ICI

Identity-Centric Internet

Proposal full title	Identity-Centric Internet
Proposal acronym	ICI
Call	FP7-2011-ICT-FI
Type of funding scheme	IP
Duration	24 months
Work programme topics addressed	1.8 Use Case scenarios and early trials Section One. Pervasive and Trusted Network and Service Infrastructure Future Internet PPP 2011: Phase 1
Name of the coordinating person	Mikaël Ates
Coordinator E-mail	mates@entrouvert.com
Coordinator Fax	
Date of Preparation	2 décembre 2010
Version number (optional)	1.0

List of participants

n°	Organisation name	Short name	Country
1	Entr'ouvert	ETO	FR
2	ADP-Internet of Subjects	IOS	FR
3	University of Nottingham	NOT	UK
4	University of Reggio Calabria	URC	IT
5	ForgeRock	FRK	NO
6	TB-Solutions SA	TBS	SP
7	University of Saint-Etienne	UST	FR
8	Kynesim	KYN	UK
9	Kuppinger Cole	KUP	DE

Table of contents

Terms of reference

Component	Definition
IC-Agent	The Identity in the Cloud agent (IC-Agent) is a component hosted by a host trusted by the user. The IC-Agent is online. It hosts a personal authorisation module and a user protocol hub. It is also in charge of retrieving and handling policies concerning the user. It can also integrate a local attribute provider and a local identity provider. It can store the certificates of trusted services providers, service provider metadata, authentication credentials, multiple-time use certificates, policies and a journal of logs containing the authorisations given. The IC-Agent makes the "Identity in the cloud" concept a tangible reality.
Access control Policy	An access control policy indicates the attributes required by a service provider to grant access.
Agreement Policy	After the trust path discovery, each party must agree on all policies before the trust path can be effective.
Attribute certificates	An attribute certificate is a digital document containing identity attributes signed by an attribute provider. Relying parties can authenticate a document as being signed by a trusted attribute provider.
Attribute Policy	An attribute policy indicates how the identity attribute has been obtained or defined by an Attribute provider. An attribute can have a degree of quality. For instance, a date of birth provided by a state administration is stronger that if one provided by a social network service provider.
Attribute providers	Attribute providers are specific service providers hosting personal data about users and able to provide them to the users or other service providers.
Audit Bus	A component of the identity centric architecture, the audit bus ensures specific privacy related audit events for users are sent to log locations and Dashboards.
Audit Service	A component of the identity centric architecture, the Audit Service provides a logging source for the architecture and interfaces to allow audit information usage.
Authentication Context	Describe the process of authentication. For instance, a physical authentication of the user in an office or a user password on a web site. The degree of strength between the same kind of authentication context can be established.
Identity Authentication Policy	Such a policy describes the authentication contexts employed by an Identity provider or a requirement of a relying party.
Identity Providers	Identity providers are specific attribute providers. They provide a specific identity attribute, usually called a pseudonym, making feasible the user authentication on a service provider. An Identity provider can be used as a support for a web single sign-on mechanism for instance.
Personal Authorisation Module	The personal authorisation module is a core component of the identity centric architecture. It is a service provider provided to each user. This component hosts the user access control policies on personal data. It allows automatic delivery of authorisations to third parties to obtain identity attributes. An authorisation can be delivered for a limited time. The user can also revoke an authorisation at any time. This component enables user control.

Component	Definition
Personal data store	A personal data store (PDS) is a term designing an attribute provider, trusted or not. For instance, this term can be used for an attribute provider hosted by the user terminal. Such a store can be used to automatically fill web forms.
Privacy policy	A privacy policy indicates the usage of personal data a service provider performs and the usage a user may require.
Provider metadata	Digital document containing the applicative endpoints of a service provider. Metadata can also contain policies and cryptographic material.
Relying party	A relying party trusts another party to provide a specific service.
Root Trusted Nodes	A root trusted node is a trusted node at the top of the trust architecture hierarchy. This role is identified to make trust path discovery easier.
Service providers	Service providers offer a service to users. They consume personal data. The service provider can require that a part of this certified data be certified by a trusted third party to deliver the service to the user. For instance, a service provider can require that a user date of birth be certified before giving access to a part of a website.
Trusted Attribute Gateways	Trusted Attribute Gateways are trusted nodes and trusted attribute providers. In some circumstances, a peer-to-peer relationship will not be possible. A Trusted Attribute Gateway will be in charge to establish a peer-to-peer relationship with the trusted attribute provider and the relying party. This entity can be used for attribute translation between countries, for instance.
Trusted attribute providers	Trusted attribute providers are both attribute providers and trusted parties of some relying parties.
Trusted Identity Providers	These are identity providers trusted by relying parties to authenticate a user. For instance, a trusted identity provider has the charge to authenticate the civil identity of a user and then provide service providers with a pseudonym. In some circumstances, identity providers revoke this anonymity to provide the civil identity to the service provider.
Trusted Nodes	A trusted node is a trusted party and a relying party. The role is to be a node of a trust path thus to allow to make a trust link between two parties not directly trusted. Each trust node will be responsible of the discovery of the sub-level trusted nodes.
Trusted parties	A trusted party is a party trusted by a relying party. For instance, a service provider, being a relying party, trusts an attribute provider for providing specific identity attributes about a subject.
User Dashboard	The user interface making the user able to pilot an IC-Agent.
User Protocol Hub	The user protocol hub is another core component of the identity-centric architecture. It allows retrieval of identity attributes from an attribute provider and their presentation to third parties. Some protocols need this kind of protocol flow. It is also necessary to make users handle cryptographic certificates. Finally, such a protocol flow can be necessary with multiple-time use certificates. The hub supports multiple protocols and can make the bridge between different protocols.
Users	The users consume services offered by service providers. A user has digital personal data. Users can provide third parties with personal data. The user exhibit an identity in the cloud.

Part A. Section 1. Summary

Abstract

The Identity Centric Internet (ICI) is born out of a response to three main challenges:

- how to provide individuals with the means to easily control access to and exploitation of their personal data while the amount and fragmentation of personal data is increasing geometrically
- how to provide individuals with the means to be in control of their identity, while most of the data is out of their control
- how to free personal data in order to allow the emergence of new services — on the model of what is currently happening with public data — while increasing the level of privacy and trust.

In order to respond to these challenges, it is not possible to simply apply patches to the current Internet architecture: ICI is based on a paradigm shift, the vision of a new architecture that places identity as the generative component, the foundation of its architecture.

We expect that ICI will contribute to building a new generation of Internet that enables Europe to gain technical and market leadership.

ICI objectives

The objective of ICI is to establish the foundation for a large-scale, open trust architecture (over 250-300 million users, individuals and organisations) that will make it possible for any entities or subjects, organisations or people, that have never previously been involved in any digital relationship to be able to establish instantly a dynamic trust relationship (1-1, 1-n or n-n). The ICI architecture is based on the dynamic construction of a cluster of distributed trusted identities. These trusted identities operate within a wide range of circles of trust:

- **institutional**: state federations, telecom operator federations, banks, university federations, etc.
- **business**: business partnerships, vendor relationship management, supply chain, demand chain, etc.
- **personal**: social networks, associations, trade unions, family, etc.

An identity-centric architecture, based on the progressive aggregation of a cluster of identities, will be scalable by nature.

ICI process

ICI will achieve its objective by:

- defining a full-scale identity layer on top of the current Internet architecture, so that every entity can have a tangible, self-controlled, representation of itself in order to interact / cluster with other parties
- defining a trust framework based on this identity layer allowing interaction through discovery and attribute sharing mechanisms
- inviting key stakeholders and their representatives to define the rules of engagement between the different parties for establishing a governance of an Identity Centric Internet
- implementing a reference architecture to grow the cluster of identities and associated services.

The libraries implementing the architecture will be provided under free software licenses recognised by both the Free Software Foundation and the Open Source Initiative.

A strong proof of concept will be achieved through the implementation of significant use cases for the Future Identity-Centric Internet.

PART B: Section 1: Scientific and/or technical quality, relevant to the topics addressed by the call

B.1.1 Concepts and objectives

Introduction

While the European Commission is reviewing data protection legislation to put forward new legislation in 2011, it is a distressing fact that Europe cannot apply its directive on privacy to its full extent: how can one enforce their right to rectify personal data when most of it is stored in places that are unknown or the result of a long forgotten business transaction? Not withstanding the vast amount of data generated in online transactions, GPS logs (with most anonymised data, the de-anonymisation process is relatively trivial), etc. that are out of our control? What is the power of the European citizen when facing Google and Facebook?

It is a cliché to state that Europe has not succeeded with the Internet as much as it could, and should, have. Indeed, Europe has many great researchers, efficient public and private research infrastructures and competitive businesses, but despite this wealth of intellectual and financial resources we have to recognise that Europe has failed to take any significant leadership role: the current architecture remains mainly defined by a US-centric vision. The Internet governance is also dominated by the same continent. One of the Internet pillars is the domain name system: from the twelve organisations hosting root DNS servers, 9 are American, 1 Japanese and only two are European. Another pillar of the Internet is information retrieval provided by search engines, the gates to the Web: 75% of the requests are performed on either Google or Yahoo!. The third search engine, Baidu, is Chinese. The most popular Web browser remains Internet Explorer which is edited by Microsoft...

The leader of online payment is Paypal[1], online auctioning eBay, shopping Amazon, music store iTune...

Another rapidly-growing pillar of the future Internet is social applications: the leading instant messaging is Live Messenger (Microsoft) and the leading digital social network is Facebook. Three American companies, Google, Microsoft and Facebook, have complete control on the whereabouts of billions of Internet users, from hosting their personal data, keeping logs of their activities and, more critically, managing their relationships, including relationships with businesses. It is Google, Microsoft and Facebook that are the leading parties of *identity provision*. Europe might have different ideas of what identity provision should be, but the hard fact is that we are not leading the actual provision of identity on the web..

Identity on the Web is a central component to the success of emerging technologies and services. New generation networks, sensors, pervasive technologies, connected devices, appliances and services fostering ambient intelligence, are going to be responsible for an exponential growth in the *quantity* and *quality* of linked data (many of them being personal). Emerging technologies will transform the *nature* of the Internet and we have the choice to either lead change or be overtaken by it. Identity and trust technologies are not just a means to *control* change but to enable a larger and deeper change. Identity and trust technologies must be positioned as the *operating system* for innovation and transformation.

Analysis of what is currently happening in the field of trust and identity elicits two main drivers, business and public interests, leading to two different kinds of architecture. The first architecture, led by Google, Microsoft, Facebook and their allies, is essentially to keep the Internet architecture as it is, while adding few patches, here and there, in order to make it easier for businesses to interact with people (and reciprocally). The Internet architecture remains document and site centric; identity and trust are just *add-ons*. In this unchanged architecture, users remain at the periphery as clients, consumers and cease to exist once the transaction is over, except in logs and Customer Relationship Management systems. It is the

[1] PayPal added 1 million new accounts each month during Q2 2010 and is growing 50% faster abroad than in the U.S

pragmatic approach: *If it ain't broke, don't fix it!*. The second approach to the Internet of the Future architecture, that is supported by ICI, recognises that an *identity-centric Internet* (ICI) is not achievable by simply adding *patches* but needs a new architecture and governance.

The Internet of the Future will have to be identity-centric. With the growing number of business and social transactions on Internet, the growing number of connections to personal data repositories will explode. At the same time, a strong relevance of the identity attributes will be needed while personal data will need to be better protected. Indeed, this growth will also increase the threats on privacy, business transactions and the infringement of persons safety. Only an identity-centric architecture can solve these issues and create a climate conducting to trust, innovation and change.

The creation of an Identity-centric Internet is a major opportunity for Europe to take a leadership role in its definition, implementation and governance. While the USA demonstrated their ability to drive successfully a business-centric Internet, Europe can lead the construction of an identity-centric Internet, leading to a better repartition of the contribution to, and exploitation of, the Internet. While we already have the technologies and standards to make it possible now, the implementation of this new architecture will create the bootstrap conditions for a rapid, viral, transformation that will benefit individuals and organisations, public and private interests, for-profit and not-for-profit services.

The Identity-Centric Internet (ICI) aims at setting-up an operational pan-European digital identity and trust architecture for the Internet of the Future. The ICI architecture will be based on the exploitation of existing open standards and open source software integrated by the consortium. The architecture targets a very large-scale architecture that makes transparent and seamless to both users and developers the geographical distribution of components.

The ICI partners believe that we already have the standards and technologies required to build an Identity-Centric Internet, but they have been exploited the wrong way, taking the current Internet architecture not just a *constraints framework*, but as a *reference framework*. ICI identifies the current Internet architecture as a *constraints framework* while providing a new *reference framework*. To use a building metaphor, it is like we had invented concrete and were using it to replace bricks with cinderblocks instead of imagining constructions that would have not been possible without its invention, like the CNIT (see picture) or the Sydney Opera house. ICI offers the opportunity to move away from laying digital bricks (cinderblocks) to build the futuristic digital landscape of tomorrow.

A number of recent experiences have cruelly demonstrated to their participants that Europe regularly fails when trying to make a *better Google* or *better FaceBook*. Europe has a better chance to succeed by doing something where we do not just try to be *better* but *different*, not where we *follow*, but where we *lead*. ICI aims at making Europe the leader of the Identity-Centric Internet.

The ICI architecture will respond to the following requirements.

Large-scale trust architecture

Aimed at reaching over 250-300 million users, individuals and organisations, such an architecture will make it possible for any entity, subject, organisation or person, that have never been involved a digital relationship is able to establish dynamic trust relationships.

The architecture is based on a cluster of distributed trusted identities, making it feasible to both provide trust pathways and to establish peer-to-peer relationships. This architecture will make interoperable macro circles of trust (state federations, telecom operator federations, university federations) interoperating with wide public circles of trust, like social networks, and circles of trust like commercial partnerships.

The identity-centric architecture is scalable by nature (design), so it will be easy to start small and grow quickly and seamlessly.

Global discovery

Trust relationships will be established by an entity with known and unknown organisations, services and people. In order to establish a trust relationship with an unknown entity, e.g. finding a trusted plumber to fix a leak, we need to establish:

1. trust path discovery
2. dynamic interconnection of information systems to work in a peer-to-peer relationship.

User privacy

An identity-centric architecture is required to have subjects in control of the exploitation of their personal data. The architecture will provide users with real control of (possibly *distributed*) personal data, granting means to subjects to be at the centre of protocol exchanges. The architecture will create the conditions to unify personal data and put an end to its increasing *fragmentation*.

NB: *fragmentation*= out of one's control; *distribution*= under one's control.

User mobility

The identity-centric architecture addresses two kind of mobility issues:

- It allows dissolution of European borders for European citizens performing on-line administrative procedures.
- It makes feasible the "Identity in the Cloud" concept: whatever terminals and the Internet media the users are provided with, the identity information is securely available and manageable.

Open source APIs

Open source standard Application Programming Interfaces (APIs) implementing the architecture will be provided via free software licences. These components are fundamental to hide the potential complexity of the architecture. It is therefore a requirement for the adoption of the architecture. Open source software is necessary for transparency and the wide deployment requirements. Such components can then be embedded in other systems such as operating systems.

User interfaces

User interfaces, enabling people able to manage their digital identities hiding all the complexity. These interfaces are dashboards that we detail in the next section. The user interfaces are fundamental for a strong user adoption.

Operational deployment

An operational deployment will prove the validity of the concept. This will include the architecture per UST, but also its quality for adoption: one can build the 'perfect' trust architecture that will never take off. The operational deployment will be the opportunity to involve users in the co-design of the architecture, which is one way to generate true innovation.

Relevance of the Identity-Centric Internet project

The project is clearly in the scope of the first challenge of the call, a pervasive and trusted network and service infrastructure (Objective 1).

The objective "Use case scenario and early trials" (1.8) is the set of objectives Future Internet Public Private Partnership (FI-PPP).

In this set the identity and trust architecture is clearly highlighted as a generic enabler: "trust and identity capabilities enabling end-users, devices, digital objects and service providers to be identified globally and across multiple domains in a trusted manner".

Moreover, an identity-centric internet will make public service infrastructures and business processes smarter:

- an identity-centric internet will increase the effectiveness of business processes and of the operation of infrastructures supporting applications in many sectors,
- an identity-centric internet is propitious for innovative business models in these sectors,
- the goal of the project is to make Europe more competitive on the internet architecture strengthening the competitive position of European industry in domains like telecommunication, mobile devices, software and service industries, content providers and media.

We satisfy the requirements in the following ways:

- We identify, define and update the Future Internet requirements coming from the innovative use cases presented in the following
- The ICI project clearly aims at providing an open standardised generic framework

The consortium has also clearly identified that we are in phase 1 of the project and that knowledge sharing is a strong requirement. The open source software implementations under free software licence of Application Programming interface by specialists of the domain (e.g. Frederic Péters, GNOME release team), and the material for adoption (API, Tutorials, Documentations) are pledged to satisfy this requirement.

We have chosen to address objective 1.8 because we believe it to be the objective that best suits our aims. The objective considers this goal: *identify trial scenarios and derive the Internet platform requirements for a particular usage area; design, develop and implement a domain-specific instantiation of the core platform building on a selection of core platform generic enablers complemented by domain-specific capabilities; provide a limited scale testing infrastructure; validate the platform through early and large scale trials.*

We consider the digital identity paradigm to be one of the main use cases for the Future Internet. Indeed, identity and trust frameworks are fundamental enablers of economic and social relationships over the Internet. The ICI project solves two problems, addressing the digital identity paradigm for the Future Internet:

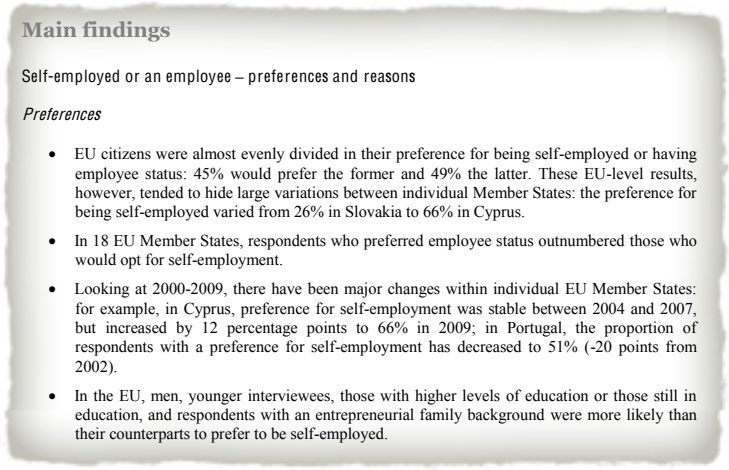
- Realise a concrete large-scale trust architecture.
- Realise a powerful and privacy-respectful identity centric internet.

For that purpose, the project depends on generic use cases and specify profiles of interoperability, to specify in a second time the architecture. We consider that the scientific and technological material to realise our vision is available. Therefore, we will use and enhance such prior state of the art in our architecture. We finally expect a strong proof of concept which justifies the early trial objective.

One particular strong point of the ICI response is the fact that we have placed the question of *adoption* at the centre of our proposal: this is why the early trial of the architecture on a series of use cases will be useful to guide the architecture design of the ICI project.

Use Cases

In the annex we have provided the details of a number of use cases. They have been selected in order to demonstrate how the ICI architecture can contribute to the development of social capital by creating the conditions for the emergence of 21st century employment patterns.



Main findings

Self-employed or an employee – preferences and reasons

Preferences

- EU citizens were almost evenly divided in their preference for being self-employed or having employee status: 45% would prefer the former and 49% the latter. These EU-level results, however, tended to hide large variations between individual Member States: the preference for being self-employed varied from 26% in Slovakia to 66% in Cyprus.
- In 18 EU Member States, respondents who preferred employee status outnumbered those who would opt for self-employment.
- Looking at 2000-2009, there have been major changes within individual EU Member States: for example, in Cyprus, preference for self-employment was stable between 2004 and 2007, but increased by 12 percentage points to 66% in 2009; in Portugal, the proportion of respondents with a preference for self-employment has decreased to 51% (-20 points from 2002).
- In the EU, men, younger interviewees, those with higher levels of education or those still in education, and respondents with an entrepreneurial family background were more likely than their counterparts to prefer to be self-employed.

According to a recent survey[2] 225 million European citizens would like to be self-employed while 30 million more are currently involved in entrepreneurial activities. We have also provided use cases related to social networking and healthcare as they are yet another powerful means to grow social capital. For each use case we emphasise the Unique Selling Point (USP) of ICI.

The use cases will be exploited during 2 phases:

- **design**: use cases are the initial requirements to be supported by the architecture
- **implementation**: they are the contents of the early prototypes, that will serve as a foundation for the *call for tenders* that will be issued once the architecture is ready and an alpha version of its implementation is available.

