

## Interim FIA ID workshop

### "privacy enhancing Identity management across the layers in the short and long term "

3 March 2010, Brussels

Location: BU29 0/08

#### Type of document:

*This document is a working document of the preparation and outcome of the Interim FIA ID workshop. It is jointly written by the participants of the event.*

#### History of the document:

<i>Version</i>	<i>Date</i>	<i>authors</i>	<i>Description</i>
Draft 1.1	08.01.10	Bart Van Caenegem	first version with annotated outline
Draft 1.2	08.03.10	Jim Clarke	Draft version
Draft 1.4	09.03.10	Antonio Skarmeta	Provided updates
Draft 1.5	09.03.10	Nick Wainwright	Provided updates
Draft 1.6	10.03.10	Keith Howker/Jim Clarke	Provide updates/Integration
Draft 1.7	22.03.10	Jim Clarke	Wrap Up section
Draft 2.2	25.03.10	David Chadwick	Contribution of David Chadwick
Draft 2.3	31.03.10	Jan Camenisch	Contribution of Jan Camenisch
Draft 2.4	02.04.10	Amardeo Sarma	Contribution of Amardeo Sarma
Final	02.04.10	Jim Clarke	Final contributions

Practical questions related to the organisation of the event can be addressed to Bart Gustav Kalbe (EC). Questions related to the report can be addressed to Jim Clarke (Waterford Institute of Technology)

In order to have an effective workshop, the number of participants was kept limited on purpose.

## Table of Contents

Scope and Objectives	3
Motivations and Background	3
Structure of the Workshop	4
Opening	4
Presentation 1: Identity Management Architecture, Technologies, and Trust Models: an introduction to IDEMIX (Jan Camenisch)	4
Presentation 2: The Identity Management Architecture and the network layer (Amardeo Sarma)	5
Presentation 3: The requirements (dos and donts) of Identity Management in the future internet (Fabio Massacci)	8
Discussion session 1: Are the proposed solutions meeting the requirements (dos and donts) of Identity Management in the Future Internet?	10
Discussion session 2: How do we take this into the FIA and FI PPP? (FIA Valencia and research roadmap)	11
Wrap-up	12
Detailed agenda	14
Annex 1: list of invitees/participants	15

## Scope and Objectives

This interim workshop was designed to focus on the discussion of privacy enhancing identity management across the different communication layers (from network to application) for the short term (i.e. in the current 'internet' and 'telecom' context) as well as for the longer term (i.e. in the context of the anticipated or unanticipated evolution of the 'network'). Given the current internet evolution and impact of the internet on society, we assume that the 'future network' is the same as the 'future internet', i.e. the successor of the current internet. Still, the future internet may exist in different coexisting flavours to serve different purposes; we assume that the future network will be more based on the principles of the internet in contrast to the principles of the traditional telecommunication network.

Like we currently refer to the Plain Old Telephone System (POTS), we may in future refer to the Plain Old Telecommunications System as well, for the hierarchically built, and single owned network of a telecom operator. However, telecom operators are constantly changing their network architecture in light of 'cost of ownership', flexibility, etc. converging to what we later will call 'the future network'.

The objectives of the workshop were:

- present current views on requirements, concepts and technology for 'privacy enhancing identity management';
- achieve common understanding on the state of the art and future research in this area (i.e. to identify research on identity management technologies and network protocol requirements for the future internet that can be proposed for future funding in the context of the PPP in Future Internet);
- achieve consensus on how to present the topic in the Future Internet Assembly (in Valencia, 12-14 April 2010) towards the wider research audience; a session slot is already foreseen in the 'architecture session'.

## Motivations and Background

In the workshop of 7 October 2009 and in the successive FIA meetings, we discussed this topic of privacy enhancing identity management in the context of the 'Future Internet'. However, none of these discussions were conclusive mainly for the reason that time was insufficient, or interactive discussion or diverging views were missing. With this workshop consisting of specific researchers targeted by invitations, we hope to address previous deficiencies.

Often also common understanding is not achieved because of the intrinsic problem of 'communication'. The sender assumes contextual information that is not explicitly expressed, but that is implicitly filled in by the receiver. For that reason, it is as important to say 'what you do not mean' as 'what you do mean to say'.

This topic is a core topic of several of previous and current EU funded projects. Foundations have been made in previous projects like PRIME, FIDIS and DAIDALOS. In the current projects Primelife, TAS3, SWIFT and Picos, which are gathered in the 'Primcluster', architectures and concepts, such as those of virtual identities, and technologies, such as IDEMIX, Identity Aggregator and others are discussed to achieve this same goal of privacy enhancing identity management.

