

Wrap-up

A number of conclusions were drawn from the results of the workshop, including:

1. Although it wasn't presented in too much detail at the workshop, the technology developed in PRIME and PRIMELIFE can control and minimise the identity-related information relating to the user that is made available to ***application-layer*** entities, disclosing only the necessary and sufficient certified credentials for the current need;
2. in the networks space, we need information relating to communicating entities that allows/supports routing of traffic between them - or rather, their respective end-points;
3. we need to avoid the disclosure (in the network, in this particular case) of information that could be used to provide ***unauthorised*** identification, linking, or tracing of the communicating entities (including indirectly, through profiling/mining/etc.); The presentation on the networking approach seemed to indicate that the combination of technology and policies can bring together the privacy respecting aspects all the way down to the network level. In addition, there is already work on separating locator and identifiers so we are in the right place to work this into the new design of the Future Internet with an "identifier layer" over the Internet.
4. Before coming into the workshop, the big question was the following: ***Is the (type of) technology in 1. able (or can it be adapted) to satisfy the requirements of items 2. and 3.?***

Following the workshop discussions, the answer to the question seems to be: there is broad agreement that the approaches of the applications/services and networks communities are similar with some nuances like the SWIFT use of an ID Aggregator, which can aggregate at user level or network level. Even here, the approaches are similar whereas while the approach of PRIMELIFE is from the user perspective, it can also cater for the network level. The feeling was that there is very good potential to get an initiative in the core part of the PPP, ensure privacy-preserving ID provisioning including through to the network level including how privacy preserving routing can be provided that is consistent with a) business models and b) state-imposed obligations on carriers.

The main outcome of the workshop was consensus was reached on the way forward for a privacy enhancing Identity management framework across the layers. With this in mind, it was agreed to present the joint approach in FIA Valencia. It was agreed to try to get a longer slot than 15 minutes for presenting these important works explaining how this should be brought forward for the PPP.

Once presented at FIA Valencia, we could work together on a joint position paper to further elaborate technologies and the solutions that are already available and those still required. One of the ideas expressed was the filling of a matrix to highlight what is needed throughout the layers for each approach that could be discussed and agreed together (as shown in the following figure).

**Privacy preserving ID across the layers matrix –
required components and solutions**

Approaches Layers	User centric approach (a)	Application/ Service-provider -Centric approach (b)	Network-centric approach (c)	Integrated approach (d)
User (j)	**	**	**	$(d_j) = \sum (a), \dots, (c)$
Application (k)	**	**	**	$(d_k) = \sum (a), \dots, (c)$
Services (l)	**	**	**	$(d_l) = \sum (a), \dots, (c)$
Transport (m)	**	**	**	$(d_m) = \sum (a), \dots, (c)$
Network (n)	**	**	**	$(d_n) = \sum (a), \dots, (c)$

**cells to be filled with some detail by Primelife/TAS3/SWIFT/... where you can provide a solution or have a dependency

Figure 1. ID management across the layers matrix

The idea was suggested that it could be a starting point to populate a matrix of sorts with some detail of solutions or dependencies that could then be discussed and agreed by the communities to end up with an integrated solution across the layers (if feasible)

The presentation for Valencia could focus on:

- Defining the scope of the work, which is looking for an approach or way forward on ID management across the layers;
- Highlight the reason it is so important;
- why it is being done within FI;
- What are the consequences if not addressed;
- The current state of the discussions;
- The key stakeholders (incl. projects);
- Conceptual description of the various approaches being taken and the importance of convergence here;
- Future avenues for addressing this important topic;
- What concrete contributions related to trust & security can we propose to FI projects?

It was agreed that Amardeo Sarma would start with a first draft of the presentation.