



EUROPEAN COMMISSION

Information Society and Media Directorate-General

Converged Networks and Services / Emerging Technologies & Infrastructures

Subject: Content received for session on ID Management, including routing and addressing in the FI

ID Management, including routing and addressing in the Future Internet

Consolidated version from Markus Brunner (Mana) and Jim Clarke (T&I)

Title: *Electronic ID (eID) management and provisioning in the Future Internet infrastructures including routing, services, and content.*

Problem Statement(s): As can be seen in the title, the scope of eID management and provisioning in the Future Internet in this document encompasses the identities across the various levels (stacks) – networks, services, applications, device and terminals (set of devices) and content, as well as the minimum requirements for identifying user(s) when accessing a resource. The following are the summary problems statements that have been brainstormed amongst the caretakers (*principally from the T&I and MANA caretakers thus far but we welcome more*) related to this topic and considered important in going forwards amongst all of the cross domain areas. Further reference materials are contained below and the caretakers are working on a longer position document for discussions [[will provide link for larger document when completed](#)].

Identification, Naming, Addressing requirements for the Future Internet: From the management perspective, there are already well-known problems concerning the scalability of current internet (protocol) object_identifier and addressing schemes; these become critical in the near future, and totally inadequate in the longer term.

The FI vision is for an explosion of networked entities, not least as the objects of the Internet of Things need to be named and accessed, but also as the underlying current trend continues for (sort-of exponential, as yet) growth in users, services, and usage. In addition there will be dynamically compound identities/identifiers/addresses dependent on context, location, etc., as services and other entities (re)configure, (de)compose, federate/secede, and as clouds form and evaporate. The challenge is to enable continuity and interoperability across the FI.

A coherent and comprehensive *framework* for handling all aspects of usage and management of eID from the bottom to the top of the stacks. This should include:

- administrative aspects: the creation, provision/registration, revocation of identities, and the management of attributes;
- operational aspects – how eIDs and their attributes are used, controlled, protected, and monitored (including accountabilities) – paying particular attention to the need for interoperability on the widest scale;
- the supporting abstract services to provide interoperability;
- the access controls by (productive) networked services based on eID;

- considerations of supportive legal measures covering possible rights, responsibilities and liabilities, as below.

Contextual usage of multiple identities and user aspects: Investigate naming and multiple attributes covering aspects of identity required in different contexts (eg. if it is a virtual entity such as a web service or a network resource, or in the case of natural or legal person whether you are a parent, a citizen, an adult, a patient, consumer, etc.). It is essential that research is carried out on how to balance the sophistication required for all these attributes and the usability required. If the systems are too cumbersome to use, it will disable the usage and confidence levels.

Links to "service description frameworks" and languages, in particular from a naming and a semantic perspective: For the service-oriented-architecture approach, it is necessary to think in terms of the knowledge and semantics of the attributes, and the necessary interoperability for a wider use across heterogeneous platforms. This must be extended to attribute definition of the services themselves. For example, characterizing the "state" of an individual service and the functions it offers [including its security state]. Other aspects include discoverability, availability, and composability for more sophisticated services.

Consideration of Legal, Regulatory and governance policies: Another challenge related to Identity and naming management and provisioning in the Future Internet that must be addressed is the links with legal, regulatory and governance policies.

Security and Privacy aspects: although this may be considered as a full topic itself, if not addressed elsewhere, it could be addressed here as the role/contribution of good eID to privacy aspects:

Other issues for consideration:

- Different types of identifiers: IP addresses (structured addresses), context-identifiers, information object-identifiers, resource (i.e. network, computation, storage) – identifiers, content-identifiers, device identifier, computational objects identifiers, service identifiers, virtual objects identifiers, virtual resource–identifiers, artifacts–identifiers, interface-identifiers; multihoming identifiers;
- naming and addressing issues in federations and multi-domain environments;
- addressing schemes where identity/identifiers and location are not embedded in the same address;
- mechanisms for publish/subscribe, aiming for a balance of incentives and roles between the sender and the receiver, e.g., information based publish / subscribe routing protocols;
- New and integrating naming frameworks, including both channel/session identifier and location, endpoints (source & destination points)-to-location resolution, identifier/location splits, and support for addressing and observability of information, context objects and services at all relevant FI levels;
- security properties of names and identifiers;
- Governance schemes for FI identifiers.