## Structure of the Workshop

The workshop started with three presentations and followed with 2 sessions of interactive discussion.

The approach is based on the following two points of view:

1- Are the proposed solutions meeting the requirements (dos and donts) of Identity Management in the Future Internet?

2- How do we take this into the FIA and FI PPP? (FIA Valencia and research roadmap)

### Opening

The background and purpose of the workshop was re-iterated, which was borne out of a number of recommendations made during the “ID approaches for the Future Internet” and “trust and identity” plenary sessions during FIA Stockholm.

- All agreed that this topic is critical to the success of the design of the architecture of the Future Internet;
- Instead of having yet another session at FIA Valencia, a more results oriented view was taken to move this forward together for short and long term with all stakeholders involved. Thus, the results could be presented at FIA Valencia;
- The experts amongst us agree that there are building blocks already being worked on (with some technologies already available) within the communities/projects and to achieve maximum impact, we need to come together now to put together a coherent picture together both for the PPP on Future Internet and long term research;
- We could position ourselves by making the ID layer a core principle/module of the PPP on the Future Internet;
- Let's do it together!

### **Presentation 1: Identity Management Architecture, Technologies, and Trust Models: an introduction to IDEMIX (Jan Camenisch)**

The presentation covered the foundational architectural concepts of an identity federation system using anonymous credential technology as explored in the PRIME and PRIMELIFE projects. This operates above the network layer and assumes some kind of network-level anonymity. The vision of this research is: ***“In the information society, users can act and interact in a safe and secure way while retaining control of their private sphere.”***

Therefore, within the high level requirements of enhancing privacy for the information society, the solution has to be technically feasible, understandable and manageable by end users, socially desirable and acceptable and legally compliant. The principles include the design should start with maximum privacy and system usage is governed by explicit privacy rules.

Vint Cerf has said, “We need identification in the Internet. We need both: sometimes we want to be anonymous, sometimes we need to be identified.”

How do we achieve both of these at the same time? This is the focus of PRIME and PRIMELIFE projects.

The presentation included a discussion on the particularly strong trust model that can be achieved with anonymous credential technology. Furthermore, the talk highlighted the powerful identity federation capabilities of such systems, such as the capability of making identity statements with attributes of different providers. The presentation sketched how accountability can be achieved in the setting of data minimizing scenarios. A number of scenarios were presented showing the minimal information needed that is still sufficiently authenticated and guaranteed by some government credentials. For example, a person wants to rent a car. The person needs a driver’s license and insurance to rent the car. These aspects can be described similarly into the electronic domain. However, if we use more than the minimal data, the data can be mined and used for illegitimate purposes. Therefore, one solution is Anonymous credentials<sup>1</sup>.

In this scenario, it can use pseudonyms and get driver’s license confirmation as Alice, insurance confirmation as Eve and rent car as Bob. Thus, only the data you are willing to reveal will be revealed. It is up to the user only as to what is revealed. However, more information may need to be available if there is a car accident so the car agency can go to a third party using encrypted data to get the car repaired or take the escalated scenario further. The technology allows you to specify the minimum data in the normal operation. If the car gets broken, it is pre-established what additional information is needed for the car fixing company to figure out how you are identified to the insurance company.

More precisely, a credential is a means to establish a claimed identity, roles, or attributes about oneself with an entity, typically as part of an access control request. So for instance an identity card can serve as a credential to establish that one is between 12 and 15 years old as might be required to access a teenage chat. Using a traditional identity card, this would also reveal to the chat site all the other information contained on the card.

Anonymous credentials overcome this: with such credential a user can selectively reveal information about the attributes contained in the credential without revealing any other information about them whatsoever. Thus, with an eID card equipped with anonymous credential technology, a teenager to prove to the chat site that she is between 12 and 15 years old without revealing any other information stored on the an eID card such as her exact birthday, name, or address.

Thus, anonymous credentials are a key ingredient to protect one’s privacy in an electronic world.

## ***Presentation 2: The Identity Management Architecture and the network layer (Amardeo Sarma)***

The presentation focussed on a sustainable Identity Architecture including the network layers that caters to what the user wants (performing tasks towards an intention) with the necessary privacy and data protection constraints (avoiding

---

<sup>1</sup> It is not the only solution. The TAS3 project has a linking service which links short lived credentials from different issuers using a random identifier.

personally identifiable data including at the network level eg. via IP and MAC addresses and enabling OECD guidelines (collection limitation principle and data quality principal).