Use cases are:

- Use case 1: employment mobility in Europe —who needs an (bad) employment agency?
- Use case 2: Self employment —achieving the dream of 225 million European citizens!
- Use case 3: Business creation —finding partners, investors and clients in one go!
- Use case 4: 21st century worker —part time employee, independent and social entrepreneur!
- Use case 5: re-localisation of the economy —reduce carbon footprint while revitalising local communities and economy!
- Use case 6: Vendor Relationship Management (VRM) — CRM is dead!
- Use case 7: Social networks —Facebook is dead!
- Use case 8: Demand Chain Management (DCM) and Demand-Driven Supply Network (DDSN) — Supply Chain Management is dead!
- Use case 9: Ambient intelligence and pervasive networks of the Future Internet —
- Use case 10: ''Break glass'' policy —help!
- Use case 11: eVoting — make direct democracy a reality!

All use cases are build on the idea that (meta) data is freely and (truly) anonymously accessible by trusted services, and innovative services can exploit This data anonymously in order to create new *personalised* services by linking multiple sources of data and services — "*I am an entrepreneur, give the 10 CVs of the people I need to create my business, a list of potential clients and investors*". They also show how ICI, a symmetric architecture, changes the relationships between individuals and organisations making a reality what once were little more than elusive dreams: Vendor Relationship Management (VRM) systems and Demand-Driven Supply Networks.

---

[2] Entrepreneurship in the EU and beyond, A survey in the EU, EFTA countries, Croatia, Turkey, the US, Japan, South Korea and China

The Identity-Centric Internet project Vision

As David Siegel writes in "The Power of Pull": "Our information infrastructure isn't scaling up very well at all. The average person now sees over 1,000,000 words and consumes 34 gigabytes of information every day. Mike Bergman estimates white-collar workers spend 25% of their time looking for the documents and information they need to do their work. One billion people are on-line now, and 4 billion have mobile phones. Exhaustion of IPv4 addresses (limit is 4 billion) is predicted for sometime in 2011. By 2030, there will be a minimum of 50 billion devices connected via Internet and phone networks. Our information infrastructure is built to haul electronic versions of 19th century documents for humans to read, and it's keeping us from using information effectively."

While the debate concerning the primacy of either structure or agency on human behaviour is a central ontological issue in sociology, political science, and the other social sciences, what can be said about the Internet? What relationships are there between structure and agency, between the Internet (architecture, technology, governance, businesses, organisations etc.), and the capacity of individuals to act independently and to make their own free choices? How do varying conditions (political, economical, sociological, technological and legal) influence individuals' sense of agency? Reciprocally, how does the structure emerge as the result of agents' interaction with and within the Internet? How can reflexive self-knowledge and self-control over one's representation contribute to one's emancipation and be conducive to improved relationships with others (individuals, organisations, businesses)?

While the emergence of social networks has certainly contributed to an increased sense of agency, they have not yet contributed to any kind of decrease of personal data fragmentation. Moreover, personal data in reality 'belongs' to the social network's host, not to the individual. Facebook, Google and others alienate personal data for their own profit in exchange for services such as hosting data, connecting to others, finding information etc. What might initially appear to be fair trade is in reality an alienation process where *free choices* are limited by what the service provider sees fit and destroying the main elements of one's identity when a person decides to quit the social network: one can probably export photos and other digital artefacts, but relationships, historisation of exchanges, reputations are lost — when leaving eBay or Amazon, vendors can take their goods with them but lose their reputation, as this is part of the service provided by eBay and Amazon.

One of the goals of ICI will be to provide an increased sense of agency by dissociating the storage of data, metadata, history and relationships that are part of one's identity from the service provision.

The increasing number of digital data, by and about ourselves, leads to the emergence of what is now referred to as 'digital identity', i.e. all the attributes and digital production by and about a person — school records, health records, employment records, business records, credit records, surveillance records, etc. But digital identity is not just a set of attributes stored in a personal database that could be isolated from the rest of the Internet: it also includes relationships to others, individuals, organisations, businesses, ideas, values etc. It is not possible to 'locate' someone's identity in a particular point, or even in a limited series of points, as one's identity is composed of self-identity (Giddens) and identity through others (Laing). Translated into the Internet, that means that one's identity can be located in places under one's control and places under others' control, such as a public authority (e.g. identity card provider), a business (e.g. credit card provider, a university (e.g. a diploma provider) a colleague (a testimony provider) a client (a testimonial provider) or a foe (a trouble provider). So, by nature one's digital identity(ies) is distributed over the Internet, over other people and organisations.

As result of today's Internet architecture, digital identities are not just distributed (which is in the nature of identity), but 'fragmented' across an ever increasing number of services, often without our knowledge or our informed consent.

This increased fragmentation leads to a series of problems:

- Individuals do not have the means to control how their personal data is being used by the myriad of Internet services they interact with —something as elementary as the ability to update or erase personal data hosted by third parties is the exception, not the enforced rule.

- Organisations have to pay a high price if they want to protect the personal data they handle; and many do not know how to do it properly and if they do, there is still the risk of mismanagement and hacking, especially for those hosting mega databases of personal data.
- Businesses have to pay a high price to keep records of prospects and clients, and even more to reach new prospects while most newcomers have to face high barriers to enter a market.
- Marketing is being dominated by de-facto monopolies concentrating the collection and exploitation of personal data without real informed user consent.

While standards and technologies, in terms of Identity and Access Management (IAM) and Privacy Enhanced Technologies (PETS) are sufficiently developed to provide a 'good enough level' of control and protection, current implementations have not provided the degree of transformation expected to address all the identified problems. And they lack scalability.

To achieve the level of transformation required, and expected, we need to move from an Internet where individuals are at the periphery of the architecture, as users acting behind a browser, to an Internet where individuals have a proper tangible representation of themselves, aggregating (even hosting) all their personal data and select what services (and people) can access it. This can be achieved by an architecture based on a separation between the storage of data and metadata from the services creating and exploiting them. In other words, the solution to the protection of personal data is not to be found in higher and thicker walls around large farms of personal data (health records, bank records, education records). Protection is to be found in:

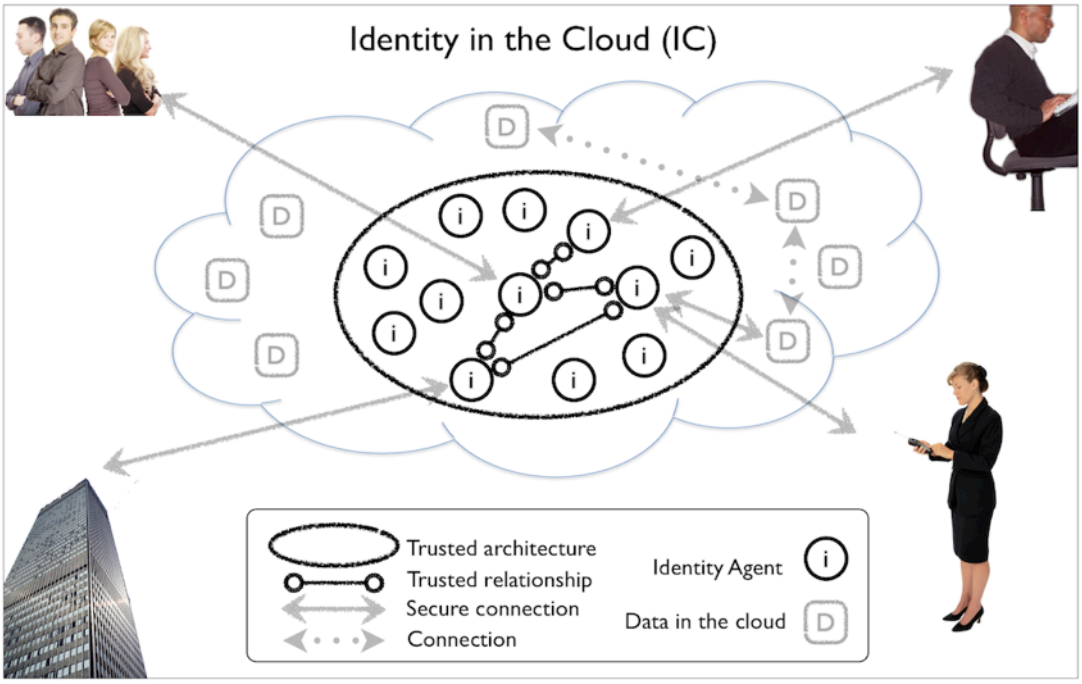
- the total separation between the storage of personal data and their exploitation by organisations,
- the dis-aggregation of organisation-centric data systems, and their re-aggregation around identity-centric systems.

Many agree on a similar architecture even if the names differ: Identity Centric Internet (the name of the project), Attribute-Based Architecture (a distributed model with discovery mechanisms) and the Internet of Subjects. There are different possible implementations, from providing each individual with a personal data store, or personal locker, to providing a proxy through which individuals can interact with other individuals and organisations. It is also possible to have each person storing all their personal data, including logs, geo-positioning data, etc. in distributed data stores, some of them being provided by trusted service providers. Removing any physical barriers, such an architecture makes concrete the *Identity in the cloud* concept.

Identity in the Cloud

Identity in the Cloud (IC) is based on the idea that every entity, person, network or organisation, is represented by a *thing* to manage the storage and access control to personal (resp. organisational) data. We will call this *thing* an IC-Agent: it is through the interaction among IC-Agents that trustworthy relationships are established and developed.

In the course of the project, in order to focus the proof of concept, IC-Agents of collective entities, like networks, organisations, businesses, will be managed by one person, some kind of webmaster or sysadmin. If the proof of concept is satisfactory, it will be possible to manage such IC-Agents either through a gateway with the legacy system or inviting employees to create their own IC-Agents to establish trust relationships with the *collective* agent —which is just another IC-Agent.



The *society of IC-Agents* is democratic and egalitarian; a person, like an organisation, can potentially be:

- attribute provider / consumer
- identity provider / consumer
- service provider / consumer

In the use case described below, *the 21st century worker*, the same person can simultaneously (or successively) be employee, employer, sole trader and social entrepreneur. It is therefore critical that the IC-Agent representing her is able to find an employer, employees, partners and clients, under the same or different identities.

In an identity centric Internet, what the old 'ex-centric' identity paradigm called identity provider (IDP), is now one *IC-Agent* among others. IC-Agents can be more or less trusted than others, and the decision to trust or not belongs to the party receiving information; decisions can be made either because the IC-Agent knows the party or after calling a *trust computing service* providing in real-time a trustworthiness indicator, just like one would ask a friend: "*do you trust so and so?*"

The process for joining the ICI is straightforward: every entity willing to join simply creates an IC-Agent, the creation of such agent being sufficient to automatically join the *Society of IC-Agents*. Such agent could run on a personal device, a set-top box, a server in a cloud-computer etc. The IC-Agent can also travel in the cloud while preserving its *identity*.

Dashboard

Next, users must be provided with a dashboard providing a unified view of their *identity in the cloud*. This dashboard will provide individuals with a unified view of

- fragmented personal data in the current architecture: all 'by me' (R/W control) and 'about me' (R control)
- the means of access and usage control of their personal data: private access control and privacy policies, privacy indicators, risk indicators, etc.

- all the operations revealing personal information: authentication, self asserted personal data propagation, administrative procedures, social network relationships, traces etc.

NB: such a dashboard will offer a place ('about me') for existing service providers to 'register' which data they use, providing individuals with the means (e.g. a simple encrypted pointer) to rectify stored data, creating the conditions for practical applicability of current European privacy legislation.

The dashboard will reveal trust indicators about interlocutors to individuals and to interlocutors about individuals. It will become the interface to establish trust relationship across parties. Such indicators can be recommendations, member ratings or certified data.

NB: reputation indicators can be dynamically computed (by a trusted external party) from data collected from external sources listed in the 'about me' part of the dashboard (e.g. provider, authority, colleagues, friends, etc.)

Ultimately, the dashboard will provide citizens, not only with the means to have a certain level of control on their personal data —which is almost impossible within the current architecture— but also to create the conditions to put an end to the fragmentation of personal data through the adoption of personal data stores, personal lockers or personal proxies, as a means to store personal data independently from services. In storing personal data independently from services individuals will become the hub of interoperability across heterogeneous services and organisations. It is an opportunity for the emergence of new and improved services in a number of sectors, i.e. ePortfolios and personal learning environments (education), personal health records (healthcare), personal knowledge management systems (employment), and vendor relationship management systems (business).

NB: Personal data stores(PDS) are logical units, not physical; so a PDS can be distributed over a number of hosting providers with different levels of security.

Liberating personal data from service silos will create the conditions for innovation and the emergence of new services, just as what is happening today with the liberation of public data and initiatives such as "raw data now!", led by Tim Berners Lee.

To illustrate the transformative effect of a dashboard, we can define a kind of maturity matrix, from simple awareness to transformation:

- Level 1: data storage remains fragmented across services, but people can have a global perspective of where it is. Personal data can be discovered by trusted services.
- Level 2: data storage remains fragmented, but people can aggregate data and assign policies within the dashboard.
- Level 3: data storage remains fragmented, but an increasing part is stored in a personal data store; some service providers accept to use PDS to store / copy transaction data.
- Level 4: a majority of service providers have accepted to primarily use PDS to store personal data.
- Level 5: legislation has made mandatory that all personal data is stored in a store chosen by individuals. People have a tangible representations of themselves on the Internet through a personal proxy.

NB: the project will provide a more complete maturity matrix with additional columns for legislation, service provision, identity providers, hosting providers, etc.

The benefits of such an architecture are numerous:

- innovation— thanks to the liberation of data from applications and silos
- data and people are easily findable —thanks to trusted discovery mechanisms
- interoperability —as data is stored or made accessible through the dashboard or some kind of personal proxy
- co-operability —multiple, independent services will be able to interact with the same sets of data, just like in a Unix pipe command
- massive meaningful anonymous interaction —connect instantly all people / organisation with a specific profile, independently from service providers

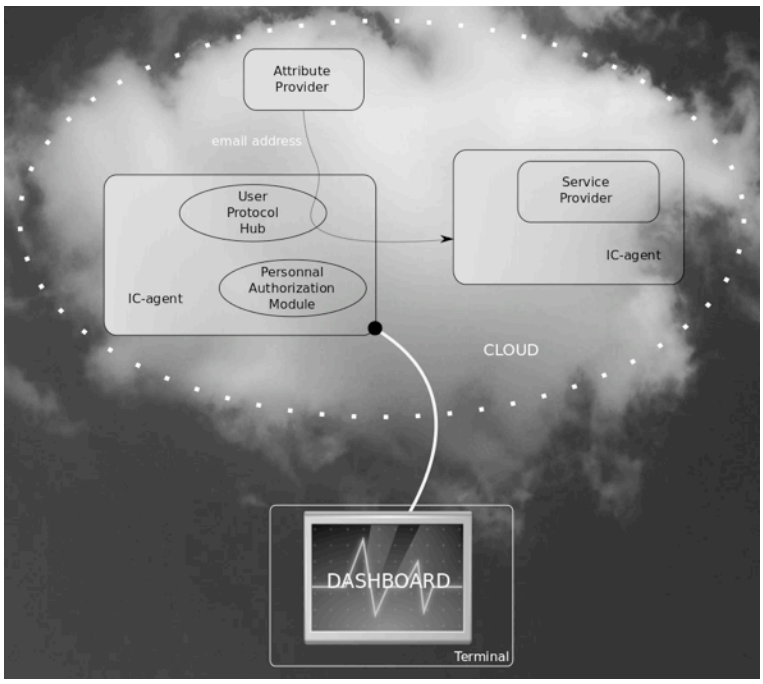
- vendor relationship management can become a reality —without such an architecture VRM services cannot be much more than glorified data silos...

The Identity-Centric Internet project answer

Here, we present the technological answer to build an Identity-Centric internet.

Overview of the architecture

When a user consumes a service on-line she can be requested to provide personal data. Such data can be used to provision the service, for instance providing an email address to receive a newsletter. This data can also be used to perform access control. For instance, a service provider requires that a user be of age and have a valid driver licence to be able to rent a car.

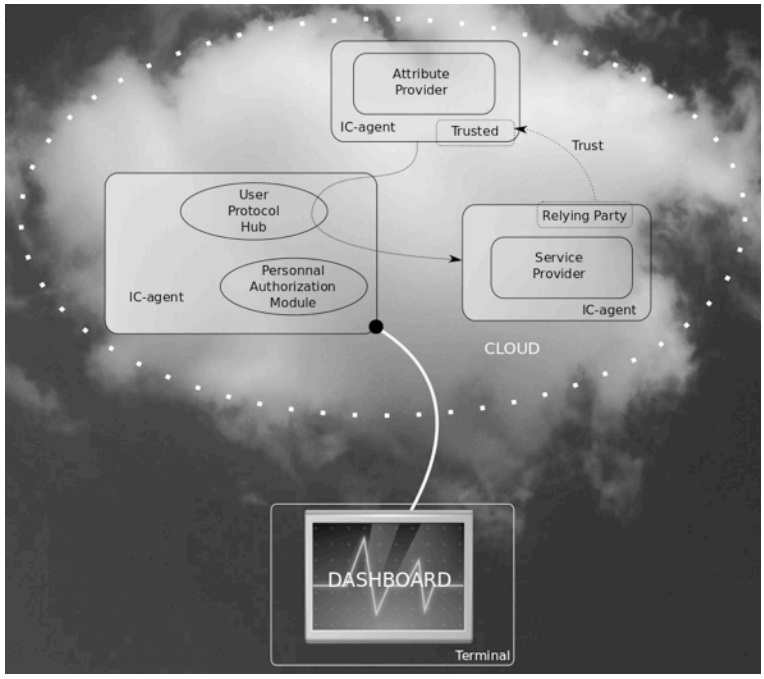


The attribute may be self-asserted by the user, e.g. the email address can be filled by the user. In ICI, the service provider is expected to provide to the IC-Agent an attribute requirements policy, indicating that an access control policy requires, e.g., user's email address. The IC-Agent analyses the policy. If the user has an attribute provider able to provide this data, the IC-Agent requests via the dashboard the user's consent for distribution. Otherwise, it asks the user to provide the attribute value (i.e. self provisioned and self asserted) and stores the attribute value for future use in the user's attribute provider. The IC-Agent then provides the email address to the service provider as shown on figure 1.

In a car rental use case, the service provider indicates in the attribute requirements policy that it expects certified data from a trusted attribute provider (driving license authority). The IC-Agent determines from the policy, and the trusted attribute providers of the user, where the data can be obtained. Then, either the IC-Agent retrieves the data and presents it to the service provider (relying on the User Protocol Hub component as shown on figure 2, next page), or the IC-Agent delivers an authorisation to the service provider (relying on the Personal Authorisation Centre as shown on figure 3, next page). Then the service provider retrieves it in a peer-to-peer relationship with the Attribute Provider. When consuming attributes from trusted attribute providers, the service provider relies on third parties to perform access control and is thus called a *relying party*.

It is important to consider is that a trusted party is trusted from the information consumer point of view. Then, each party can trust a set of known third parties and can also trust anyone else connected to the trust architecture. The user can be provided with attribute providers not directly trusted by the service provider. However, a trust path may exist between the service provider and an attribute provider of the user. The IC-Agent can then indicate the service provider to the attribute provider and ask it to establish a trust path. Or, conversely, the IC can indicate the attribute provider to the service provider and ask it to discover the trust path. If trusted nodes exist, the trust path is discovered. Then, according to their agreement policies, the service provider may establish a trust relationship with the attribute provider. The agreement policy of the service provider could include a privacy policy indicating that the service provider satisfies certain requirements about personal data storage, for instance. The agreement policy of the service provider may also contain authentication and attribute policies

indicating requirements on the expected strength of the user authentication process on the attribute provider and on the quality of attributes by the Attribute provider.

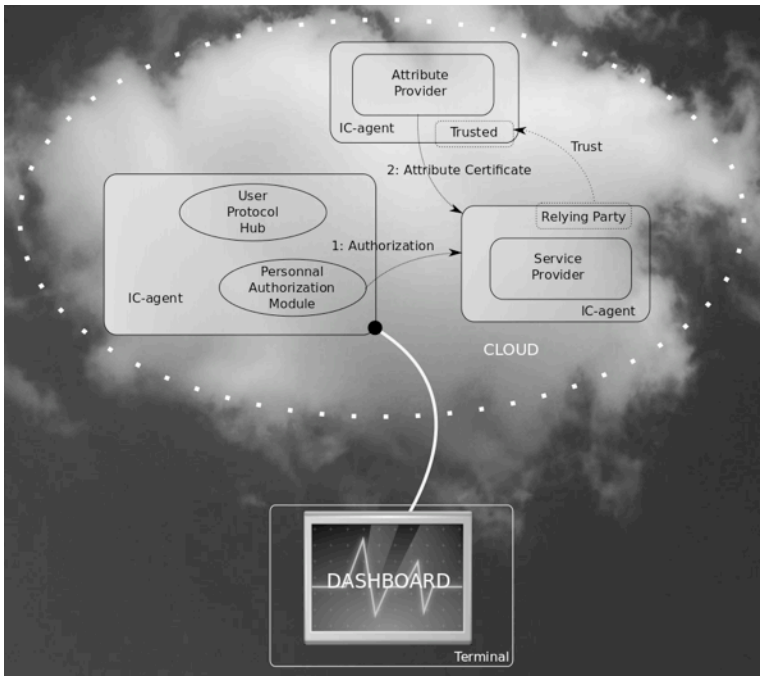


Before providing personal data to the service providers, the IC-Agent retrieves the service provider's privacy policy and compares it with the its own privacy policy. Then, the IC-Agent may ask the user for consent though the dashboard, or may automate the diffusion if the user has previously authorised this diffusion.