Caretakers that volunteered for this topic: <Jim Clarke and Marcus Brunner – main authors of draft, with alignment with other caretakers pending>, Alex Gluhak (RWI),

Michel Riguide (TI), Norbert Niebert (FCN), Pierre-Yves Danet (FCN), Tasos Gavras (FIRE), Theodore Zahariadis (FCN)>

Participants: same as listed in caretakers plus research community people invited to workshop in October 7 2009.

Points of agreement:

Include areas to attract wide coverage from cross domains.

Points of Discussion:

Holding workshop on 7th October 2009 to prepare for FIA Stockholm.

Follow up actions: Further align the submissions for this session.

Reference: In Madrid (Dec. 08) and Prague (May 2009), the Future Internet Assembly workshops held initial dedicated sessions on these topics, organised by the Trust and Identity caretakers.

A clear need was established for a coherent approach to careful handing, usage, and management of identities and identity-related information (eIDs) in the Future Internet. This must cover both future requirements for global interoperability and the current legacy. Principles set out in the *Laws of Identity*¹ provide guidance.

A common identity framework addressing these principles has been outlined². In the digital society, *Identities* will be multi-faceted and identity-provisioning and usage must take account of fundamental differences between physical identity and our digital identities. The Future Internet must move on from the flat or unique protocols for identity to more flexible ways of expressing and using identity appropriate to specific contexts and supporting interoperability.

In addition to the above topics already started in Madrid and Prague, the session for Stockholm will cover network infrastructure issues such as addressing, routing, and caching, separation of network endpoints from identity of people/entities and also issues of privacy and accountability mechanisms as substantive cross-domain topics to work through.

Does this topic require a follow-up discussion in Valencia? Yes

If yes, specify draft title: ... ***Possibly same, To be determined***

¹ <http://www.identityblog.com/stories/2004/12/09/thelaws.html>

² Posch, R., Rannenber, K., Cameron, K., "Proposal for a common identity framework: A User-Centric Identity Metasystem";

Input received from RWI (Syed Navqi):

Topic title: 2. ID Management, including routing and addressing in the Future Internet

1.1.1. Problem statement

Insert here the problem statement: no problem = no need for a session! The length should be short, max 3 paragraphs of 5 lines. It should include and put in perspective 'the commonly' thought solutions to the problem or a reasoning behind the fact that there are no known solutions. History of the problem and background should not be included here, but in the reference section.

There is an exponential rise in the use of eID nowadays. A trend of convergence for these IDs can also be observed. The use of national electronic ID card (with built-in chip containing personal data) is emerging as the unique eID for a number of applications. It is logical to see application of these eIDs in the Future Internet based services. However, the greatest concern in my point of view is how to manage the situation when this ostensibly unique eID is stolen? How the revocation of eIDs to a larger scale should be managed to gracefully contain the losses? How to limit false-positives and false-negatives?

1.1.2. Points of agreement

List here the points of agreement and a brief explanation of why/how a consensus has been reached. Include as well significant options that have been left behind.

Having a consensus on the broadening of eID management scope by including routing and addressing in the Future Internet can un-doubtedly be a major breakthrough that can provide a common ground for the evolution of a unique eID that can serve different layers for addressing and identification purposes simultaneously.

1.1.3. Points of discussion

List here the sub-points which are still under discussion as well as a brief explanation of the open options for each.

We need to discuss the scope of 'forensics' in the eID management so that any accident related to eID theft can be handled. This can also help in providing design-level security to the eID; and also provide a feedback loop in the overall trust management of the Future Internet services.

1.1.4. Follow up actions

List of agreed actions to do after Stockholm and before Valencia. These actions are to be undertaken by the 7 groups.

There will be very limited time between Stockholm and Valencia meetings, so we have to make some rational expectations while defining the follow-up actions. It will be great if we can propose a high-level eID format by the Valencia meeting. This format will have specific bits (or the specific order of its bits) for routing, addressing, and identification. This segmentation can improve the performance of a revocation process. However, this

scheme may give the over eID a look of 'federated ID' instead of a unique & harmonised one. The pros and cons of these arrangements require further evaluations and follow-up discussions. We can prepare a timeline of these discussions and their anticipated results in Stockholm.