The approach would be towards understanding and taming Identity at its roots by the abstraction of real entities with all their properties. This would be moving away from the real world of things where we abstract things where we can use logic. This would include abstracting the user from the terminal, the network, and just concentrate on the user intentions and communication properties that are associated to the Virtual ID he is using in that aggregate of attributes/context.

Identity data exists as identifiers in the network today: examples are IP and MAC addresses with revealing personally identifiable data available in interim nodes today without a conceptual identity framework supporting privacy. Therefore, we must address how to use ID data wherever needed in the while preserving maximum privacy?

From the SWIFT perspective, the previous presentation focussed on the technology to support partial IDs whereas this presentation focuses more on how to relate the solution to the way partial IDs are provided across the layers. Looked at in another way, within the Future Internet, there would need to be a combination like User IDs and Service/Applications IDs: Network IDs. There is a need to connect this topic with the network world. It requires an investigation into how we use the network and how the network will support privacy. This would require a cross-layer approach to identity and IdM systems in accessing ether application services or the network, providing different transport mechanisms for a common token and credential if you are using a web application (https or soap) or if you are accessing to the network service (EAP).

Moving into the future, it is clear that the OSI model is outdated. Different locator/identifier approaches exist for NGI. Locating objects with topology-independent identifiers has emerged as a key functionality in data centric approaches to networking. The user identity and context must be an integral part to be able to link session operations (not to identify people). The entity considers different virtual identities to create a view onto the communication sphere which is singular, unique and optimised.

We will also be moving towards virtual terminals. Today, people are mainly bound to a specific device. In the FI, there will be a move towards virtual terminals. Therefore, it will be needed to have time limited ID links for users – devices. An example could be to enable use of hired devices (eg. Airport).

The relationship between the device and network provider will provide attribution. This ID framework gives a choice of solutions for things you want to solve. How much do you want to make someone identifiable to whom and vice versa in the sense that we are talking about end-end communications and that implies a two way identity communication.

The approach would be to start at anonymous and then start to add credentials. Certain things should be done anonymous eg. Whistleblowing and they should not require someone to get a pre-paid SIM card for this.

With respect to identity transfer during a session, some identification could be at the network level but it could also be at the user and application level.

Who controls the IDAgg? It can be either on the user side or the network side. This is an element that needs to be analysed closely. Do you want to do the integration between the network identification with the application identification things? How much do you want to integrate these? Swift is saying you do not need to IDAgg – does it come in two flavors – one for network and one for services, or either one linked to the user. It is collecting whichever information you want to use and it manages it in a distributed way reducing the bottleneck of just having a unique one but also giving option to allow different stakeholder to be involved. Additionally the IDAgg can be distributed in a domain base approach allowing to control by means of policy the information to be provided/disclose based on local policies or SLAs

The IDAgg is in some sense related to the objective of the partial disclosure model of IDMix where instead of the user being the final entity that manage the token and attributes disclosure it could be a trust entity doing it on behalf of the user.

Can you have the escrow category with this model? It may be better to take it apart. The presentation invokes these kinds of discussions. How to bring a framework to also address at the lower level. One of the very important elements in the discussions is the control domains. IDAgg can be in any domain. It will be an additional function and someone will have to manage it. If on user side, it will be the user that will do it. Example of a desired scenario

Two entities can establish a communications based on their virtual identities:

- each entity can authenticate the peer based on the received information
- each entity can access the partners information (attributes) based on the received information (Age, gender), ...
- the real identities of the entities are not revealed.

The evolution of NGI to clean slate approaches where there is a clear split between identifier and locator brings an opportunity to define a new framework where the identifiers get more semantic including the Identity as part of it and in that sense to provide a new session concepts where the identity could profile the communication abstraction. This process implies a cross layer approach and a framework for identity that creates an identity vision where:

- Identity plane allowing entities to address each other by means of an intuitive “ID to ID” approach;
- Control plane to ensure that end to end communications is made possible by negotiating any agreement needed between pairs of different administrative domains;
- An evolved routing scheme which is capable of routing on such identities: proposing a transition approach to allow a routing based on identities.

For a clean slate and migration approach, it is suggested to replace the transport layer by session aware transport eg. New switching layer mapping sessions to labels enabling overlay connectivity.