Authentication and authorisation

These operations may require the user to be authenticated with the attribute provider and the service provider. More precisely, either the IC-Agent authenticates against the attribute provider to retrieve the identity attributes, or the IC-Agent delivers an authorisation to the service provider. Then, the attribute provider must be able to authenticate the authorisation as having been delivered by the user. The IC-Agent must thus host credentials to be authenticated by attribute providers and also cryptographic material to sign authorisations, the attribute provider being able to authenticate the users' signatures. The IC-Agent is the place for storing authentication materials. This material can also be used to authenticate against service providers. The IC-Agent then acts as an identity provider in the sense that it allows authentication on every third parties providing a single sign-on system.

The authentication to third parties consists in providing per party credentials necessary for identification. However, trusted identity providers are still necessary. These are in charge of providing the per party non-correlatable identifiers (aka pairwise pseudonyms) of real user identities. This makes it feasible to revoke anonymity by legal request to the trusted identity provider. For instance, when a user only needs to authenticate on a personal webmail, the IC-Agent authenticates the user on the webmail relying on the local identity provider. For renting a car, the service provider may not maintain a user account but may require a pointer on a real identity of the user. Then, the user would be required to provide certified pseudonym obtained from an identity provider trusted by the car renting company.



The IC-Agent may play a strong role in architectures with cryptographic credentials. In such architectures, the user must perform some operations on the certificates before presenting them to relying parties. These kind of certificates allow for instance multiple-time use certificates with selective disclosure (cf. Idemix and U-Prove). The IC-Agent may retrieve and store such certificates. Then, according to the service providers access control

policies, the user would only reveal a subset of the attributes contained in the certificates. More sophisticated functionalities can be realised, for instance, the user would be able to prove that she is of age without revealing the date of birth contained in a certificate. This kind of certificates are very useful when strong privacy is required, for instance for e-voting and e-cash.

The IC-Agent has a central place by design. It is thus the right place to monitor and log all personal data disclosure and related authorisations. It is also possible to journalize user accesses and traces known by third parties.

An online IC-Agent ensures accessibility to personal data in a user mobility context. It also ensures the user-controlled personal data access when the user is not directly involved (off-line), e.g. when a break glass policy must be applied as consequence of an accident.

In the following section, we provide more details about the trust architecture and the IC-Agent.

The Trust architecture

The trust architecture is based on a root of trusted nodes that form a meshed network of trust. A node can give an agreement to another entity that de facto becomes a sub-level node in a hierarchy. Then, the trust architecture becomes a hierarchy with multiple entities at the top.

An agreement indicates that a upper level node assumes the responsibility to ensure that its sub-level nodes respect a number of requirements. A sub-level node may then be trusted because the upper-level node is trusted to deliver agreement on these requirements. For instance, at any position in the hierarchy, we may find a banking authority delivering agreements to banks.

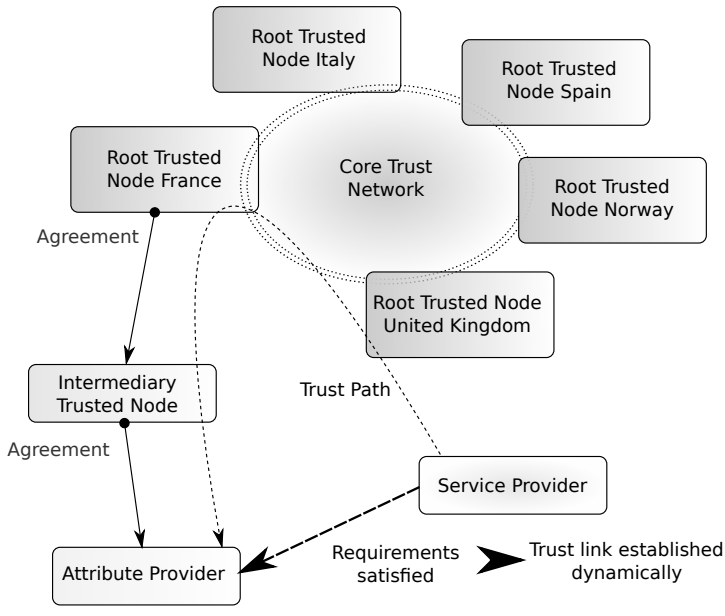
Requirements satisfied by a node are certified by its upper level node. Then, a dynamic trust relationship may be established because a party digitally unknown satisfies a set of requirements.

The agreement policies are the policies used to indicate the requirements to be satisfied. It is in fact a kind bag of policies that may contain privacy policies or authentication contexts. These policies may also contain cryptographic material and applicative endpoints.

It is important to consider that the position in the hierarchy does not mean that the root authorities can deliver agreement on any types of requirements. It is not their role. Their role is to bootstrap the process of agreements to deliver agreements on basic sets of requirements. Then, specific nodes will enter the trust architecture, e.g. universities, public authorities, bank authorities, and each one will deliver its own agreements on the requirements of their domain.

From the agreement policies, a trust link can be established. However, it is necessary to previously discover a trust path, from the relying party to the potential trusted node. This is the second role played by the root authorities.
As in a DNS architecture, they will be used to discover a trust path made of one or many intermediary trusted nodes.

For instance, an attribute provider may be a trusted node. A relying party may search a trust path to that (unknown) attribute provider if a user provide the service provider with a certificate of this attribute provider. The service provider would make a discovery request to its upper-level node. Like a DNS request, the path will be found through the root trusted nodes. The relying party will then be able to look at the agreement policies of the intermediary nodes to validate its requirements. If the requirements of the relying party are satisfied, the relying party establish a trust link with the attribute provider and accept the user attribute certificate.



This trust architecture is a requirement in establishing dynamic trust relationships in business and e-administration domains. Transactions of this kind need assurance and governance relative to the service provider requirements needs. For social networks, there is no strong requirement for those agreements mechanisms since the trust is mainly based on informal criteria. For social networks, we will mainly rely on attribute certificates of 'friends' or 'friends of friends' to establish the credentials of requested attributes.

To prove this concept, we plan to deploy the root nodes of the trust architecture in several organisations among the project partners : URC/Italy, FRK/Norway, NOTT/United Kingdom, TBS/Spain and ETO/France. We will then rely on the dissemination work package to have other nodes joining the trust architecture.

Auditing infrastructure

Messaging

The development of the trust framework and identity management architecture supports individuals in a live scenario. During the phase of user engagement it is expected that services may change in terms of reputation and events such as notifications of data access will be sent to the user's dashboard. This messaging in the back channel will be supported by a robust auditing bus infrastructure that handles with high reliability the delivery of application critical messages to support the live system.

Storage

The Auditing Bus will also plug into databases to store the audit information from the system. This storage will ensure that the central infrastructure is anchored and any past application executions can be checked. In terms of retrospective analysis of interaction it is expected that users may wish to query this following an alerts via the dashboard or post application execution reports they may receive.

Query

In terms of user friendly audit querying, there are a few examples that we can refer to. Looking at the banking industry and the way transaction logs are kept by banks is a good insight into possible developments. Many online banking system software equip users with the means to analyse their bank statements. In this context, commodity is money, while in ICI scenarios we are analysing personal data accesses, an issue that could be as sensitive as unauthorised financial transactions.

Thus the project will investigate and design audit querying software to complement the Audit Bus and storage services. This software will be presented within an Auditing Service and made available for users to query past transactions.

The "Identity in the Cloud" Agent (IC-Agent)

Presentation

The "Identity in the Cloud" Agent (IC-Agent), is a logical system that symbolically represents the avatar of one entity in the Cloud. In the Future Internet, any entity would be provided with its own IC-Agent. As previously introduced, the IC-Agent gathers many functionalities in order to provide a seamless user experience when personal data propagation is necessary. It provides a unified view of data sources. Above all, it ensures privacy, making it feasible to avoid direct exchanges between an interlocutor and trusted third parties, to achieve easily manageable pseudonymity and to use cryptographic certificates with advanced functionality.

Nevertheless, the IC-Agent is not a fortress, less still a bottleneck or a single point of failure. The IC-Agent is a "physical" aggregator of personal data. It only provides means for a unified view with a dashboard. And this, even if only a fraction of personal data is directly hosted by the IC-Agent. It is exactly the same as with a driver's license. Everyone host a physical document that is a duplicate of an entry of a state admin registry. If one loose the document, it is possible to ask the state administration a duplicate because the state administration hosts what can be considered as "one's driving license". With digital attribute certificates, the attribute provider host the data. The users can obtain one-time use attribute certificates dynamically and present them (the most common way), or the user can give permissions to an interlocutor to retrieve it directly. However, the user may also host a "copy", a multiple-time use certificate, and present it as needed.

For, a better user experience, the IC-Agent may host a local identity provider that would be in charge of managing authentication with third parties. It is the way OpenID works. It is an identity provider online providing users with a better experience by avoiding the submission of multiple login and passwords. However, this kind of mechanism does not remove the need for keeping authentication mechanisms: if the chosen identity provider goes off business, a user can still log in with the credentials of the different service providers (usually a login / password). This can be considered as a built-in recovery mechanism. It may be the same with the user personal identity provider.

An IC-Agent is not more an impenetrable fortress than a user laptop, mobile phone or a set-top box accessible online 24/24 7/7. Any host stores a number of sensitive data but they are not designed to prevent massive and aggressive attacks. The IC-Agent does. The IC-Agent is a central point where most of the user communications converge. But it is not more that the Internet access point to which the user terminal is connected. However, a specific system designed for privacy, like the IC-Agent, may have a built-in privacy mechanisms as onion routing, a technique hardly accessible to the wider public. Moreover, if the attack is massive, *the society of AC-Agents* can act quickly, independently, while organising a collective defence, at least by communicating to trusted parties that they are under attack.

Even if an IC-Agent was just as prone to failure as a user terminal or an OpenID provider, the difference is that it is much easier to create an unlimited number of *clones* of an IC-Agents (a glorified name for a simple back-up) that could be rapidly reconnected to the trust network —a much more user friendly process than asking users to manage their own backup.

Where are IC-Agents hosted?

This is a fundamental question that everybody should ask. The IC-Agent is in the cloud, but where in the cloud? Many answers are possible.

The hosting environment must be fully trusted by the user, trusted like the user trusts her own laptop and mobile phone —even more.

We plan to conceive a prototype for the paranoid. An IC-Agent that anyone could deploy on a personal server installed from scratch, with data split and encrypted between multiple databases. That would be the same prototype as the IC-Agent for organisations. We also plan more integrated deployments for the wide public as IC-Agents for mobile phones and ISP set-top box.

However, one must pay attention to the fact that, due to their physical proximity, mobile phones and ISP set-top boxes might provide users with a false sense of security, privacy, and ownership of personal data: "my data is here". To the exception of the expert able to dive into the operating system of these devices, most users will not be aware of the content of the outbound traffic of set-top box that are administered by third parties: operators, constructors, etc.

An alternative would be to use a third party to host the IC-Agent —one could even a 'moving' IC-Agent, changing location to increase its anonymity while preserving its identity. Such organisations could be regulated, they could be registered and audited to be able to provide this service. Users should have the choice to deploy the IC-Agent on their own server but would be also able to pay for this —this could also be a service provided by public authorities. The ICI project will explore whether there is a market for this kind of service. While there are emerging companies providing this type of services, today's provision is not easy to decipher: it is anarchic, uncontrolled and unregulated.

One of the objectives of ICI is to explore the conditions for the emergence of a sanitised market for personal data hosting. We will be working on defining the requirements for being able to audit these services to validate their conformity with local legislation on privacy.

Functionality and symmetry

We have already introduced the main functionalities of the IC-Agent.

However it is important to consider the symmetry of a relationship. Even if we still consider the point of view, the user, requester, and the service provider, that answers. Other, all entity provided with an IC-Agent is potentially a user, a service provider and an attribute provider. For instance, the service providers require the user to provide certificates to prove that she is of

age. The user can at the same time require from the service provider that it provides her a certificate from a customer rating site. A user can access a service provider because she can obtain a certificate from a state administration trusted by the service provider. In a social network, I can give access to some data to friends of friends. We are attribute providers delivering certificates to friends saying we are friends. They will use them to obtain access from indirect friends. The users lambda perform an access control on her personal data. An organisation do the same on its services. The subjects of the access control rules are only of different kind, that does not matter the algorithm of decision.

The conclusion is, whatever the entity represented by an IC-Agent, the IC-Agent has the same core functionalities. For some entities, some extra functionalities are needed. According to the entity, we have to preconfigure the IC-Agent differently. The dashboard must be different. However, the core algorithms are the same for every entity, only the set-up varies.

IC-Agent integration

Having the IC-Agent publicly addressable means that the IC-Agent must be discoverable. It is a requirement to make the personal data accessible when the user is not involved, for instance in social networks. We could rely on the actual DNS system, but it less powerful than relying on the trust architecture since the trust architecture also allows to discover trusted nodes.

Conversely, the IC-Agent is directly called by users when they want to reveal personal data. For privacy reasons, we do not expect that by default a public address of the IC-Agent by given to each interlocutors. Conversely, by default, we expect to avoid the user to reveal any identifier. The architecture must be designed as a consequence. Then, the user is free to reveal data making her transactions linkable by an identifier. However, if the users does not voluntarily reveal such data, users' transactions remain unlinkable.

For, instance, if the mode of integration is to use the IC-Agent as a real protocol proxy, the user would connect to service providers through the IC-Agent, and the IC-Agent communications with a service provider would be routed over a TOR network for instance. In that way, the IC-Agent is not publicly known by default.

If the integration of agent implies that the service provider learn the location of the IC-Agent to make the user able to reveal her personal data, all the transactions are linkable if this location don't change. However, this can be prevented making the IC-Agent host able to modify its location and making the user able informed of each new location.

Many solutions are possible, and the notion of linkability of transactions will depend on IC-Agent mode of integration.

It should be considered that the ICI architecture won't decrease the privacy from this point of view. At worst, the mode of integration will result in the same traceability as in the actual architecture, for instance with an IP address. However, the ICI architectures makes possible strong mode of integration, even the anonymity in the sense of unlinkable user transactions is possible.

Modes of integration

Then we can sketch the different modes of integration of the IC-Agent in the applicative flows. To sum-up, the user consumes a service on a service provider, the service provider ask for personal data, the personal data must be delivered by the IC-Agent.

The modes of integration are now well-known. A piece of additional software may be necessary, either on the service provider, either on the user terminal (for instance a Web browser plugin). The role of this piece of code is to trigger the call to the IC-Agent. If it is hosted on the service provider, the user must be provided with an easy mean to indicate the ID-Agent location. It it is hosted on the user terminal, the configuration of the software contain the IC-location.

A third way of doing this integration avoid this discovery method. The IC-Agent may be inline, between the user terminal and the service provider. When the service provider asks for personal data, the IC-Agent is able to catch the personal data request and is able to handle it.

All these solutions have advantages and drawbacks. The ICI will specify them and will prototype the most relevant.

All these solutions relies on a secure communication between the user terminal and the IC-Agent, even if the IC-Agent is hosted by the user terminal.

Overview of the name spaces and ontologies

Namespaces and ontologies address two dimensions of the ICI project:

- identity credentials
- service provision based on the exploitation of personal data

An ontology of identity credentials, is an explicit specification of a conceptualization of identity credentials, including the actors, actions, and objects that establish the relationships of their production, use, and destruction. Ontologies for service provision are domain dependent, e.g. employment, ICT, legal etc. and the relationships between their components.

While not at the core of the project, ICI will certainly explore the contribution of ontologies —for example, the exploitation of identity credentials ontologies could be an alternative to XACML.

Open specifications and implementations, a requirement for transparency

Why not propose to develop IC-Agents and the software for the deployment of the core trust architecture. We will do prototypes of components to validate the concept. But it will obviously be the role of the software developers, editors and societies to develop their own product for real deployment purpose and to feed the public offer.

However, we propose to specify Application Programming Interfaces and to implement them as libraries. The API will give a common signature of the functionnalities of the core architecture. Then, the libraries will implement the basic standard blocks necessary for interoperability, like the protocol flows. The goal of an API is to expose as simply as possible the basic functions. In that way, an API hides the underlying complexity of the architecture. A library implementing an API makes the features of the architecture easily accessible and allows a non expert developer to handle the architecture to develop higher level software.

The API and libraries are thus requirements for the adoption of the architecture. The library developed will be designed to be used in a productive environment. They will be open source and published with a free software licence. We think that open source software are requirements for an architecture that handles sensitive data like personal data. It is a pledge to users of the architecture transparency. Transparency does not mean security but security can be audited by accessing a code publicly available.

Several of the partners are experts in API conception. SAML2 is the core protocol of the ICI architecture. SAML2 is also the standard for architectures of identity protocol architectures. SAML2 is for exemple used by all the state and university identity federations across the world. In the ICI consortium, there are the publishers of the only libraries of SAML2, Lasso (Entr'ouvert) and ZXID (zxid.org - Levelview). Moreover, both are used in large-scale production environments, and both are certified conformant to the SAML2 standard, conformance delivered by the Kantara Initiative Consortium. Kantara initiative, formerly know as Liberty Alliance, stronly contributed to the SAML specifications before the normalisation by the OASIS.

For a better, adoption all the libraries will be usable in at least two languages between C, PHP, Python, PHP and Perl.

Then, the following API will be specified into the ICI project:

- API to discover the trust paths
- API to retrieve agreement policies (add in WP2 the definition of a basic agreement policy to sketch the use cases)
- API to establish a peer to peer trust relationship
- API of the User Protocol Hub (will support the different roles defined in the specifications of SAML2, OpenID and WS-Trust)
- API of the Personal Authorisation Enter

The most relevant API for adoption will be developed under the following Open Source Licences: GNU GPLv2 and above, BSD and Apache.

Dashboard and interfaces

A dashboard will be designed for the different use cases. However, these use case are sufficiently generic to make the dashboard interface specifications cover a great part of the needs. A dashboard will be developed to realise the proof of concept.

To sum-up we expect that the dashboard provides the interface to make the users control their IC-Agent. This include but is not limited to:

- Make decision about data propagation, select attribute sources, obtain and present attribute certificates, deliver authorisations.
- Verify the interlocutor identity and consult trust indicators about the interlocutor.
- Configure personal data access control for automatic diffusion.
- Consult journals of events.

Another work proposed by the project is to study the cases where users are provided with limited interfaces to give instructions to the IC-Agent. We then consider workflows raised to obtain the user agreement for personal data diffusion when a third party requests it and the user is not involved in a direct communication with the requester. For instance, on a crash scene, users could be required to validate diffusion of their personal by presenting their fingerprint on a terminal of the police. Or, when someone a health record, a consent request could be sent on the mobile phone of the user to validate the diffusion.

Science and Technology (S&T) Objectives

The project has defined a number or science and technology objectives:

Scientific objectives

- Formalize the identity in the cloud paradigm as a networked, interactive, social or fuzzy identity (being a personal and social construct, one's full identity is not restrained to a limited set of attributes that can be isolated from the rest of the Internet);
- Formalize and analyze the security properties of the identity-centric architecture.
- Analyze efficient algorithm for complex trust path discovery.
- Formalize and analyze the quantity of personal data spread at any moment. Highlight greedy service providers and the threat on privacy according to potential third parties collusion.
- Study and implement the discovery mechanisms to provide the means for
- anonymous discovery (in a social network context) —be able to find all the people or organizations with specific attributes and be able to interact meaningfully anonymously and massively.
- Analyze the trust and reputation paradigms to make efficient algorithm used to provide trust indicators to users (individuals and organization) and to be used in automated trust establishments.
- Study the user behavior and identify the needs on user interfaces. Identify risky behaviors when revealing sensitive personal data. Propose means to address this issue.
- Identify unexpected user interfaces in pervasive environments and anticipate for compatibility with the IC-agent.
- Identify new logical systems, model them and prove their properties.

