Internet Identity Workshop, OpenID, ...

monitor
contribute
monitor

collaborate
Conclusions

• Identity Management is a technology for user based access: *Potential Key Convergence Technology* addressed by several standards bodies e.g. ITU-T Focus Group and initiatives

• In combination with Federation: *Daidalos* pioneered *bridging the gap between traditional IdM and Telecommunications*.

• The next steps e.g. in SWIFT: *Leverage Virtual Identities and Identity Management for the Network and Telco Services as a Convergence Technology*
Thank you!

Amardeo Sarma
NEC Laboratories Europe
sarma@neclab.eu