Some issues for future research

1. Flat versus hierarchal approaches in the use of identity
2. managing the scope of identity
3. expressing the context of the identity
4. identity as roles and grouping of persons
5. integration of IoT as another user of Identity
6. ....

In conclusion, in order to make Identities part of the Future Internet, the following should be catered for:

- Communications setup and routing should be aware of the relevant identity attributes (not identifiers!) for network functions without making users identifiable;
- Ensure better privacy and security than available today!
- Make identities represent not only devices/users.

### ***Presentation 3: The requirements (dos and donts) of Identity Management in the future internet (Fabio Massacci)***

This presentation contained requirements of dos and donts and of IdM in the Future Internet and referred to questions related to the previous presentations to indicate potential risks that the solutions might have.

Four requirements / challenges were presented in the form of questions related to Identity and privacy.

Q1. Zoning of Identity:

- **D. Lessig. “Code and other laws of the Internet”**
  - **Zones separate “individuals” to build local trust**
  - **Within the zone we are fully accountable (can build trust)**
- **In physical life we are pretty good at zoning**
  - Separate our relations (eg friends, work, relatives, neighbors) by “distance”
  - Searches are difficult by people outside each zone
  - Law enforcement can break zones but have hurdles
  - Individual *and* government can build zones
- **Do solutions allow individuals to zone identities?**
  - Applications/Services view: Pure P2P Attributes → No Accountability: Zones too small
  - Networks view: Purposeful Address → Total Accountability: Zones too big

Q2. Commercial Identity:

- **Identity tech so far conceived for “clients”**
- **What about “identity” of “partners” ?**
  - You want to know who is the other!

- **In the physical realm**
  - Identity of partners is regulated (you cannot just open a
  - supermarket, a dentist's practice or a bank)
  - Commercial identity is *distinct but always linked* to identity of
  - human individuals (legal responsible)
  - strictly linked to specific attributes *and* taxable
- **How to link the identity of end point to the accountable identity for humans behind it?**
  - Applications/Services view: escrow of credentials → requires third party
  - Networks view:: master addresses → accountable if physically located

#### Q3. Identity for Carriers:

- **Today huge legal shelter by principle "Mere Conduit"**
  - We drive bits, not responsible for their meaning
  - Phone Harrassment: 85 Italian Supreme Court cases, not a single conviction of telecom provider
- **Carriers are lured by Google's business model**
  - offer "free" services, profile users and gets money by advertising
  - (more identity information, more valuable for advert)
  - But now they "*know*" the meaning of bits
  - First Instance Italian court sentenced CEO of Google Italy to 6 months to prison for a video where a handicapped is beaten
- **• Can carriers run identity-based services without knowing identity (and other attributes) or need legal upheaval?**
  - Also go back to zoning (carriers offers zones and users disclose zoning info at their will but carriers not responsible for content)

#### Q4. Guarding Identities

- **Back to Paolo Junior**
  - He is on internet, has a LEGO account
    - There is lots of notices for parents, but I didn't check...
  - not yet an email account
    - His cousin (12) has Yahoo+ Microsoft messenger accounts (likely she lied on her age... as all her friends did)
- **In the physical realm well understood problem:**
  - my children are on my passport
  - Can be sent to buy bread with ready cash but can't borrow
  - can't commit the family for large amounts
- **In the Future Internet Research Agenda?**
  - Option 1 – Ignore the problem
  - Option 2 – Solve before the world solves it in some way
- **How do you provide "limited" identity to minors with a fall back "guardian" identity that is accountable?**
  - Goes back to accountability: a linkage between identities

In conclusion, we must look at these solutions for Identity with the frame of mind that people's lives/data/actions have been on the Future Internet since they can read or write (age 6)

The questions were summarised as follows:

- Do solutions allow individuals to zone identities?
- How to link the identity of a partner to the accountable identity of humans behind it?
- Can carriers run identity-based services without knowing identity (and other attributes)?
- How we can provide “limited” identity to minors?

***Discussion session 1: Are the proposed solutions meeting the requirements (dos and donts) of Identity Management in the Future Internet?***

In the discussion that followed the presentations, it seemed agreed that this issue of age protection can be solved with the technology presented by both the Applications and Networks viewpoints. It is necessary to get the token to say you have the authority to do something. The area of liability in these new environments must be further explored.