Technological objectives

- Design the ICI reference model and requirements
- Define a protocol framework based on existing standards.
- Provide protocol-agnostic APIs (Application Programming Interfaces) for the protocol framework.
- Provide libraries of the API for the protocol framework defined.

- Design an IC-Agent.
- Implement an IC-Agent software including the main modules.
- Implement the ICI trust architecture and study the technical stakes related to
- scalability.
- Integrate the IC-Agent on different platforms: user station, server, mobile devices
- and Set-Top box.
- Design an extensible dashboard (graphical interface) for the IC-Agent.
- Implement groundbreaking uses cases.
- Provide material for adoption and interoperability testing.
- Contribute to standardization in the respective application fields —within Kantara,
- Oasis group, CEN ISSS, etc.

B.1.2 Progress beyond the state-of-the-art

State of the art

Introduction

The ICI project aims at reusing a large body of existing technical and scientific work to build an identity centric Internet.

To progress beyond the state of art we need a new architectural and protocol framework in order to create a trust architecture for dynamic trust relationship establishments, perform data exchange in an identity centric Internet, and to empower users with the full control of their personal data in such an environment.

As explained in the scientific and technical objectives section, the project includes work on legal issues, a conceptual architecture, a protocol framework, APIs and API implementations, user interfaces and the implementation of use cases. All this work will be the source for further scientific work and technical innovations. We also state that the identity centric Internet will generate new services and usages by a chain of adoption and innovation. In the synthesis of this section we provide more arguments on why the ICI project clearly goes beyond the state of the art.

We then introduce the main outcomes and projects relevant to the ICI project. When necessary we explain how they will be used or how they will be enhanced. We highlight that a number of activities are converging towards an identity centric Internet, but none of them realises the full ambition of the ICI project.

Most relevant related work

"Identity in the cloud" : a seminal report

One of the most significant documents related to our project is surely the report "Identity in the Age of Cloud Computing: The next-generation Internet's impact on business, governance and social interaction" by J.D. Lasica. This document is issued from a roundtable of the ASPEN Institute gathering 28 leaders and experts in Information and Communication Technologies in summer 2008. This work does not deal with architectural and technical considerations. However, it relates the stakes and benefits of an identity centric Internet, from the document sections: Identity Meets the Cloud, New Concepts of Money, Implications for Commerce, Implications for Government and Governing, Implications for Personal Well-being and Conclusion: Market Forces Meet Public Policy.

The synthesis of this study is given by the following sentence taken from the report: "Throughout the sessions personal identity arose as a significant issue. Get it right and many services are enabled and enhanced. The group tended to agree that a user-centric open identity network system is the right approach at this point. It could give everyone the opportunity to manage their own identity, customize it for particular purposes, (i.e., give only so much information to an outsider as is necessary for them to transact with you in the way you need), and make it scalable across the Net. Other ways of looking at it include scaling the social web by allowing the individual to have identity as a kind of service rather than, as Lasica writes, "something done to you by outside interests."

Identity dashboard and user interfaces

Many research and development efforts can be related to the user interface for digital identity management. We here present the most significant related to the idea of a dashboard making users able to monitor their personal data. The dashboard is the subject of the fifth work package of the ICI project. The dashboard design and the dashboard capabilities will strongly depend of the architecture requirements defined in WP2.

Privacy dashboards

Identity Dashboard - http://identitydashboard.com/

Surely the most significant one, Identity dashboard is an online paying service. The service consist in giving a user a unified interface on the distribution of personal data. This is an expected functionality of the ICI dashboard. However, this tool is designed for actual identity and trust architecture. The consequence is that the dashboard only deals with personal data which location is known from the user.

Privacy bird - http://www.privacybird.org

Privacy bird is a Web browser plugin. It is used to display P3P policies of visited Web sites to inform the user about the use of personal data by service providers. This is a basic requirement that will be implemented by the ICI agent and shown to the user by the dashboard.

Privacy dashboard - http://www.privacybird.org/

Privacy dashboard is a Web browser plugin. It is used to grab P3P policies of visited Web sites to inform the user about the personal use made by service providers. This is a basic requirement that will be implemented in the ICI user proxy and the dashboard will inform users.

Google privacy dashboard - https://www.google.com/dashboard

This is an interesting initiative by Google. This dashboard informs Google users about personal data known by Google about them. However, the information displayed is incomplete and only relate what Google knows. With this model each service provider should implement such a dashboard. The user interface would not be unified by default and the information given to users restricted to the information the service provider wants to reveal. The ICI architecture offers to monitor the personal data from the source and not from the receiver point of view. Information will be complete and the dashboard will give a unified view of personal data dissemination.

Facebook privacy dashboard - https://www.google.com/dashboard

This dashboard is in principle similar to Google's. Moreover, the graphical interface provides users with the means to control accesses to their personal data by other member of the social network. As explained before, current social network models do not allow users to have a full control on their personal data. Access control functionalities are thus natively limited. In the ICI architecture, access control will be fully under the user control, not only managed by the service provider.

User tools for identity management over the Web

This section presents a series of components integrated to identity and trust architectures making users able to manage the dissemination of their personal data. All these components provide users with a graphical interface. We give later more detail about the architectures to only focus here on the user interface.

Consent and Attribute Selection Interfaces on identity providers of browser-based identity federations

These architectures have been designed to make possible the propagation of certified personal data between organisations when users are only provided with a standard Web browser (like SAML and WS-Federation specifications). When a service provider expects certified data from a user, it redirects the user's browser on a so-called identity provider able to provide certified personal data. The Identity provider then usually displays to the user a page asking her consent, and eventually make her able to select the identity attributes to reveal. This mechanism is a requirement is cross-organisational personal data exchanges. In the ICI architecture, the IC-Agent allows either the user to obtain and present certified data by herself, or to deliver an authorisation to the service provider. The user is fully in control of these mechanisms through the dashboard, the user interface to the IC-Agent.

The identity provider discovery is a known issue in web-browser based architectures (it is also the case of OpenID-like architectures which does not deal with certified data). When there is a choice between multiple identity providers, users have to indicate their choice to the service provider, something not trivial in large federations. In the ICI architecture, the ICI-agent hosts metadata (containing locations) of all the identity providers of the users —that are other IC-

Agents. It is therefore easier for the dashboard to make a choice. This choice can also be automated.

Cardspace - http://msdn.microsoft.com/en-us/library/aa480189.aspx

Cardspace is the Microsoft implementation of the user component of the Microsoft Identity Metasystem hosted on the user terminal. This architecture relies on the user component to make the user able to retrieve certified personal data and to present them to service providers. This is an important step towards the implementation of an identity-centric architecture. The graphical interface displays to users the relevant sources of data and users are able to select the attributes. Cardspace can store personal data to facilitate the process of form filling with uncertified data.

The main limitations of Cardspace are due to its architecture. We detail them later when dealing with architectures. However we point out here the ones that have the most impact on the user interface. For example, it is not possible to obtain certified data from multiple data certifiers during the same transaction. If a service provider has such a requirement, the user experience is really uncomfortable. The Identity Metasystem does not aim at managing every kind of personal data, the interface is not adapted to manage specific data like the one used in social networks. Finally, Cardspace is not really a dashboard. The functionalities to consult logs and disseminated data is very limited, not to say inexistent.

There is an open source implementation of the user component of Microsoft Identity Metasystem called Higgins. This implementation offers multiple enhancements from the architectural and the user interfaces point of views: the most interesting is the ability to select multiple sources of certified dat. More details are given later in this section.

ISA of the Kantara ULX group - http://kantarainitiative.org/confluence/display/ulx/Charter

According to the work group charter, the ULX (Unique Login eXperience) work focuses on a user interface that best guides a person through the login to a website. However, this work is not limited to login and is extended to user interactions to select sources of personal data, certified or not, and to the policy provided by the service provider to indicate its requirements. The ULX group treats this requirements to match with the policy of personal data providers. The user environment ISA (Identity Selection Agent) is expected to be hosted either by the service provider, the user's terminal or a third party. However, two kinds of ISA are expected: the ones that knows the user and the others.

The ISA is dedicated to user interactions. The group's work only covers a limited scope of the the ICI architecture but it will be a useful reference. Indeed, the IC-Agent is a powerful ISA that knows the user and is hosted independently from the service provider. Then, the work done on the matching between service provider requirements and the personal data providers from the usability point of view will be a task for the ICI project.

FP7 Prime project – works on the user interface

The PrimeLife project is a huge source of seminal works for identity and trust architectures and thus will be a relevant source for the ICI project. Among other topics, the project deals with strong cryptographic schemas for privacy purpose, with policies for privacy and the user interface in a privacy by design identity and trust architecture. Few implementations have been done within the project. The objectives of the project are different from ICI's. No dashboard has been designed and the question of an IC-Agent or similar component has not been addressed.

However, as defined in a project deliverable (d4.1.1) : “PrimeLife has the vision of bringing sustainable and user-controlled Privacy and Identity Management (IDM) to future networks and services. User-controlled Privacy and Identity Management implies that users can make informed choices about the releases of personal data, the selections of credentials for proving personal properties, their privacy and about trust policy settings. For enabling users to make well-informed decisions, user interfaces (UIs) are needed that inform them about the trustworthiness and the privacy policies of their communication partners as well as the implications of personal data releases. These user interfaces should be informative while not being perceived”.

As we share similar goals it is likely that we will be able to reuse some of the Prime's outcomes. Graphical components have been defined and studied with focus groups. For

instance, some icons have been defined (d4.3.1) as shown below, and those may be reused in the dashboard design.

Payment data

Sensitive data

Pseudonymisation

More details are provided on Primelife site in the state of the art section related to architectures.

Paying Online stores

There is a growing number of initiatives offering users online personal hosting for a fee. Their goal is mainly to store digital documents (for instance, “La Poste” or “Air France” personal data stores). However, none of them is accessible by protocols making it feasible for users to share them during digital transactions.

La poste: https://www.digicoffre.com/index.php?m=e2c90ed8&a=1b7541c2

Air France: http://www.airfrance.fr/FR/fr/common/resainfovol/achat/coffre_numerique.htm

We believe that this kind of business, with enhanced functionalities, can play a major role in the adoption of the ICI architecture in order to realise the separation between services and hosting of personal data. There is an opportunity to see the emergence of a new business for hosting IC-Agents.

Such businesses will have to be regulated. The legal and privacy issues will be studied in WP2 and the outcomes of this work will be disseminated to public authorities and legislators.

Identity and Trust Architectures

The ICI identity and trust architecture requirements will be defined in WP2 and the protocol framework will be designed in WP3. However, we can already highlight the main candidates, especially because some standards have recently emerged. Also because we will start from the outcomes of other successful research projects.

Security Assertion Markup Language version 2 (OASIS)

SAML2 is a set of specifications for certified identity exchange between organisations for user equipped with a standard web browser. The privacy is taken into account by a pseudonym system. The user experienced is addressed by a Web SSO. The specification also coins a component for user provided with an enhanced web browser. However, this specification has been enhanced under the specifications ID-WSF described later.

SAML specifications provide a set of namespaces and two of them will be of interest to the ICI project. SAML2 assertion define a namespace for short-life attribute certificates. These documents are well exploited, or at least supported, in many identity and trust architectures. The second interesting namespace is about metadata providers. They allow to define applicative endpoints, that can include public key certificates. They can be used as elementary components to be enhanced, for instance to allow dynamic agreements or to embed any kind of policy.

The protocols defined in SAML2 are mainly defined for web browsers, however they could be employed by the IC-Agent for a single sign-on purpose (SAML SSO profile) or to deliver authorisation (SAML artefact profile).

Another relevant protocol provided by SAML2 specifications is the metadata exchange protocol which could be employed to establish dynamic trust relationship.

There are 4 main open source implementations of SAML2 specifications that are in line with the ICI architecture. Shibboleth, by Internet2, does not implement the whole SAML2 specification but it is widely used in universities across the world. The three other open source

implementations are realised by ICI partners. OpenSSO from ForgeRock (consortium member) is issued from a former code from SUN MicroSystems. OpenSSO provides an implementation of the SAML SP and IDP roles. ZXID by Sampo Kellomaki (Levelview, Associate member) is both an API and implementation of SAML SP and IDP roles. ZXID is certified by the Kantara initiative as conformant to the specifications. Finally, Lasso, by Entrouvert, also provides an open API. This API can be used either in C/C++, Java, PhP, Perl and Python. Entr'ouvert also provides an open source SAML IDP called Authentic. LASSO/Authentic are also certified Conformant by the Kanatara Consortium.

Identity Web Services Framework version 2 (Liberty Alliance)

The specifications ID-WSF2 are closely related to SAML since SAML is partly originated from Liberty Alliance (now Kantara Initiative). IDWSF specifications aim at defining a user controlled authorisation service to web services. A web service consumer will request a web service provider with an authorisation token obtained from the user's identity provider. The latter only delivers such authorisations after user consent.

A second important functionality of ID-WSF is the web service discovery. IDWSF specify protocols for an authority called discovery service which registers services locations.

Both these functionalities are necessary in the ICI architecture and IDWSF is a good candidate for exploitation.

There are only two open source implementations of ID-WSF2.0, ZXID by Sampo Kellomaki and LASSO by Entr'ouvert.

OpenID

OpenID defines a set of implementation to realise a Web SSO. It is not defined to support exchange of attribute certificates. However, it is widely supported. It may then be a good candidate for the authentication protocol with service providers —equivalent to SAML2 Web SSO.

WS-Trust (OASIS)

WS-Trust is a specification which defines a XML namespace for a protocol of attribute certificates retrieval and presentation. The WS-Trust model defines three roles: the certificate issuer, a client and a relying party.

This specification is a standard used in the protocol framework for Cardpace. This protocol is also a good candidate for the ICI architecture, even is not yet widely supported.

Cardspace (formerly InfoCard) / Microsoft Identity metasystem

Both the names Cardspace (formerly InfoCard) and the Microsoft Identity Metasystem are used to name the same protocol framework. In this architecture, the service provider delivers a policy to the user to make the user agent able to determine which personal data the service provider requires. Either the policy is given is an HTTP response. Then, the compliant web browser (IE8 and Firefox 3) detects a specific object in the HTTP header which contains the policy. The bowser triggers a call to the identity client, CardSpace, giving it the policy (or, it gets an applicative endpoint from the HTTP header). Then CardSpace retrieves the policy from this endpoint. The policy is formatted according to the WS-SecurityPolicy XML specifications (OASIS). From the policy, CardSpace infers whether the requirements can be satisfied and then interacts with the user to obtain her consent. Then CardSpace may retrieve with WS-Trust the attribute certificates. Only one attribute certificate can be obtained at a time. Then, CardSpace returns the attribute certificates to the browser. The browser posts it to the service provider in the header of an HTTP request.

This protocol framework covers most of the functionalities required in the ICI architecture. However, the ICI architecture will differ from the CardSpace protocol to go beyont its current limitations.

The first limitation is that CardSpace software must be deployed on the user terminal —hence on all the terminals used by a person... The ICI architecture aims at an IC-Agent in the Cloud, so if retained, Cardspace will have to be moved on the IC-Agent with a user interface accessed from a dumb user terminal.

The second limitation is that CardSpace is limited by the implementation to a unique attribute certificate at a time. To provide a seamless online transactions where many certificates may be required at a time, the IC-Agent and the user interface must be designed for this purpose.

CardSpace offers a generic interface that is not extensible to cover the use cases. We aim at a generic interface with easily pluggable add-ons for specific use cases.

The protocol framework relies on a single name space or protocol per functionality. We aim at providing a protocol-agnostic architecture where we will implement the main protocols with multiples standards. For instance, SAML/IDWSF and WS-Trust for attribute certificates transport, SAML2 SSO and OpenID for the Web SSO.

As CardSpace must be deployed on a user terminal that is not always online, the CardSpace architecture does not allow automatic distribution of personal data at anytime.

CardSpace implementation cannot be considered as a dashboard because the consultation of auditing of personal data diffusion is not addressed.

Higgins

Higgins is an open source implementation of the Microsoft Identity Metasystem protocol framework. It provides also an implementation of the user client. Higgins mainly suffers from the same limitations as CardSpace implementation. However, a prototype of an agent as been created and deployed online with a Web interface. This is an important step towards an IC-Agent. The results of this prototyping will be an interesting source of information for the ICI project.

Being open source, parts of these implementations might be reused in the ICI project.

OAuth

OAuth is the standardisation and combined wisdom of many well established industry protocols. It is similar to other protocols currently in use (Google AuthSub, AOL OpenAuth, Yahoo BBAuth, Upcoming API, Flickr API, Amazon Web Services API, etc). Each protocol provides a proprietary method for exchanging user credentials for an access token or ticker. OAuth was created by carefully studying each of these protocols and extracting the best practices and commonality that will allow new implementations as well as a smooth transition for existing services to support OAuth.

An area where OAuth is more evolved than some other protocols and services is its direct handling of non-website services. OAuth has built in support for desktop applications, mobile devices, set-top boxes, and of course websites. Many of the protocols today use a shared secret hardcoded into the software to communicate, something that might become an issue when the service trying to access one's private data is open source —bye bye shared secret!

UMA Kantara

The work of the UMA Kantara group aims at providing an enhanced mechanism comparable to the IDWSF Discovery service. ICI consortium members are part of the UMA WG and UMA will certainly contribute usefully to the design of the ICI architecture.

Attribute-based Access Control and Access Control on Attributes

The field of access control is of interest from the standard protocol point of view. Indeed, the ICI project has not as objective to provide an access control system, but rather to allow personal data to be taken in so-called Attribute-based access control systems.

XACML (Extensible Access Control Markup Language (OASIS)) is a set of specifications defining a distributed access control architectures, and more specifically an XML based protocol to allow authorisation delegation between a decision point and an enforcement point. This feature may be necessary to standardised some protocol flow of the ICI architecture.

XACML also defines a namespace to create access control policy documents. This name space could be used to define some of the policies employed in the ICI architecture. For the same reason we will also consider the WS-SecurityPolicy namespace.

Privacy considerations

The goal of ICI is to realise a trust-by-design-Internet. Here are some of the technologies relevant to the ICI architecture.

Pseudonymity

As far as pseudonymity the architecture will rely on (one time) pseudonyms to link the different user identities and on user-performed account linking on service providers. The SAML SSO is compliant with this requirement.

Cryptographic attribute certificates

Attribute certificates generated dynamically allow users to obtain certificates only containing the set personal data required by service providers. For instance if the service requires to know the user age, it is not necessary to provide a certificate containing the full date of birth. However, it is not always feasible to deliver dynamically attribute certificates, for instance in spontaneous networks and pervasive environments. This means that the user will obtain multiple-time user certificates, will store them and use then when necessary. It is however still required for a privacy purpose that the user only releases the set of data required by service providers. This can be done relying on certificates generated with specific cryptographic signature scheme (for instance the Camenisch-Lysyanskaya Signature and the Brands Secret Key Signature scheme). It is then feasible to have certificates containing a date of birth and to only prove to be of a certain age when presenting a certificate.

There are open source implementations of such signature schemas, mainly the IBM Idemix and Entr'ouvert Cryptic implementations of the CL-Signature. Microsoft U-Prove is a partly open source implementation of the Brands signature schema. The ICI project will study their integration in a identity centric Internet.

Privacy policies

Privacy policies are used to specify to users how and how long the service providers will store the personal data after a transaction. Assuming that service providers is willing and capable to enforce those policies, this is a useful feature. Enforcing such policies will be facilitated when every service will also be represented in the trust network by an IC-Agent (by design, an IC-Agent contains a policy enforcement point).

They will be integrated in the architecture. The standard for privacy policy is P3P (W3C).

Dynamic trust establishment – Agreement policies

The dynamic trust establishments could become a very complex architecture depending on the parameters taken into account. For the proof of concept, the granularity of the parameters taken into account will be limited.

However, the project aims at defining a (simple) protocol and a policy framework on which will be based the agreements and the thus the trust establishment of decisions. There is significant work done within the Assurance and Governance workgroup of the Kantara Initiative for this purpose.

This workgroup works on the following topics:

- IAF - Identity Assurance Framework (mainly about legal aspects of running a trust network and the admission or intake procedures and vetting)
- IGF - Identity Governance Framework (mainly about management of identity requirements and policy requirements of SPs and Attribute Providers)
- CARML - Declaration of attribute requirements of an SP, and the policies it is willing to support if it gets the attributes.
- AAPML - Declaration of generally available attributes and the policies of an Attribute Provider: what SP has to satisfy to get the attributes.

We will rely on outcomes of this work, such as existing protocols and namespaces to allow policies definition and exchange. As said earlier, we will limit the number of parameters taken into account to establish the trust relationship. For instance, being accepted by a single trusted node of the trust architecture might be enough. Then, specific parameters as the authentication context and the attribute quality may be taken in account.