Regarding zoning, zones are groupings on a different level (eg. people). The rules that apply are set down in the policies. The speakers felt that the zoning questions can be done already with the technology described.

There was a discussion on the question –“to what degree is identifiability necessary?” Data retention laws in a German court said they wanted some documentation and service providers said they couldn’t provide these due to privacy laws. Government didn’t do their homework and they were not specific enough on what data they wanted and what would be done with it. It may later come to the conclusion that the constitution is not working for the Information society.

We take care that the identity data will not combine with our personal life that will cause the problem. Regarding accountability and privacy, there are some situations where accountability is required and some where it isn’t appropriate.

The processing behind the capturing of ID data is one of the important issues. Another ruling involved that the rules must be clear where you can understand what the risks are. We need good terms to describe these things.

We need to clearly separate the two issues: Privacy and Privacy respecting ID management. At the recent [Trust in the Information Society conference](#) in León, Spain, Peter Hustinx raised the importance of getting assurances from the companies/data collectors about how and what they collect and ensure that they are liable if they misuse the data. It was pointed out the videos of this event are now available [here](#) .

## **Discussion session 2: How do we take this into the FIA and FI PPP? (FIA Valencia and research roadmap)**

The role of identity management in the Future Internet Public Private Partnership (FI PPP) was discussed. The consensus of the meeting was that given that the key elements of the solution are available, then identity management should become a key part of European Future Internet Initiatives.

It was agreed that group should work to ensure that an approach to identity management as described above is included in the core network that will be developed under the FI PPP call to be announced in Valencia in April 2010. This is in line with the thoughts of the European Future Internet Initiative, which states

*"The proposed Public Private Partnership (PPP) will enable Europe to consider supporting the sector driven requirements, such as identity management, scale and user acceptability, by using known and emerging technologies in a holistic approach to providing entire solutions for societal challenges<sup>2</sup>"*

It also states that the core platform should include

*"Trust and Identity capabilities enabling end users and service providers to be identified globally in a trusted manner including lawful interception."*

The next steps agreed were to develop a presentation for FIA Valencia session on Architecture for the Future Internet. This should build on the materials presented at the meeting and would outline the requirements for including identity management capabilities in the core network infrastructure, describe the key principles for privacy respecting identity management, illustrate the solution, and articulate from the service provider perspective the arguments for including identity management of the network and why routing in the network requires a privacy respecting approach. It was recognised that it is important to stress that the approach is federated and scales.

---

<sup>2</sup> *White paper on the Future Internet PPP Definition*, January 2010. The European Future Internet Initiative

## 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.

## Detailed agenda

- 11:00-11:15** Opening and table round (all) (JC, BVC)
- 11:15-11:45** Presentation 1: Identity Management Architecture, Technologies, and Trust Models: an introduction to IDEMIX (Jan Camenisch)
- 11:45-12:15** Presentation 2: The Identity Management Architecture and the network layer (Amardeo Sarma)
- 12:15-12:45** Presentation 3: The requirements (dos and donts) of Identity Management in the future internet (Fabio Massacci)
- 12:45-13:30** Lunch
- 13:30-15:00** Discussion session 1 (KH): Are the proposed solutions meeting the requirements (dos and donts) of Identity Management in the Future Internet?
- 15:00-15:15** coffee break
- 15:15-16:45** Discussion session 2 (NW): How do we take this into the FIA and FI PPP? (FIA Valencia and research roadmap)
- 16:45-17:00** Wrap up and closure

## **Annex 1: list of invitees/participants**

<b>Fisrt name</b>	<b>Family name</b>	<b>Affiliation</b>
James	Clarke	Waterford Institute of Technology -TSSG
Nick	Wainwright	HP
Keith	Howker	WIT-TSSG
Jacques	Bus	EC, DG INFSO, F5
Gustav	Kalbe	EC, DG INFSO, F5
Bart	Van Caenegem	EC, DG INFSO, F5
Wout	Van Wijk	EC, DG INFSO, F5
Amardeo	Sarma	NEC Europe Ltd.
Fabio	Massacci	University of Trento
Jan	Camenisch	IBM Zurich
Joao	Girao	NEC Europe Ltd.
Antonio	Skarmeta	Murcia University
Giuseppe	Bianchi	University of Roma
Kai	Rannenber	Goethe University Frankfurt
David	Chadwick	Univ. of Kent
Christian	Weber	Goethe University Frankfurt
Martin	Kuppinger	Kuppinger Cole
Lefteris	Leontaridis	IKED