Domain specific

Social Networks

There are a number of proprietary and open source applications for social networking. They can be classified into 2 main groups:

- centralised social networks: Facebook, renren.com, Elgg, Mahara, etc.
- distributed social networks: DFRN, Appleseed, Turbulences, Diaspora, FOAF+SSL etc.

It is interesting to note that there are few distributed social networks and that they are mostly open source. It is also interesting to note that they do not co-operate and each one is reinventing its idiosyncratic solutions...

DFRN stands for 'Distributed Friends and Relations Network'. DFRN provides the means for people to conduct online social network activities without requiring a central website The basis of DFRN is the DFRN protocol – a definition of social communications amongst inter-related 'cells'. Each cell can make friends with and communicate with other cells in the network. This protocol is built using HTTP and XML – the language of the web. The protocol allows for a rich set of communications to be supported, including most activities that we take for granted on modern social networking sites. It also goes a bit beyond the mundane technical description of the communications flow – to cover what we term "policy decisions" which are critical to the success of any online network.

FOAF+SSL

FOAF+SSL is a secure authentication protocol that enables the building of distributed, open and secure social networks. Foaf+ssl is a very simple protocol. It authenticates a user in one connection, the same connection he makes when accessing a web site. This is because it make clever use of the SSL layer built into virtually every standard Web browser that implements HTTPS. Because of the way foaf+ssl uses certificates, these can be self signed. They can be signed by anybody in fact, it does not matter. So as a result the cost of producing one is insignificant, close to the cost of downloading a random web page. Making one is very easy for the desktop browsers such as Safari, Firefox, and Opera. These browsers support the KEYGEN element, which allows the browser to create a public/private key pair. So the private key never leaves the browser.

SocialOX

SocialOX is a set of features in Open-Xchange to make management of personal information a seamless experience, regardless of how distributed a person's data may be. OXMF (Open-Xchange Meta Format) is inspired by microformats.org and uses HTML to carry semantic markup. Advantages are simplicity, human readability, simple extension. OX version 6.10 is the first release that contains social features, i.e. the first release of SocialOX.

OpenSocial

OpenSocial is a set of common application programming interfaces (APIs) for web-based social network applications, developed by Google along with MySpace and a number of other social networks. Applications implementing the OpenSocial APIs will be interoperable with any social network system that supports them. An open source project, Shindig, was launched in December, 2007, to provide a reference implementation of the OpenSocial standards. It has the support of Google, Ning, and other companies developing OpenSocial-related software.

Data Portability

Data portability is the ability for people to reuse their data across interoperable applications. Historically, the DataPortability Project has been associated with advocating open standards. Formally, the group does not endorse any specific technologies over another - but its leaders have said they support the broader concept of open standards because they help achieve the vision of data portability [7].

There are numerous open standards that are considered to advance the vision, such as RDF, RDFa, micro-formats, APML, FOAF, OAuth, OpenID, OPML, RSS, SIOC, the XHTML Friends Network (XFN), XRI, and XDI.

Employment

There are a number of standards relative to human resources:

- HR-XML - Human Resources XML has developed a set of standards to support the different activities of human resource management, from recruitment to compensation management
- Leap2A - is XML format used to describe the profile of a learner developed in the perspective of ePortfolio interoperability
- Europass CV —an XML format for making CV interoperable in Europe
- Microformat — is a web-based approach to semantic markup which seeks to re-use existing HTML/XHTML tags to convey metadata and other attributes in web pages and other contexts that support (X)HTML, such as RSS. hResume is the micro-format use for CVs

Attempts have been made to connect employment standards with IDM standards, such as ID-WSF (Liberty Alliance) with HR-XML, but one of the limitations of current approaches to existing standards is their lack of granularity, and redundancy (multiple representation of the same set of data) something addressed by the HR-XML consortium in its more recent release of standards (V3), with an idea akin to 'speclets' or mini-specifications.

A general remark on standardisation organisations working on employment standards is that they are oblivious to the issues of identity management, despite the fact that they are dealing with personal data. HR management is still dominated by the vision of centralised systems, for which the need to deal with identity and access management is secondary.

It is interesting to note that there are initiatives at regional and national level to provide workers with some kind of personal data store.

The Dutch Committee on Labour Market Participation has formulated a series of recommendations for getting more people into work in the Netherlands and improving the operation of the labour market. The Committee's most significant conclusion is that the Dutch labour market is about to undergo drastic change, and among the recommendations, the fifth one is related to the ePortfolio (a personal data store) as a means to improve employability:

> "Digital e-portfolio. Every member of the labour force will be entitled to a digital e-portfolio, i.e. an electronic inventory of their competencies, diplomas, experience, and accreditation of prior learning (APL). This will give people a better understanding of their position on the labour market and their career prospects, and of any need they have for further training." (Dutch Committee on Labour Market Participation, 2008)

Healthcare

The Continuity of Care Record standard, often referred to simply as the CCR standard or CCR, is a patient health summary standard, widely used for secure, computable, electronic capture and transfers of personal health data from one health IT system to another, e.g. EHRs or EMRs, and to and from these to personal health record (PHR) applications, such as MedCommons, Google Health and Microsoft HealthVault. The CCR standard utilizes W3C compliant eXtensible Markup Language, XML, to create flexible documents that are intended to contain relevant summary health information about a person for the purposes of coordination of care, continuity of care, and access on networked systems.

> "The vision for the future of health care starts with the premise that consumers should own their own total personal health and wellness data and that only consumers, not insurers, not the government, not employers and not even doctors, but only consumers should have complete control over how it is used," declared Adam Bosworth, Google Vice- President, in a speech to the 2007 AMIA (American Medical Informatics Association) Spring Congress.

For example customers who register for MyRecords at MinuteClinic can securely access their medical information, and also choose to upload their information via the CCR standard to Google Health and/or to Microsoft HealthVault accounts.

There are a number of similar initiatives in Europe like Dossier Médical Partagé (France) and European projects like Smart Personal Health designed to promote awareness and a deeper understanding of the need for interoperability among personal health systems (PHS), devices and other eHealth systems across Europe.

MedCommons (www.medcommons.net), is a pioneer for "personalised healthcare 2.0" that aims at providing citizens with control over their personal health record (PHR) whether created by a physician for their own convenience in telemedicine, by a sponsor such as an insurer or employer to promote consumer control and wellness or directly by a patient. Regardless of how it was created, a MedCommons PHR account can be claimed and controlled by the person who is its subject through a simple address verification procedure.

Education

There are a number of standards used in the world of education that are relevant to ICI. Here are some of them (from different categories):

- Leap2A (mentioned above).
- IMS Global ePortfolio standards, a specification on learner information profile; an ancestor to Leap2A with a life of its own
- Shibboleth, a SAML implementation in the world of higher education institutions — originally libraries.
- OAI-PMH, a protocol for harvesting metadata from learning objects repositories that would be relevant for collecting metadata from ePortfolio repositories —something yet to be done.
- SIF, a school interoperability framework defining exchange protocols between the different service providers of an institution (canteen, transport, library, etc.)

The adoption of ePortfolios is growing in the world of education, but the main obstacle is the issue of interoperability:

- synchronic interoperability: how one person learning in simultaneously in different, disconnected institutions can maintain ePortfolios from a single point
- diachronic interoperability: how can a person keep her learning history when moving from one learning episode to the next

So far, the focus of the educational community has been oblivious to the issue of synchronic interoperability, exploring how standards on data formats could allow the import/export of ePortfolio data from one system to another. The other issue that the ePortfolio community has not been able to resolve is the fact that while ePortfolios are supposed to be *personal*, they are in reality *owned* by the institution.

The ICI project will create the foundations for full synchronic and diachronic interoperability by splitting personal data storage (moving with the person) from the applications feeding/ exploiting personal data storage.

Synthesis

During the previous section we highlighted some works relevant for the ICI architectures and explained why they are relevant. When necessary we explained their limitations or how they may be used to cover a functionality required in the ICI architecture.

From all these works and many other we can state that an identity-centric Internet is not only a trend but a widely shared objective though no project succeeded in setting-up such an architecture:

- No project provides a complete protocol framework for an identity centric internet that we will define in the second and third work packages.
- No project provides a proof of concept of a trust architecture allowing dynamic trust establishment that can be used for business and e-administration purpose that we address in the second and third work packages. .
- No project provides the specifications of the API for a protocol framework though it is a requirement for adoption that we will do in the forth work package. As said before, an API give a unified view of interface, ensure interoperability of implementations and hide the architecture complexity.

- No project provides a set of open source libraries allowing to come into an identity and trust architecture with few efforts that we will do in the forth work package.

All these major component are necessary for a strong adoption. And finally significant progress beyond the state of the art is that our project takes the adoption as a main objective. It explain why we have a stron seventh work package dedicated to adoption. We have also voluntarily oriented our use cases addressed in the sixth work package towards the business and the social networks for two main reasons. Business is seen as a factor of adoption and we see the Identity-centric Internet as a unique worldwide social network. Finally, we have a strong relationship with Kantara which is also a strong factor of dissemination. We also aim to become closer to Identity Commons and the OASIS.

From the technical point of view, there is no project that covers all the functionalities. We propose to solve this issue with a best effort with existing technologies. To accomplish this goal we will especially rely on successful projects as FC², PrimeLife and TAS3. They will be great sources of seminal scientific and technical works and of building blocks.

We aim at building a protocol-agnostic architecture through the API and make it runs through libraries. However new protocols would be de facto integrable.

We also aim at defining a generic user interface extensible with specific interface. The generic interface will include a real dashboard of the digital life. We will design some specific interfaces for the use cases in the fifth work package and we will prove this extensibility in the sixth work package.

To conclude the main progress beyond the state of the art is to prove that it is still time to build by design the future Internet.

B.1.3 S&T Methodology and Work plan

Overall strategy of the work plan

The whole ICI project is geared towards verifying the *feasibility* and *adoptability* of a trust architecture based on the free interaction of individuals and organisations through IC-Agents. The issues of feasibility and adoptability are deeply intertwined as it is always possible to design a 'perfect' architecture that non one will adopt, like a plane that will never crash because it is too heavy to ever take-off. Hence a strong focus on adoptability *within* the projects's time frame, even if the main objective is to inform future research and developments and not to provide a fully operational working solution.

Adoptability will be addressed from two points of view:

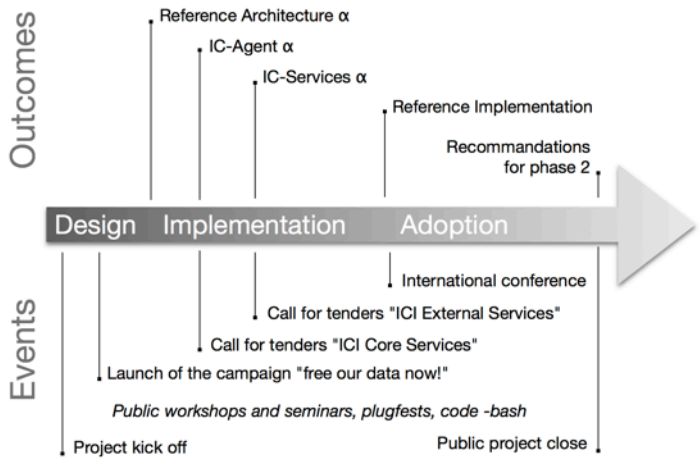
- technical: what makes a architecture and protocols easy to adopt by developers?
- non-technical: what makes a disruptive technology desirable by end users?

In order to be able to collect relevant data within a 24 months project to inform phase 2 of the Internet of the Future platform, activities are organised to rapidly provide the components from which an IC-Agent-based architecture will be boot-strapped and its capacity for adoption tested.

The project is designed along 3 main phases:

- **Design** of an ICI architecture (first elements available M3 and M4)
- **Implementation** of the ICI architecture through prototypes of the trust infrastructure and prototypes of services covering the identified use cases (first implementations M 7 and 8)
- **Adoption** of the architecture (proof of concept) — verification of its *adoptability* through dissemination and call for tenders (first outcomes of the calls M14 & M17)

The development model is highly iterative and interactive, involving the community of developers and service providers to inform, review and exploit the outcomes of the project in order to provide services that will make the ICI architecture attractive to the end user.



The activities are organised in 7 work packages:

- WP1: Coordination
- WP2: ICI architecture requirements (design)
- WP3: Definition of the ICI architecture (design)
- WP4: API specification and implementation
- WP5: Interfaces and dashboard (implementation)
- WP6: Proof of Concept (adoption)
- WP7: Dissemination

As the development of the ICI architecture is highly iterative and interactive, there are close feedback loops between the different work packages: implementation will inform next iteration of design, adoption will inform next iteration of implementation, etc. 10% of the budget is earmarked to associate external partners through a call for tenders that will be launched once the initial conditions for adoption are met: architecture definition and prototypes of its implementation and selected use cases are implemented.

Timing of different WPs (Gantt chart)

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
WP1: Coordinations, ETO																								
T1.1 Project Initiation, meetings, ETO			D1.0		D1.3						D1.3						D1.3						D1.3	
T1.2 Operational project management, ETO	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1	D1.1
T1.3 Project reporting, ETO												D1.2a											D1.4	D1.2b
WP2: The ICI architecture requirements, NOT																								
T2.1 State-of-the-art and legal requirements, NOT			D2.1a			D2.1b																		
T2.2 Use cases report, URC			D2.2a						D2.2b															
T2.3 Technical Architecture Requirements, FRK				D2.3a							D2.3b													
T2.4 Agreement Policies Requirements, NOT				D2.4a							D2.4b													
WP3: ICI Architecture and Protocols, ETO																								
T3.1 Conceptual Architecture, ETO					D3.1a							D3.1b						D3.1c						
T3.2 Specifications of the protocol framework, TBS						D3.2a							D3.2b						D3.2c					
WP4: API specifications and libraries, FRK																								
T4.1 API specification, TBS								D4.1a						D4.1b						D4.1c				
T4.2 API implementation, ETO									D4.2a						D4.2b						D4.2c			
WP5: User Interfaces and dashboard, KYN																								
T5.1 Requirements, UST			D5.1a			D5.1b						D5.1c								D5.1d				
T5.2 Design dashboards on different user terminals, KYN							D5.2a						D5.2b								D5.2c			
T5.3 Testings, TBS									D5.3a						D5.3b									
T5.4 Study of user interfaces in pervasive environments, URC					D5.4a						D5.4b								D5.4c					
WP6: Proof of Concept, TBS																								
T6.1 Prototype a basic IC-Agent, ETO												D6.1a				D6.1b						D6.1c		
T6.2 Prototype use cases, TBS													D6.2/3a				D6.2/3b						D6.2/3c	
T6.3 Coordinate the call for tenders, ETO																				D6.4				
T6.4 Large scale user tests, TBS																		D6.5a						D6.5b
WP7: Dissemination and Adoption, IOS																								
T7.1 Dissemination strategy and implementation IOS	D7.1	D7.3	D7.8		D7.6			D7.6			D7.6					**D7.6**				D7.6			D7.6	
T7.2 Liaisons with Future Internet Core Platform IOS			D7.2			D7.2			D7.2			D7.2			D7.2			D7.2			D7.2		D7.2
T7.3 Stakeholders involvement IOS				D7.4										D7.5a		D7.5b								
T7.4 Plugfests, Code bash FRK											D7.9a					D7.9b								

A larger table with dependencies is provided in the section *Component dependencies*.

Activities are planned in order to provide rapidly the community of developers and service providers with the necessary resources to make the testing of its adoption possible. Timing might seem tight, but it is important to remember that the objective of this call is to inform phase 2, not to provide by itself the final design of the *core platform*...

- **M1-M12**: Initial development stage. During this stage user requirements are collected and exploited to create the first iteration of the ICI framework (WP2 & WP3) that will be used to create a series of prototypes (WP4 & WP5) supporting the chosen use cases (c.f. annex). The goal of this stage is to provide resources that are *developer-friendly,* not necessarily *user-friendly* (this will be for the next phase)
- **M11-M24**: Proof of concept (WP6). During this stage the prototypes created for the IC-Agents and the associated services are made available to the community of developers to create a number of innovative and user-friendly services. One of the main activities will be to coordinate the integration of the outcomes of the call for tenders. This will require close interaction with external developers and end-users. Operational and technical support will be provided and data will be collected from the different stakeholders:
  - **developers**: how easy is it to adopt ICI to create innovative services valuable to end-users?
  - **service providers**: what are the costs/benefits to move towards an ICI architecture?
  - **end-users**: what is the added value of ICI-based services?

At the end of the project, the architecture and protocols will be reviewed in light of the outcomes of the *proof of concept* and the final report will make recommendations for the core platform.

Summary work package list (1.3a)

WP	Title	Type of activity	Leader	Start and end month	Person-months
WP1	Coordination	MGT	ETO	M1-M24	12
WP2	The ICI architecture requirements	RTD	NOT	M1-M12	67
WP3	ICI Architecture and Protocols	RTD	ETO	M4-M24	52
WP4	API specifications, implementations and testing events	RTD	FRK	M4-M21	52
WP5	User Interfaces and dashboard	RTD	KYN	M1-M21	60

WP	Title	Type of activity	Leader	Start and end month	Person-months
WP6	Proof of Concept	RTD	TBS	M11-M24	88
WP7	Dissemination and Adoption	OTHER	IOS	M1-M24	114

Overall list of deliverables (1.3b)

ID	Deliverable name	WP	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D1.0	Initiation report (3 months after the beginning of the project)	1	R	CO	M3
D1.M [1-24]	Monthly minutes of calls and activity summary	1	R	CO	M1-M24
D1.2a	First project report: activity, management and financial reports	1	R	CO	M12
D1.2b	Second project report: activity, management and financial reports .	1	R	CO	M23
D1.3	Project meeting	1	O	PU	M5 M11 M17 M23
D1.4	Final public report	1	R	PU	M24
D2.1	Operating environment	2	R	PU	M3: D2.1a, M6: D2.1b
D2.2	Use cases	2	R	PU	M3: D2.2a, M9: D2.2b
D2.3	Core trust architecture	2	R	PU	M4: D2.3a, M11: D2.3b
D2.4	Agreement policies.	2	R	PU	M4: D2.4a, M11: D2.4b
D3.1	Conceptual Architecture of ICI.	3	P	PU	M5: D3.1a, M12: D3.1b, M18: D3.1c
D3.2	Specification of the protocol framework and credential and policy formats for prototypes.	3	P	PU	M7: D3.2a, M13: D3.2b, M19: D3.2c
D4.1	ICI API definitions, including documentation and tutorials.	4	P	PU	M8: D4.1a, M14: D4.1b, M20: D4.1c
D4.2	ICI API open source implementations.	4	P	PU	M10: D4.2a, M15: D4.2b, M21: D4.2c
D5.1	Interface requirements	5	P	PU	M3: D5.1a, M6: D5.1b, M12: D5.1c, M20: D5.1d
D5.2	Screen displays	5	P	PU	M7: D5.2a, M13: D5.2b, M21: D5.2c
D5.3a	Testing report (phase 1).	5	P	PU	M10
D5.3b	Testings (phase 2).	5	P	PU	M15
D5.4	User interfaces in pervasive environments	5	P	PU	M5: D5.4a, M11: D5.4b, M19: D5.4c
D6.1	Prototype of a generic IC-Agent documentation.	6	P	PU	M12: D6.1a, M16: D6.1b, M22: D6.1c
D6.2	Documentation of integration of the services in the architecture.	6	R	PU	M13: D6.2a, M17: D6.2b, M23: D6.2c
D6.3	Use cases implementation report.	6	P + R	PU	M13: D6.3a, M17: D6.3b, M23: D6.3c
D6.4	Report on adoption by developers and service providers.	6	R	PU	M20
D6.5	Report on the large scale user tests.	6	R	PU	M18: D6.5a, M24: D6.5b
D7.1	Public and internal website	7	D	PU	M1
D7.2	Liaison report with Future Internet Core Platform	7	D	PU	M3, 6, 9, 12, 15, 18, 21, 24
D7.3	Dissemination and Adoption plan	7	D	PU	M2
D7.4	Network of associated partners and developers	7	D	PU	M4

ID	Deliverable name	WP	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D7.5	Call for tenders for IC Core services and IC external services	7	D	PU	M14, M18
D7.6	At least one international conference (M16) and 5 public workshops	7	D	PU	M5 M8 M11 **M16** M20 M23
D7.7	international campaign free our data now!	7	D	PU	M3
D7.8	Plugfests, code bash	7	D	PU	M11, M16

Overall list of milestones (1.3c)

Milestones are control points where decisions are needed with regard to the next stage of the project. For example, a milestone may occur when a major result has been achieved, if its successful attainment is a required for the next phase of work. Another example would be a point when the consortium must decide which of several technologies to adopt for further development.

Show how you will confirm that the milestone has been attained. Refer to indicators if appropriate. For example: a laboratory prototype completed and running flawlessly; software released and validated by a user group; field survey complete and data quality validated.

Ref	Name	Expected date	Work package(s) involved	Means of verification
M1.1	Kick-off meeting	M1	All	Minutes
M1.2	Signature of the consortium agreement	M1	All	Signature of partners
M1.3	Project management board meetings	M5 M11 M17 M23	All	Minutes
M2.1a	(M3) Agreement on operating environment for the use cases in both technical and legal terms.	M3	4, 5, 6	Approval of D2.1a
M2.1b	Agreement on operating environment for the use cases in both technical and legal terms.	M6	4, 5, 6	Approval of D2.1b
M2.2a	Agreement on use cases.	M3	4, 5, 6	Approval of D2.2a
M2.2b	Agreement on use cases.	M9	4, 5, 6	Approval of D2.2b
M2.3a	Project wide Agreement on the specification for the core trust architecture and the IC-Agent.	M4	4, 5, 6	Approval of D2.3a
M2.3b	Project wide Agreement on the specification for the core trust architecture and the IC-Agent.	M11	4, 5, 6	Approval of D2.3b
M2.4a	Project wide Agreement on the requirements for the agreement policies.	M4	4, 5, 6	Approval of D2.4a
M2.4b	Project wide Agreement on the requirements for the agreement policies.	M11	4, 5, 6	Approval of D2.4b
M3.1a	Agreement on architecture.	M5	4, 6	Approval of D3.1a.
M3.1b	Agreement on architecture.	M12	4, 6	Approval of D3.1b.
M3.1c	Agreement on architecture.	M18	4, 6	Approval of D3.1c.
M3.2a	Project wide Agreement on the protocol framework.	M5	4, 6	Approval of D3.2a
M3.2b	Project wide Agreement on the protocol framework.	M13	4, 6	Approval of D3.2b
M3.2c	Project wide Agreement on the protocol framework.	M19	4, 6	Approval of D3.2c
M4.1a	Project wide Agreement on the API definitions.	M8	4, 6	Approval of D4.1a
M4.1b	Project wide Agreement on the API definitions.	M14	4, 6	Approval of D4.1b
M4.1c	Project wide Agreement on the API definitions.	M20	4, 6	Approval of D4.1c

Ref	Name	Expected date	Work package(s) involved	Means of verification
M4.2a	Project wide Agreement on the open source implementations.	M10	4, 6	Approval of D4.2a
M4.2b	Project wide Agreement on the open source implementations.	M15	4, 6	Approval of D4.2b
M4.2c	Project wide Agreement on the open source implementations.	M21	4, 6	Approval of D4.2c
M5.1a	Agreement on generic and specific requirements of the graphical user interface.	M3	6	Approval of D5.1a
M5.1b	Agreement on generic and specific requirements of the graphical user interface.	M6	6	Approval of D5.1b
M5.1c	Agreement on generic and specific requirements of the graphical user interface.	M12	6	Approval of D5.1c
M5.1d	Agreement on generic and specific requirements of the graphical user interface.	M20	6	Approval of D5.1d
M5.2a	Agreement on sets of screen displays of the graphical user interfaces for different devices.	M7	6	Approval of D5.2a
M5.2b	Agreement on sets of screen displays of the graphical user interfaces for different devices.	M13	6	Approval of D5.2b
M5.2c	Agreement on sets of screen displays of the graphical user interfaces for different devices.	M21	6	Approval of D5.2c
M5.3a	Agreement on tests.	M10	6	Approval of D5.3a
M5.3b	Agreement on tests.	M15	6	Approval of D5.3b
M5.4a	Agreement on user interfaces in pervasive environments.	M5	6	Approval of D5.4a
M5.4b	Agreement on user interfaces in pervasive environments.	M11	6	Approval of D5.4b
M5.4c	Agreement on user interfaces in pervasive environments.	M19	6	Approval of D5.4c
M6.2a	Documentation of integration of the services in the architecture.	M12	3, 4	Approval of D6.2a
M6.2b	Documentation of integration of the services in the architecture.	M17	3, 4	Approval of D6.2b
M6.2c	Documentation of integration of the services in the architecture.	M23	3, 5	Approval of D6.2c
M6.3a	Use cases implementation report.	M12	3, 4	Approval of D6.3a
M6.3b	Use cases implementation report.	M17	3, 4	Approval of D6.3b
M6.3c	Use cases implementation report.	M23	3, 5	Approval of D6.3c
M6.4	Report on adoption by developers and service providers.	M20	3, 4	Approval of D6.4
M6.5a	Report on the large scale user tests.	M24	3, 4	Approval of D6.5a
M6.5b	Report on the large scale user tests.	M25	3, 5	Approval of D6.5b
M7.1	Public and private portal ready	M1		Approval of D7.1
M7.2	Dissemination and Adoption plan	M2	WP1	Approval of D7.2
M7.3	Network of associated partners and developers	M5	All	Over 60 associate partners
M7.4	Call for tenders for IC Core services	M11	WP4 WP5 **WP6**	Over 200 responses, 100 valid
M7.5	Call for tenders for IC external services	M14	WP4 WP5 **WP6**	Over 200 responses, 100 valid
M7.6	International conference	M16	All	Over 200 delegates
M7.7	Interoperability events	M11 M16	WP6	At least 40 participants

Ref	Name	Expected date	Work package(s) involved	Means of verification
M7.8	Public adoption	M24	All	1 M IC-Agents created

Work packages (1.3d)

WP1: Coordination

Work package number	1	Start and end	M1-M24
Work package title	Coordination		
Activity type	MGT		

Partner Nº	Partner mnemonic	PM per partner	Contribution Summary
P1	ETO	12	WP leader, T1.1 leader, T1.2 leader, T1.3 leader
P2	IOS	-	-
P3	NOT	-	-
P4	URC	-	-
P5	FRK	-	-
P6	TBS	-	-
P7	UST	-	-
P8	KYN	-	-
P9	KUP	-	

Description of work

Working in close co-operation with WP leaders, the Entr'ouvert team will continuously coordinate and evaluate the progress of the project and take corrective actions as soon as any difficulty is detected.

To provide for an effective management of the whole project in administrative and technical matters, a Project Management Committee will be convened every six months. All project partners will nominate one member of staff from the project consortium to participate in this committee. On an annual basis, a full consortium meeting will be held comprising representatives from each partner.

A Project Kick-Off Meeting will be held at the start of the project involving all project partners to further define and fine-tune the overall project work plan. An internal deliverable will be produced from this meeting, based on individual partners' detailed work plan submissions.

A signed copy of the Consortium Agreement will be provided to the Commission during the contract negotiation process. An additional agreement will be provided for associated organisations that are not core partners of the project, to ensure smooth and open cooperation. This 'charter' for ICI Associate Partners will include a mission statement and make clear how unfunded members can contribute to and benefit from ICI current activities and future direction.

A groupware tool will be established to facilitate coordination and exchange among project partners and associated organisations in coordination with WP7 to ensure smooth transition when private documents are made public for dissemination.

For all project meetings and workshops, the coordinator will prepare input and the framework, and collect, edit and disseminate the outcomes to partners and associated organisations as relevant.

Reporting Mechanisms: Entr'ouvert will be responsible for co-ordinating all management and progress reports and providing these to the Commission. The project co-ordinator will also ensure that summaries of progress on the project are posted on the project web site at least once every three months.

Objectives summary

Ref	Description
Obj1.1	Ensure the delivery of the project on time and on budget.

Ref	Description
Obj1.2	Coordinate the technological and scientific orientation of the project.
Obj1.3	Secure the quality of the work to be undertaken and of the delivered documents and software.
Obj1.4	Management of knowledge.
Obj1.5	Risk management and contingency planning.

Tasks summary

Ref	Start-End	Description
T1.1	M1-M3	Project initiation: The effective initiation of the project involving e.g. kick-off meetings, Quality Plan, Web-site and the Consortium Agreement.
T1.2	M1-M24	Operational project management: The co-ordinating partner will conduct the operational management of the project on a day-to-day basis. Each months the minutes of calls and an activity summary will be reported.
T1.3	M9-M12, M21-M24	Project reporting: The formal project reporting deliverables, including the 6-month progress and financial reports and the final project report. Two project progress reports will be prepared for the commission.

Deliverables summary

ID	Description	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D1.0	Initiation report (3 months after the beginning of the project)	R	CO	M3
D1.M [1-24]	Monthly minutes of calls and activity summary	R	CO	M1-M24
D1.2a	First project report: activity, management and financial reports	R	CO	M12
D1.2b	Second project report: activity, management and financial reports .	R	CO	M23
D1.3	Project meeting	O	PU	M5 M11 M17 M23
D1.4	Final public report	R	PU	M24

Milestones summary

Ref	Name	Expected date	Work package (s) involved	Means of verification
M1.1	Kick-off meeting	M1	All	Minutes
M1.2	Signature of the consortium agreement	M1	All	Signature of partners
M1.3	Project management board meetings	M5 M11 M17 M23	All	Minutes
M1.4	Project collaboration tool	M1	All	Site running

WP2: The ICI architecture requirements

Work package number	2	Start and end	M1-M11
Work package title	ICI architecture requirements		
Activity type	RTD		

Partner Nº	Partner mnemonic	PM per partner	Contribution Summary
P1	ETO	4	T2.3, T2.4
P2	IOS	6	WP board, T2.1, T2.2
P3	NOT	7	WP leader, T2.1 leader, T2.4 leader, T2.2, T2.3
P4	URC	15	WP board, T2.2 leader, T2.1, T2.3, T2.4
P5	FRK	12	T2.3 leader, T2.1, T2.2, T2.4
P6	TBS	8	WP board, T2.1, T2.2, T2.3, T2.4
P7	UST	-	
P8	KYN	7	T2.1, T2.2, T2.3, T2.4
P9	KUP	8	T2.1, T2.2, T2.3, T2.4

Objectives summary

The main objective of WP2 is to conduct a requirements analysis of the state of the art and feed this into use case specifications and the functional requirements of the trust architecture. The requirements driven out of WP2 will be used throughout all technical workpackages in the project to ensure consistency of design and implementation.

Ref	Description
Obj2.1	Create a report on the state of the art. Focus on work from research and standardisation groups such as Kantara along with applied commercial state of the art in the social networking and business integration domains.
Obj2.2	Develop use case specifications specifically designed to expand the current technical horizons detailed by the state of the art report.
Obj2.3	Define usability profiles for the use cases based on target personas.
Obj2.4	Generate a legal requirements report.
Obj2.5	Feed the legal, use case and technical requirements into a specification of the core trust architecture and the IC-Agent. The work in this specification will involve trade off's and compromises in technical approach in order to best accommodate the requirements.

Description of work

The work in WP2 will cover a wide range of focus for the architecture ranging from legal input to user environment needs. It is therefore expected that the work package will suggest trade offs and possible compromises on the design to best accommodate the wide requirements of the project, in particular the means for adoption of the architecture.

D2.1: This report will establish the operating environment for the use cases in both technical and legal terms.

D2.2: This report will describe the use case specifications and how they expand the state of the art. Also this report will contain persona analysis in order to link the use case specification directly with user requirements.

D2.3: This report will propose a specification for the core trust architecture and the IC-Agent based on user consultation, work into the use cases and state of the art report. The report will also be a result of negotiating and trading off specific requirements with the implementation teams in order to create a workable design.

D2.4 This report will propose a specification for the protocols.

Tasks summary

Ref	Start-End	Description
T2.1	M1-M6	State of the art and legal requirements report. This report will establish the operating environment for the use cases in both technical and legal terms.
T2.2	M1-M9	Use cases report. This report will describe the use case specifications and how they expand the state of the art. Also this report will contain persona analysis in order to link the use case specification directly with user requirements.
T2.3	M1-M11	Technical Architecture Requirements. This report will provide the requirements for the core trust architecture and the IC-Agent based on user consultation, work into the use cases and state of the art report. The report will also be a result of negotiating and trading off specific requirements with the implementation teams in order to create a workable design.
T2.4	M1-M11	Agreement Policies Requirements. This report will provide the requirements for the agreement policies, including the related ontologies and matching of namespaces.

Deliverables summary

ID	Description	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D2.1	Operating environment	R	PU	M3: D2.1a, M6: D2.1b
D2.2	Use cases	R	PU	M3: D2.2a, M9: D2.2b
D2.3	Core trust architecture	R	PU	M4: D2.3a, M11: D2.3b
D2.4	Agreement policies.	R	PU	M4: D2.4a, M11: D2.4b

Milestones summary

Ref	Description	Expected date	WP(s) involved	Means of verification
M2.1a	(M3) Agreement on operating environment for the use cases in both technical and legal terms.	M3	4, 5, 6	Approval of D2.1a
M2.1b	Agreement on operating environment for the use cases in both technical and legal terms.	M6	4, 5, 6	Approval of D2.1b
M2.2a	Agreement on use cases.	M3	4, 5, 6	Approval of D2.2a
M2.2b	Agreement on use cases.	M9	4, 5, 6	Approval of D2.2b

Ref	Description	Expected date	WP(s) involved	Means of verification
M2.3a	Project wide Agreement on the specification for the core trust architecture and the IC-Agent.	M4	4, 5, 6	Approval of D2.3a
M2.3b	Project wide Agreement on the specification for the core trust architecture and the IC-Agent.	M11	4, 5, 6	Approval of D2.3b
M2.4a	Project wide Agreement on the requirements for the agreement policies.	M4	4, 5, 6	Approval of D2.4a
M2.4b	Project wide Agreement on the requirements for the agreement policies.	M11	4, 5, 6	Approval of D2.4b

Approval is by email vote or online poll.

WP3: ICI architecture and protocols

Work package number	3	Start and end	M4-M24
Work package title	ICI architecture and protocols		
Activity type	RTD		

Partner Nº	Partner mnemonic	PM per partner	Contribution Summary
P1	ETO	6	WP leader, T3.1 leader, T3.2
P2	IOS	1	T3.1
P3	NOT	6	WP board, T3.1, T3.2
P4	URC	14	T3.1, T3.2
P5	FRK	8	WP board, T3.1, T3.2
P6	TBS	8	T3.2 leader, T3.1
P7	UST	-	
P8	KYN	5	WP board, T3.1, T3.2
P9	KUP	4	T3.1, T3.2

Objectives summary

Ref	Description
Obj3.1	Design an ICI architecture and protocols that is fully trustworthy while being easily adoptable by the community of developers and service providers.
Obj3.2	Design a secure, trustworthy architecture according to the rules identified for an identity centric Internet, e.g. data minimality, symmetry, user empowerment, etc. capable of supporting the defined use cases
Obj3.3	Provide a list of components to be developed and match them with the capacity of each partner and the call for tenders
Obj3.4	Explore different models for adoption of ICI architecture and document the model selected
Obj3.5	Define APIs and libraries
Obj3.6	Align protocol choices with API, while maintaining opportunity to evolve protocols without breaking the API.
Obj3.7	Design a model for trust establishment, facilitation, and introduction.

Description of work

Starting from the outcomes of WP2, prioritise the requirements to take into account in the architecture and protocols according to their feasibility, how critic they are to achieve a truly identity centric Internet. WP3 will rest on state of the art and other projects in same call. WP3 will Support viable commercial and business models in the ecosystem. WP3 will work with WP7 to provide public at large an understanding of the ICI architecture and its relation to other architectures and technologies.

D3.1 Conceptual Architecture of ICI. The conceptual architecture is published early in the project to provide coordination between the partners. It will paint the overall picture, with architecture diagrams, and move to specifics, such as list of components and interfaces, without entering into too low level. It will stay outside the domain of software and deployment architectures. It will discuss trust discovery and policy agreement as well as Peer2Peer relationship establishment. Framework for personal data exchange will be specified. It will present broad choices such as exiting reference architectures and frameworks that will be used as building blocks. It will also discuss the alternatives to these choices and whether the alternatives can be implemented later or were rejected with reason. Relation to other projects and IdM technologies is discussed.

D3.2 First version Specification of the protocol framework and credential and policy formats for prototypes. This specification enumerates the standards, profiles, and bindings to be used, with discussion of alternatives and whether alternatives are implemented later, optionally

implementable, or rejected with reason. Where standards based solution is not found or feasible, this deliverable will specify new protocol or profile as needed. The deliverable will discuss attack vectors, risks, and available protection. If complete protection is not available it will discuss mitigation. It acts as specification and interoperability profile for ICI implementations. It may also act as basis for conformance certification.

Levelview, associated partner will be associated to tasks T3.1, T3.2

All deliverables will be reviewed internally and externally by associated partners.

Tasks summary

Ref	Start-End	Description
T3.1	M4-M24	Architecture consensus seeking and drafting, including face to face workshops and other communications required to bring all players to mutual understanding. In later part of the project this turns to educational mission to evangelize as many developers, businesses, and users as possible about what ICI is.
T3.2	M6-M24	Protocol framework specifications, development and consensus seeking. This activity will liaison tightly with WP2 to follow the core trust architecture and the IC-Agent requirements and the agreement policies requirements. This activity will liaison tightly with WP4 to ensure that the API is in alignment with the protocol framework and that API maintains sufficient genericity to allow evolution in the protocol choices.

Deliverables summary

ID	Description	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D3.1	Conceptual Architecture of ICI.	P	PU	M5: D3.1a, M12: D3.1b, M18: D3.1c
D3.2	Specification of the protocol framework and credential and policy formats for prototypes.	P	PU	M7: D3.2a, M13: D3.2b, M19: D3.2c

Milestones summary

Ref	Description	Expected date	WP(s) involved	Means of verification
M3.1a	Agreement on architecture.	M5	4, 6	Approval of D3.1a.
M3.1b	Agreement on architecture.	M12	4, 6	Approval of D3.1b.
M3.1c	Agreement on architecture.	M18	4, 6	Approval of D3.1c.
M3.2a	Project wide Agreement on the protocol framework.	M5	4, 6	Approval of D3.2a
M3.2b	Project wide Agreement on the protocol framework.	M13	4, 6	Approval of D3.2b
M3.2c	Project wide Agreement on the protocol framework.	M19	4, 6	Approval of D3.2c

WP4: API specifications, implementations

Work package number	4	Start and end	M4-M21
Work package title	API specifications and libraries		
Activity type	RTD		

Partner Nº	Partner mnemonic	PM per partner	Contribution Summary
P1	ETO	15	WP Board T4.2 leader T4.1 T4.2
P2	IOS	-	
P3	NOT	-	
P4	URC	3	T4.1
P5	FRK	15	WP Leader T4.1 T4.2
P6	TBS	14	WP Board T4.1 leader T4.2
P7	UST	-	
P8	KYN	2	WP Board T4.1
P9	KUP	3	T4.1

Objectives summary

Ref	Description
Obj4.1	Converge various current open source implementations to common API framework for implementation of ICI architecture and services.
Obj4.2	Provide a modular API framework that is easily adoptable.
Obj4.3	All specifications compliant APIs are necessarily interoperable. You should not be able to claim to be specifications compliant ICI implementation without being interoperable. This objective is meant to enforce specifications quality: the specifications should be written such that nobody is able to exploit a loophole and claim compliance without actually being interoperable.
Obj4.4	Using at least two independent and interoperable implementations of API framework modules, get API modules standardised on an appropriate forum among Kantara, OASIS, W3C, and IETF.
Obj4.5	Demonstrate concrete interoperability between at least three independent implementations of API framework modules. Interoperability needs to be demonstrated at two layers: (i) wire protocol interoperability, and (ii) API interoperability, exchanging toolkit implementations without changing calling application code. On each layer, at least two implementations need to be interoperable.
Obj4.6	Permit architecture evolution at protocol layer without breaking (high level) API. This implies that the abstractions at API layer are above the state of the art protocols (but the abstractions may be very specific to application domain, more specfic than the generality of protocols would imply).
Obj4.7	Be programming language, development environment, and vendor neutral. Provide conceptually same APIs on multiple environments. This includes at least C/C++, Java Servlet, Java Axis2, C#, Visual Basic, PHP, Perl, Ruby, and Python. It also includes, in the minimum, support for Unix (Linux included) and Windows Server 2000 platforms.
Obj4.8	API is minimally disruptive to existing applications. Ideally it should be "drop in" replacement for existing interfaces with no application change necessary. If change is necessary, it should be at configuration level rather than code level.

Ref	Description
Obj4.9	API addresses at least SSO, SSO to web services bootstrapping, and web service calls, as well as web services provider request validation and response envelope wrapping. The steps should be addressed on basis of holistic solution where data flows from previous step to the next in a natural and easy way, without onerous programmer involvement.
Obj4.10	API addresses service discovery and selection, with opportunity for user interaction in making the choice, trust path discovery, agreement procedure, metadata exchanges and dynamic tust link establishement. (Relative to WP2 and WP3 deliverables)
Obj4.11	API addresses the User Protocol Hub: User data retrieval, User data presentation, User authorisation delivery, User authorisation revocation. (Relative to WP2 and WP3 deliverables)
Obj4.12	API addresses a generic interface between the IC-Agent and and any dashboard. Then, specific profiles are defined for specific purposes, attribute selection, consent, source selection, logs journal consultation, social networking, etc. (To coordinate with the WP5 and WP6 works on User interface and Use cases implementations.)

Description of work

WP4 is responsible for the specifications and implementation of APIs in order for

- **users** (individuals and organisations) to be represented by an IC-Agent
- **service providers** to provide services to end users represented by an IC-Agent

Adoption is also at the heart of WP4 and will be taken into account in the specifications and implementations.

All deliverables will be reviewed internally and externally by associated partners.

Tasks summary

Ref	Start-End	Description
T4.1	M4-M20	Seek consensus and draft APIs. This activity will involve several face to face meetings and other collaborations between relevant developers, first to seek consensus on API, and then to perform preliminary interop. The audience should include both API providers and API users.
T4.2	M9-M21	API implementation.

Deliverables summary

ID	Description	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D4.1	ICI API definitions, including documentation and tutorials.	P	PU	M8: D4.1a, M14: D4.1b, M20: D4.1c
D4.2	ICI API open source implementations.	P	PU	M10: D4.2a, M15: D4.2b, M21: D4.2c

Milestones summary

Ref	Description	Expected date	WP(s) involved	Means of verification
M4.1a	Project wide Agreement on the API definitions.	M8		Approval of D4.1a
M4.1b	Project wide Agreement on the API definitions.	M14		Approval of D4.1b
M4.1c	Project wide Agreement on the API definitions.	M20		Approval of D4.1c
M4.2a	Project wide Agreement on the open source implementations.	M10		Approval of D4.2a
M4.2b	Project wide Agreement on the open source implementations.	M15		Approval of D4.2b
M4.2c	Project wide Agreement on the open source implementations.	M21		Approval of D4.2c

WP5: User Interfaces and dashboard

Work package number	5	Start and end	M1-M21
Work package title	User Interfaces and dashboard		
Activity type	RTD		

Partner Nº	Partner mnemonic	PM per partner	Contribution Summary
P1	ETO	4	T5.1, T5.2
P2	IOS	4	WP board, T5.1, T5.2, T5.3, T5.4
P3	NOT	3	T5.1, T5.2
P4	URC	14	WP board, T5.4 leader, T5.1, T5.2, T5.3
P5	FRK	-	
P6	TBS	-	
P7	UST	24	WP board, T5.1 leader, T5.3 leader, T5.2, T5.3, T5.4
P8	KYN	10	WP leader, T5.2 leader, T5.1, T5.3, T5.4
P9	KUP		

Objectives summary

Ref	Description
Obj5.1	Provide generic and specific (to use cases) requirements on dashboards.
Obj5.2	Provide an API between the dashboard and the IC-Agent, tasks done assigned in the WP4.
Obj5.3	Design graphical user interfaces be designed for lap-top with mouse and keyboard, smart phone with a touch pad and a TV screen with a standard remote control (directional pad, and few validation buttons).
Obj5.4	User adoption of the interface designed.
Obj5.5	Anticipate on user interfaces in pervasive environments and on the impact for the control of the IC-Agent.

Work description

The work of WP5 is focused on the user-interface, in particular the design of a dashboard that a person will be able to use to control his/her data from multiple devices: mobile and smart phones, computers, televisions connected to set-top boxes (a potential candidate for hosting family IC-Agents), etc.

D5.1 Report on generic and specific requirements of the graphical user interface to interact with the IC-Agent according to the requirements defined in WP2.

D5.2 Sets of screen displays of the graphical user interfaces for different devices, at least, lap-top with mouse and keyboard, smart phone with a touch pad and a TV screen with a standard remote control (directional pad, and few validation buttons).

D5.3a Testings report on predefined scenario based on the user interfaces designed on a small set of users (phase 1).

D5.3b Testings report on predefined scenario based on the user interfaces designed on a small set of users (phase 2).

D5.4 Study on user interfaces in pervasive environments and anticipate on the control of the IC-Agent.

Tasks summary

Ref	Start-End	Description
T5.1	M1-M20	Define generic requirements of the graphical user interface to interact with the IC-Agent according to the requirements defined in WP2: Take decisions, configure access control on personal data, consult logs, etc. Define application specific requirements of the graphical user interface according to the use cases defined in WP2.
T5.2	M4-M21	Design the graphical user interfaces for different devices, at least, lap-top with mouse and keyboard, smart phone with a touch pad and a TV screen with a standard remote control (directional pad, and few validation buttons).
T5.3a	M8-M10	Tests phase 1 on predefined scenario based on the user interfaces designed on a small set of users.
T5.3b	M14-M15	Tests phase 2 on predefined scenario based on the user interfaces designed on a small set of users.
T5.4	M1-M19	Study of user interfaces in pervasive environments.

Deliverables summary

ID	Description	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D5.1	Interface requirements	P	PU	M3: D5.1a, M6: D5.1b, M12: D5.1c, M20: D5.1d
D5.2	Screen displays	P	PU	M7: D5.2a, M13: D5.2b, M21: D5.2c
D5.3a	Testing report (phase 1)	P	PU	M10
D5.3b	Testings (phase 2)	P	PU	M15
D5.4	User interfaces in pervasive environments	P	PU	M5: D5.4a, M11: D5.4b, M19: D5.4c

Milestones summary

Ref	Description	Expec. date	WP(s) involved	Means of verification
M5.1a	Agreement on generic and specific requirements of the graphical user interface.	M3	6	Approval of D5.1a
M5.1b	Agreement on generic and specific requirements of the graphical user interface.	M6	6	Approval of D5.1b
M5.1c	Agreement on generic and specific requirements of the graphical user interface.	M12	6	Approval of D5.1c

M5.1d	Agreement on generic and specific requirements of the graphical user interface.	M20	6	Approval of D5.1d
M5.2a	Agreement on sets of screen displays of the graphical user interfaces for different devices.	M7	6	Approval of D5.2a
M5.2b	Agreement on sets of screen displays of the graphical user interfaces for different devices.	M13	6	Approval of D5.2b
M5.2c	Agreement on sets of screen displays of the graphical user interfaces for different devices.	M21	6	Approval of D5.2c
M5.3a	Agreement on tests.	M10	6	Approval of D5.3a
M5.3b	Agreement on tests.	M15	6	Approval of D5.3b
M5.4a	Agreement on user interfaces in pervasive environments.	M5	6	Approval of D5.4a
M5.4b	Agreement on user interfaces in pervasive environments.	M11	6	Approval of D5.4b
M5.4c	Agreement on user interfaces in pervasive environments.	M19	6	Approval of D5.4c

WP6: Proof of Concept

Work package number	6	Start and end	M11-M24
Work package title	Proof of Concept		
Activity type	RTD		

Partner Nº	Partner mnemonic	PM per partner	Contribution Summary
P1	ETO	18	WP board, T6.1 leader, T6.3 leader, T6.2
P2	IOS	6	WP board, T6.1, T6.2, T6.3, T6.4
P3	NOT	6	T6.1, T6.2, T6.3, T6.4
P4	URC	11	T6.1, T6.2, T6.3, T6.4
P5	FRK	5	T6.1, T6.2, T6.3
P6	TBS	20	WP leader, T6.2 leader, T6.4 leader, T6.1, T6.4
P7	UST	7	T6.4
P8	KYN	13	WP board, T6.1, T6.2, T6.3, T6.4
P9	KUP		

Objectives summary

Ref	Description
Obj6.1	Prove the concept of an Identity-Centric architecture is feasible and adopted by a wide range of stakeholders.
Obj6.2	Coordinate the work of the associate parties selected from the call for tenders.
Obj6.3	Implement the use cases defined
Obj6.4	Demonstrate the feasibility of new use cases
Obj6.5	Give the identity and trust architecture basis for phase 2 of the future Internet definition.

Description of work

The proof of concept must ask the views on the ratio costs/benefits of adoption to three different groups:

1. **Developers and innovators**: how easy is it to exploit the ICI architecture to create innovative services?
2. **Service providers**: how easy is it to adopt the ICI architecture with existing services?
3. **Citizens and users**: how user friendly the ICI architecture is?

For that, WP6 will implement the use defined cases by using the outcomes of WP 4 and WP5 and coordinate the call for tenders that is used to demonstrate:

1. the interest for the architecture
2. the degree of easiness of adoption

Tasks summary

Ref	Start-End	Description
T6.1	M11-M22	Prototype a generic IC-Agent.

T6.2	M11-M23	Prototype the services based on the defined use cases.
T6.3	M14-M22	Coordinate the work and outcomes of the associate parties selected from the call for tenders.
T6.4	M14-M24	Realise large scale user tests.

Deliverables summary

ID	Description	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D6.1	Prototype of a generic IC-Agent documentation.	P	PU	M12: D6.1a, M16: D6.1b, M22: D6.1c
D6.2	Documentation of integration of the services in the architecture.	R	PU	M13: D6.2a, M17: D6.2b, M23: D6.2c
D6.3	Use cases implementation report.	P + R	PU	M13: D6.3a, M17: D6.3b, M23: D6.3c
D6.4	Report on adoption by developers and service providers.	R	PU	M20
D6.5	Report on the large scale user tests.	R	PU	M18: D6.5a, M24: D6.5b

Milestones summary

Ref	Description	Expected date	WP(s) involved	Means of verification
M6.2a	Documentation of integration of the services in the architecture.	M12	3, 4	Approval of D6.2a
M6.2b	Documentation of integration of the services in the architecture.	M17	3, 4	Approval of D6.2b
M6.2c	Documentation of integration of the services in the architecture.	M23	3, 5	Approval of D6.2c
M6.3a	Use cases implementation report.	M12	3, 4	Approval of D6.3a
M6.3b	Use cases implementation report.	M17	3, 4	Approval of D6.3b
M6.3c	Use cases implementation report.	M23	3, 5	Approval of D6.3c
M6.4	Report on adoption by developers and service providers.	M20	3, 4	Approval of D6.4
M6.5a	Report on the large scale user tests.	M24	3, 4	Approval of D6.5a
M6.5b	Report on the large scale user tests.	M25	3, 5	Approval of D6.5b

WP7: Dissemination and adoption

Work package number	7	Start and end	M1-M24
Work package title	Dissemination and adoption		
Activity type	RTD		

Partner Nº	Partner mnemonic	PM per partner	Contribution Summary
P1	ETO	7	WP Board, T7.1, T7.2, T7.3, T7.4
P2	IOS	43	WP Leader T7.1, Leader T7.2, T7.3
P3	NOT	4	WP Board, T7.1, T7.3
P4	URC	13	T7.1, T7.3, T7.4
P5	FRK	9	Leader T7.4, T7.1, T7.3
P6	TBS	10	T7.1, T7.3, T7.4
P7	UST	8	T7.1, T7.3
P8	KYN	5	T7.1, T7.3
P9	KUP	19	WP Board, Leader T7.3

Objectives summary

Ref	Description
Obj7.1	Raise awareness of the different stakeholders that can contribute to the achievements of the ICI goals —free our data now! will be one of the main communication vectors
Obj7.2	Build the different communities leading to adoption —recruit associate partners willing to take an active role in the design and implementation of the ICI architecture; two call for tenders will be issued to invite them to collaborate actively
Obj7.3	Establish and maintain contact with the other partners of the Future Internet Core Platform

Description of work

The role of WP7 is not simply to *disseminate* the outcomes of the project, but to create the awareness necessary for developers and service providers to adopt the ICI architecture (the other WP address adoption by removing technical barriers).

WP7 main task will be the creation of the adoption community by publicising ICI (public web site, project brochures, newsletters and marketing materials) and creating an active online community.

One central element for building this community will be the campaign "*free our data now*" a message that can be heard by non-technical as well as technical people. The second element will be the call for tenders inviting the community of service providers and developers to adopt the ICI architecture.

A number of events will also be organised to build the community: international workshops and at least one international conference (in partnership with the European Identity Conference organised by Kuppinger Cole), and when possible workshops will be co-located with existing relevant events.

The apex of WP7 will be the call for tenders, aimed at funding small developments contributing to the architecture and service provision.

Tasks summary

Ref	Start-End	Description
T7.1	M1-M24	Dissemination of project goals and outcomes: public and private (project partners and associate partners) portal, attendance at conferences, organisation of an international conference, organisation of public workshops, mailing lists, wikis, chat rooms, public forums, etc.
T7.2	M1-M24	Liaison with Future Internet Core Platform, Kantara, TAS3, Primelife, and other EC funded research projects; conferences, white papers, and other dissemination activities.
T7.3	M2-M24	Organisation of the associate partners communities: developers, service providers, user representatives, etc. One main element will be the call for tenders to demonstrate the 'adoptability' characteristics of ICI.
T7.4	M13-M14	Organize interoperability event to test API compatibility of various implementations. At least implementations by consortium members will participate, but the events are open even to outside implementations. Should an event become oversubscribed, the WP4 leader will choose relevant participants on merit and not consortium membership, justifying his decisions in writing.

Deliverables summary

ID	Description	Nature (RPDO)	Diss level (PU PP RE CO)	Delivery date (month n°)
D7.1	Public and internal website	D	PU	M1
D7.2	Liaison report with Future Internet Core Platform	D	PU	M3, 6, 9, 12, 15, 18, 21, 24
D7.3	Dissemination and Adoption plan	D	PU	M2
D7.4	Network of associated partners and developers	D	PU	M4
D7.5	Call for tenders for IC Core services and IC external services	D	PU	M14, M18
D7.6	At least one **international conference** (M16 ±3) and 5 public workshops	D	PU	M5 M8 M11 **M16** M20 M23
D7.7	international campaign free our data now!	D	PU	M3
D7.8	Plugfests, code bash	D	PU	M11, M16

Milestones Summary

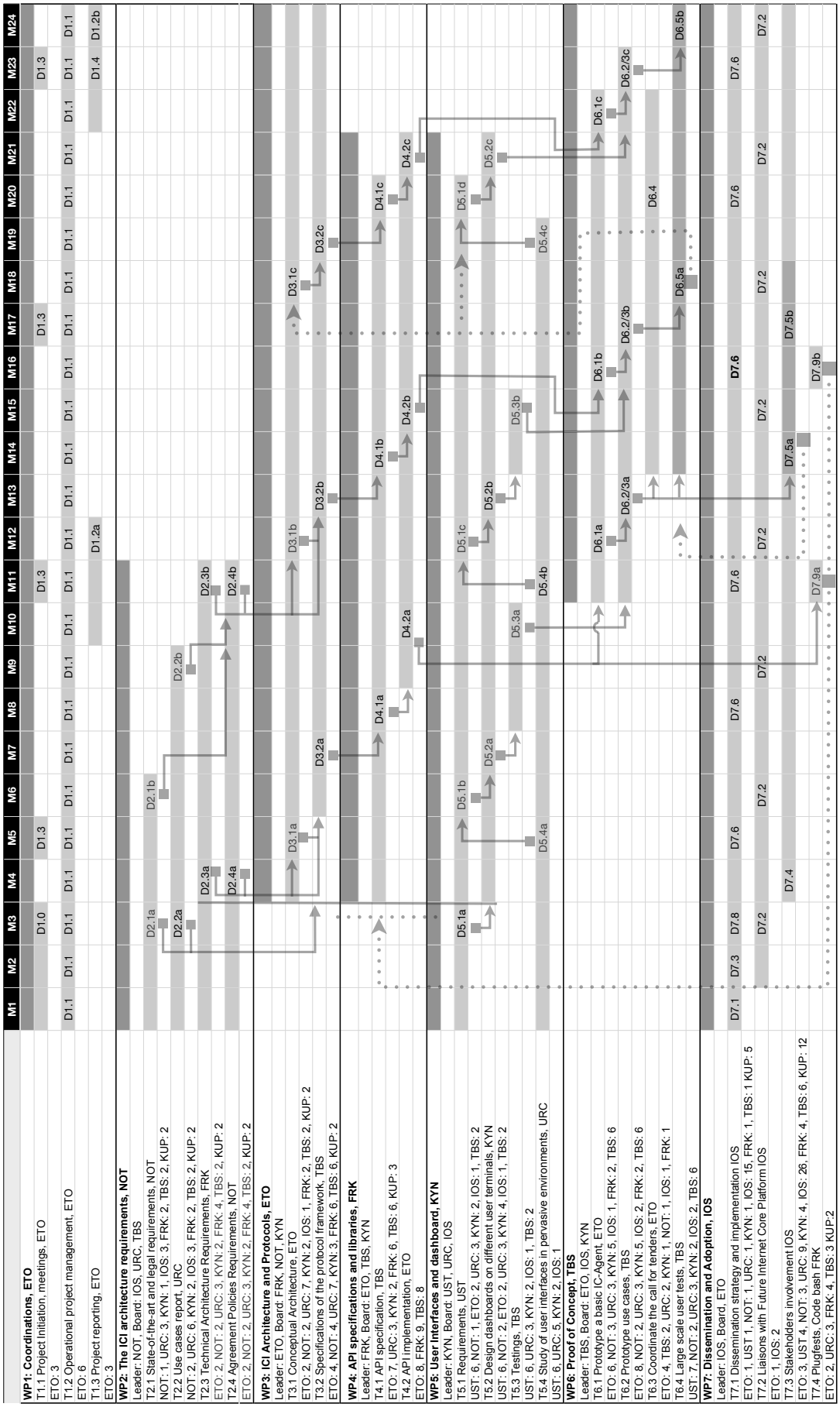
Ref	Description	Expected date	WP(s) involved	Means of verification
M7.1	Public and private portal ready	M1		Approval of D7.1

Ref	Description	Expected date	WP(s) involved	Means of verification
M7.2	Dissemination and Adoption plan	M2	WP1	Approval of D7.2
M7.3	Network of associated partners and developers	M5	All	Over 60 associate partners
M7.4	Call for tenders for IC Core services	M11	WP4 WP5 **WP6**	Over 200 responses, 100 valid
M7.5	Call for tenders for IC external services	M14	WP4 WP5 **WP6**	Over 200 responses, 100 valid
M7.6	International conference	M16	All	Over 200 delegates
M7.7	Interoperability events	M11 M16	WP6	At least 40 participants
M7.8	Public adoption	M24	All	1 M IC-Agents created

Summary of effort table (1.3e)

Partner n°	Short name	WP1	WP2	WP3	WP4	WP5	WP6	WP7	Total person months
1	ETO	12	4	6	15	4	18	7	**66**
2	IOS	0	6	1	0	4	6	43	**60**
3	NOT	0	7	6	0	3	8	4	**28**
4	URC	0	15	14	3	15	11	13	**71**
5	FRK	0	12	8	15	0	5	8	**48**
6	TBS	0	8	8	14		20	10	**60**
7	UST	0	0	0	0	24	7	5	**36**
8	KYN	0	7	5	2	10	13	5	**42**
9	KUP	0	8	4	3	0	0	19	**34**
	Total	**12**	**67**	**52**	**52**	**60**	**88**	**114**	**445**

Component dependencies (Pert diagram)



Risks assessment and contingency plans

While there are risks associated with any project (e.g. partner drop out) , projects dealing with personal data carry additional risks. Even the IC-Agent, while supposed to increase privacy could become a threat if hacked by a malicious software. It is therefore important to take into consideration predictable as well as unpredictable risks.

So the broad questions to consider are:

- What are the risks the project can generate?
- What are the risks within the project's control?
- What are the risks beyond the project's control?
- What actions can the project take to mitigate these risks?

A section in the Ethical section deals with *How will ICI ensure data protection & confidentiality?*

There follows a number of risk cases along with reasoning as to their likely impact and how they could be addressed or countered.

- **Lack of readiness of end users**: managing one's personal data could be ignored by users as they are satisfied with the current trade-off with service providers managing their personal data. They might not accept an additional responsibility, not worth their commitment for the expected outcomes.
- **Lack of readiness of service providers**: as the P3P experience demonstrate, it is not enough to have a good standard. In order to succeed, there needs to be incentives for service providers — carrot and/or stick.
- **Hacking of IC-Agent**: if a person, from a single point, can have access to all of his/her personal data, how can we make sure that someone else won't be able to steal or fabricate the attributes required to spoof the system? While the fragmentation of personal data is counterproductive for the individual, in a sense it reduces the risks of hacking all of one's data in a single move. ICI offers *distribution* as alternative to *fragmentation*.
- **Fragmentation of personal dashboards**: with the emergence of a number of frameworks for identity and access management, we might see the emergence of multiple dashboards, each adapted to its own system (SAML, OpenID, FaceBook, Google, etc.). With the ICI infrastructure, it should be possible to provide a unified framework, independently from the chosen identity and access management model.
- **Hacking ICI infrastructure**: as any infrastructure, one based on the ICI architecture will be subject to attacks. Preventing measures such as Intrusion Detection Systems (IDS), content filtering software and behaviour analysis software will be implemented. Moreover, with the ICI architecture we will be able to explore how social networks can contribute to damage limitation when under hacker attacks.
- **Emergence of disruptive technology.** Technology providers will always differentiate themselves with added features and innovations in their products. The Challenge for ICI is to have a framework that is flexible enough to effortlessly include those new and emerging features.
- **Market domination by a single (or limited number of) industry leader**: this is already the case. Data services should follow the model given by utility and railways: the requirement to split infrastructure from services. ICI creates the condition for the the emergence of an infrastrcuture with a clear separation between personal data hosting and service provision. This will be beneficial for business and privacy protection.
- **Service providers remain predominant hosts of personal data**: this is a probable scenario when taking into account the dominant position of some of the actors. Nevertheless, the lessons learnt from the Internet and innovation in general is that what happens is more than often the unexpected.

Summary of risks assessment and contingency plan

Risk	Probability	Impact	Contingency Plan
Drop out of key technical partner	Low	High	Replace the partner, reassign work or refocus the project on achievable goals
Drop out of a non-technical partner	Low	Medium	Replace the partner, reassign work or refocus the project on achievable goals
Disagreement between partners on the exploitation	Low	Low	It is clear, from the pre-project negotiation that all the partners agree that the ICI architecture will be open and royalty-free, while the services exploiting the ICI-based infrastructure could be free or commercial
Major technical problem	Low	High	Refocus the project on a different path
New standard or specification	Low	Low/ High	The partners belong to the different communities that are in charge of developing new standards, but there is the risk of an emerging de facto standard that the project will have to take into account
Difficulty with recruiting Associate Partners	Medium	Medium	There are sufficient resources within the partnership, esp. through the Kantara Initiative to have enough candidates for reviewing and testing the architecture
Emergence of disruptive technology	Medium	High	The project goals should be reassessed to include this disruptive technology, just as it will be reassessed on the basis of developers, service providers and users feedback.
Lack of adoption by end users and/or service providers —innovative projects are prone to fail...	Medium	Low	Impact is assessed as low because the lessons learned from the response to the call for tenders and the implementation of the scenarios will be available to be used to explore other paths for the Internet of the Future after the project completion.

As stated in other parts of the proposal, ICI is an innovative project and, as such, it is risky and prone to fail to achieve some of its objectives. There is one objective that we are less likely to fail, even if everything else fails, it is the ability to provide enough data to inform those who will be involved in phase 2 of the call.

Part B Section 2. Implementation

B.2.1 Management structure and procedures

Describe the organisational structure and decision-making mechanisms of the project. Show how they are matched to the complexity and scale of the project. (Maximum length for Section 2.1 - five pages)

Summary

The consortium is organised by contractual agreement between consortium partners. Ultimate power in the consortium rests with the General Assembly which can deliberate on all matters by simple majority, except to alter the consortium agreement which requires 2/3 majority. Each partner has one vote in the General Assembly. Partners voting against a change of consortium agreement may leave the consortium without penalty and with their accrued rights intact.

The executive powers are vested in the coordinator, who shall name a person to exercise the function. Should the coordinator not perform, General Assembly can change the coordinator by simple majority. The coordinator signs the name of the consortium. Until decision to the contrary, Entr'ouvert is designated as coordinator with Mikaël Ates exercising the function.

Technical decisions, such as approval of architecture and API, are made by Technical Architecture Board (TAB). Should it become necessary, the architecture board can be altered by simple majority of the General Assembly.

Technical issues are decided by the TAB with simple majority, chair's vote breaking tie. A simple majority in the GA can reverse a TAB's decision. Money and project management issues are decided by the coordinator, and if a partner disagree, he can turn to the GA. If a partner is nonperforming, he can be expelled by the consortium by 2/3 majority in GA.

Quality assurance of the deliverables will be provided by internal, and if necessary external, peer reviews.

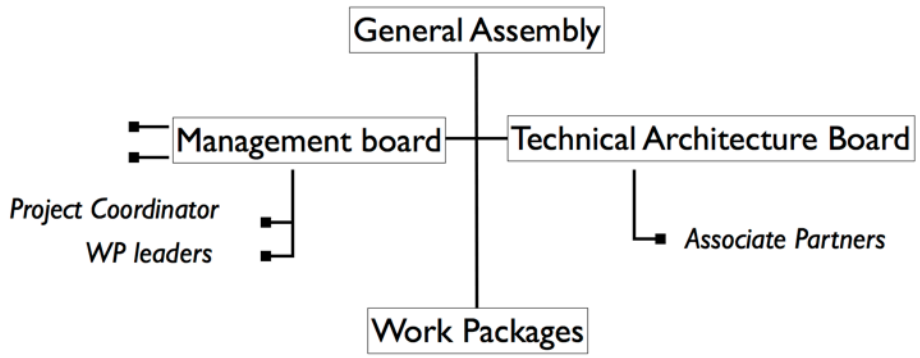
Management structure

This is an ambitious project requiring the involvement of a large number of partners throughout Europe. The management structure is organised in order to reduce administrative costs and travel expenses and ensure an efficient management of resources and decision-making.

In order to keep the project manageable, the partners are organised in two groups:

- Contractual Partners: a core of partners in charge of the overall project management; they are the work package leaders
- Associated Partners: organisations who are not contractual partners, but who will benefit from the support of the Contractual Partners, the Kantara Initiative and Levelview initially

The overall project will be administered by Entr'ouvert, which will provide the support services (web site, community service, website, newsletter, etc.). The project contractor will work using recognised standards for project management which have allowed them to deliver the outcomes of numerous projects, often involving stakeholders with diverse interests, on time, within budget and to the quality required.



The governance of the project is ensured by:

- **General Assembly** where all partners are represented
- **Management Board** where all the work package leaders and the coordinator are represented
- **Technical Architecture Board** where associate partners are invited to review and contribute to the technical architecture
- **Work packages** boards and leaders that are responsible for the production of deliverables

General Assembly

The general assembly is the main governing body of the project consortium. It is chaired by the project coordinator or a person nominated by the project coordinator. Partner representatives must be in a capacity to make decisions on behalf of their organisations.

It is responsible for strategic decisions, such as project modifications, whenever required.

The General Assembly will meet at least three times in the course of the project.

Project Coordinator

Entr'ouvert, the project coordinator and communication channel with the European Commission, will be responsible for the day to day implementation of the workplan.

The responsibilities of the project coordination are:

- Comply with legal, contractual, ethical, financial, quality assurance and administrative duties
- Create the conditions for achieving the project objectives and encourage good spirit and good working relationships
- Monitor progress and take appropriate measures when a gap is noticed
- Establish good relationships with the Commission, external partners and associate projects

The Project Coordinator will ensure that ICI is carried out using the highest standards and procedures of work. It will be in particular responsible for implementing quality monitoring.

Management Board

The Management Board is constituted of the 7 work package leaders with the project coordinator. It is responsible for coordinating the different activities of the work packages.

In particular the Management Board will:

- monitor, review and assess activities progress to ensure that the project is on track and on schedule

- review the plan if necessary
- review and accept key project deliverables before submission to the Commission
- deal with unresolved technical and administrative issues

Technical Architecture Board (TAB)

The technical architecture board will be responsible for the overall architecture of the project. It is a leadership role.

In particular the Management Board will:

- manage the integration and consistency of the project's components
- invite external experts to review project's overall architecture and deliverables
- liaise with relevant standardisation bodies, such as the Kantara Initiative, CEN ISSS

Initially the architecture board shall consist of Mikaël Ates (chair), Sampo Kellomäki (vice-chair), Fulup Ar Foll, Lasse Andersen, and Serge Ravet (3 partners and 2 associate partners).

Management issues and procedures

Monitoring progress is a critical element for the success of a project. Il will be performed at different levels:

- Every 2 weeks, by the management board
- Monthly, by the partners
- Every semester by the coordinator

Minute report: each partner fills-in online a simplified monthly report describing

1. the efforts spend per work package
2. what has been achieved
3. what problems were encountered, if any (e.g. delays) and how they were addressed
4. next month's plan

Such report should be filled-in in less that 15 minutes, and will provide valuable information to the coordinator and the partners working in other work packages.

Semester report: the Project Coordinator will organise a series of structured interviews with the WP leaders to prepare a report indicating:

- what has been achieved?
- what problems were encountered?
    - how were they addressed/corrected?
    - what impact on the future of the project?
        - Conceptual/scientific?
        - technical/implementation?
- what recommendations for the continuation of the project?

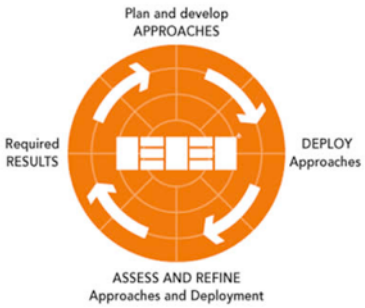
The interviews will be prepared by reviewing the monthly 'minute reports' filled-in by the partners. The coordinator will report the findings by providing information on:

- Deliverables produced vs what was planned to be achieved
- Use of resources against plans
- Impact of the project, awareness and adoption

Quality assurance

The reference model used by the project for quality assurance is the EFQM model which is more adapted to agile projects than the (too) often bureaucratic ISO 9000 model. The EFQM's RADAR Logic is a dynamic assessment framework and powerful management tool that provides a structured approach to questioning the performance of an organisation. At the highest level RADAR logic states that an organisation needs to:

- Determine the Results it is aiming to achieve as part of its strategy
- Plan and Develop an integrated set of sound Approaches to deliver the required results both now and in the future
- Deploy the approaches in a systematic way to ensure implementation
- Assess and Refine the deployed approaches based on monitoring and analysis of the results achieved and ongoing learning activities



For the ICI projects

- Results: a trust architecture easily adoptable
- Plan: a series of prototypes implementing the architecture
- Deploy: engage the community at large through call for tenders
- Assess: review the plan implementation and its outcomes

Management of knowledge

Knowledge management will be an important part of the project, internally and externally. All new knowledge produced in the course of the project will be uploaded on the project portal to be shared, reviewed and exploited by the partners and associated partners.

(for foreground and background IPR, see section "IPR")

The project portal will allow external parties to have restricted access in order, for example, to review a document or a deliverable.

ICI will minimise the use of sending multiple files as attachments to emails and encourage the use of wikis and equivalent technologies.

Once ready for publication, the deliverables will be granted public access.

Meetings

The project will be launched by a Consortium plenary Kick-off meeting and closed by another plenary meeting. A number of meeting have been planed for the consortium. Additional work meetings will be organised by the work packages as needed.

The Management Board and Technical Architecture Board will meet regularly, in relation to consortium meetings and independently.

Risk management

A number of risks have been identified in the section "Risks assessment and contingency plans." Risks will be monitored through constant project monitoring. Depending on the potential damage and capacity to find a solution, it will be managed at:

- WP level
- Management Board level
- General Assembly level

The Risk & Contingency Plan matrix defined in this document will be reviewed in light of developments within and outside of the project. Data collected during project monitoring will provide a basis for identifying emerging risks and reduce potential threats.

Co-operation, communication and conflict resolution

Co-operation and communication

The Project team and Work Package Leaders will confer fortnightly to review progress, issues and forthcoming tasks.

Partners will report formally on a monthly basis on work package progress, work package links, work and cost inputs.

The project manager will submit a report for review with the project officer, at agreed interval, to ensure good communication and identify and resolve issues between formal project reviews. This will cover progress, work and costs against plan together with dissemination, exploitation, IPR and other aspects of external engagement.

Partners will meet quarterly for formal review, co-located wherever possible with dissemination seminars and workshops and/or with relevant meetings and conferences.

A quarterly report will be circulated to Partners, followed by a review of progress against contractual obligations with the Co-ordinating Partner responsible.

A mid-project review will be held with the Project Officer at intervals to be agreed.

Resolution of conflicts

The procedures defined above are designed to minimise the chances of conflicts arising. Nevertheless, should such problems occur, the first step towards resolution would be for the Project Coordinator to discuss the problem with the involved parties in order to seek amicable settlement. If the lead partner is one of the parties involved then another member of the General Assembly will take on the role of facilitator and arbitrator. If a resolution is not achieved, then a majority vote of the General Assembly will decide the issue.

In case of non-performance of a partner, the General Assembly shall have the power to exclude the offending partner by a vote of unanimity minus one. In such circumstances the provisions of the Grant Agreement guidelines will apply as well as relevant non-conflicting provisions made in the Consortium Agreement.

Project monitoring and assessment

To facilitate communication and monitoring of activities within the ICI consortium, different procedures and tools will be established at the beginning of the activity:

- Tools for service co-ordination and communication among the ICI partners
- Tools for monitoring ICI services usage
- Analysis of Web usage statistics
- Inclusion of conclusions and recommendations in periodic reporting
- Procedure and tools for reporting
- Monthly internal activity reporting from ICI Contractual Partners
- Quaterly report to the European Commission
- Periodic activity reports on the progress of the different work packages

Working languages

The working language for the management of the project will be English.

B.2.2 Individual participants

Summary of the consortium

	Short name	Full Name		Type	People	Contribution
P1	ETO	Entr'ouvert	FR	SME	Mikaël Ates, Pierre Cros, Frédéric Péters, Benjamin Dauvergne, Jérôme Shneider, Thomas Noel, Victor Claudet	Coordinator, WP1 (WP1 Leader), WP2, WP3 (Board), WP4 (Leader), WP5, WP6 (Board), WP7
P2	IOS	Internet of Subjects Foundation	FR	NGO	Serge Ravet, Marc Van Coillie	WP2 (Board), WP5, WP6 (Board), WP7 (WP7 Leader)
P3	NOT	University of Nottingham	UK	University	Sandra Winfield, Thomas Kirkham	WP2 (Leader), WP3, WP4, WP6 (Board), WP7
P4	URC	University of Reggio Calabria	IT	University	Francesco Buccafurri, Gianluca Lax, Domenico Ursino, Domenico Rosaci	WP2, WP3, WP5, WP6 (Board), WP7
P5	FRK	Forge Rock	NO	SME	Lasse Andresen, Victor Ake	WP2, WP3 (Board), WP4 (Leader), WP6, WP7
P6	TBS	TB-Solutions SA	ES	Large Enterprise	Mayte Hurtado	WP2 (Board), WP3, WP4, WP5, WP6 (Leader), WP7
P7	UST	University of Saint-Etienne	FR	University	Jacques Fayolle	WP2, WP3, WP5, WP6, WP7
P8	KYN	Kynesim	UK	SME	Richard Watt	WP2, WP3, WP5, WP6, WP7
P9	KUP	Kuppinger Cole	DE	SME	Martin Kuppinger	WP2, WP3, WP5, WP6, WP7

Associated Partners

Non funded contributing partners

AP1	LLV	Levelview	PT	SME	Sampo Kellomäki, Daniel Gomes, Pedro Magalhães	Associate partner. TAB Vice chair. TAS3 knowledge transfer and liaison, FI-CP liaison, Kantara API work, Exploitation.
AP2	KAN	The Kantara Initiative	USA	NGO	Fulup Ar Foll	Technical Architecture Board, Knowledge transfer

P1: Entr'ouvert (ETO), France

Legal name	**Entr'ouvert**
Acronym	**ETO**
PIC number	**971954357**
Department carrying out the work	**Research**
Role in project	**WP4 leader, WP2 board, WP3 board, WP5, WP6 board, WP7**
Responsible persons	**Mikaël Ates**

Entr'ouvert is a French company specialized in digital identity management and e-administration.

Entr'ouvert has been involved in the following research project: FederID, FC², TAS3 and RoleID.

Entr'ouvert is used to manage large projects about identity management, e.g. the SAML2 identity federation deployment of the FEPEM/IFEF (100K users), the integration of SAML2 in the Cisco appliance Iron port, pilots for "Mon Service Public" (Direction Générale de Modernisation de l'Etat) and for the French deposit office (Caisse des dépôts et Consignations).

Entr'ouvert develops widely recognized quality softwares like Lasso (SAML2 Library), Authentic2 (SAML2 Identity Provider) and WCS (workflow and form management).

Entr'ouvert is deeply involved in the free software community. Entr'ouvert members individually take part to different boards, e.g. the GNOME release team and the APRIL board.

Entr'ouvert relies on a full democratic model, each employee owns the society at equal shares, each decision is voted by all employees and each vote has the same weight.

Mikaël Ates is a young researcher and leads his research works for Entr'ouvert. He took his PhD in computer science in 2009 at the Université de Lyon. The subject of his thesis is *Digital Identities: A user-centric and privacy-respectful cross-organisational architecture*. He obtained his MSC in telecommunications, his engineer diploma and his MBA in 2004 from the université de Lyon. He has been involved in the projects FederID, FC² and RoleID. He gives lectures at the Télécom Saint-Etienne Engineer School on computer science and information security and keep writing articles on this matter. Mikaël Ates is also involved in free software developments and open source communities.

Frederic Péters, developer, debian developer, GNOME release team member, is an experienced and recognized analyst programmer. He has developed and contributed to many software and was the maintener of the software Lasso and Authentic. He has developed the tool wcs. He also worked on the pilots for "Mon Service Public" (Direction Générale de Modernisation de l'Etat) and for the French deposit office (Caisse des dépôts et Consignations). Frédéric Péters has been involved in multiple research projects: FederID, FC² and role-ID.

Benjamin Dauvergne is an experienced developer and identity standards expert. He leads the development of Lasso and Authentic, Entr'ouvert main projects as far as Identity Management is concerned. Benjamin Dauvergne has been involved in multiple research projects: FederID, FC² and RoleID.

Pierre Cros is a consultant, IM Expert and experienced project manager. Graduate from Sciences Po, Social Sciences and ENSSIB, he works for Entr'ouvert since 2004. He followed all Entr'ouvert projects concerning Identity Management and know s particularly well the economical and strategical aspects of this field.

Thomas Noel is an information system architect, a system administrator and a project manager. Ex-CTO of the Agence Universitaire de la Francophonie (as so he was in charge of digital campuses in about 50 countries), he just joined Entr'ouvert to bring his huge experience and abilities to our projects.

Jerome Schneider is an identity management system architect and a developer. Involved in Pardus (Turkish GNU Linux distribution), he is also the maintener of Larpe, a SAML2 reverse proxy. Jerome Schneider has been involved in multiple research projects: FederID, FC² and RoleID.

Victor Claudet is a commercial engineer. In charge of Entr'ouvert e-government products, he is very familiar with the citizens needs and views concerning privacy on the Internet.

P2: Internet of Subjects Foundation (IOS), France

Legal name	**Association de Préfiguration de l'Internet of Subjects**
Acronym	**IOS**
PIC number	**971936412**
Department carrying out the work	**Research**
Role in project	**WP7 Dissemination**
Responsible persons	**Serge Ravet**

Before joining ADP-IOS in 2010, Serge Ravet was Chief Executive of EIfEL. Combining both technological and pedagogical expertise (25 years experience in learning technologies, training and human resources development) with work experience in Europe and the USA, he is retained as learning technology expert, keynote speaker and consultant in a number of European projects. Publications include 'Technology-based Training' (Kogan Page, 1997);'Valider les Compétences avec les NVQs' (DEMOS, 1999); a Guide to e-learning Solutions (2001) and numerous articles on individual and organisational learning technologies, ePortfolios, competency development and recognition, quality systems. Serge was also at the initiative of the creation of the European Foundation for Quality in eLearning (EFQUEL). Serge coined the concept "Internet of Subjects" in the *internet of subjects manifesto* which is one of the ideas developed on the path towards an *Identity Centric Internet.*

Marc van Coillie has more than 10 years background in Research and Development in the eLearning and KM fields for public and private sectors (CNDP - french national educational institution, AFT-IFTIM - training company, Orange labs - telecom operator, EIFEL - european assocation...). He is an expert in Interoperability and integration of IT systems using SOA for eLearning, HR, KM and digital identity (using specifications such as HR-XML, IMS Global, Liberty Alliance, OpenID, Kantara, Micro-Format, OpenSocial, RDFa...) with a focus on ePortfolio and CV interoperability (CV transcoding web service, LinkedIN to Europass converter) and organising plugfest events to demonstrate conformance and interoperability of software and services regarding eLearning, Human Resources and Identity standards.

Marc Van Coillie is member of IEEE LTSC (Learning Technologies Sub Committee), expert for the CEN/ISSS WS/LT (Workshop on Learning Technologies), leader of the HR-XML Europass CV Interoperability Working Group of the HR-XML consortium, chair of the HR-EDU Special Interest Group of Liberty Alliance.

Projects in line with the scope of the project

- TAS3: a European integrated project dedicated to the development of trust technologies
- TELCERT: a European project dedicated to interoperability and conformance testing of learning environments.
- CV-Universel: a French project on CV management for large companies (l'Oréal, la Poste, etc.) based on digital identity technologies (SAML)
- Identités Actives: a 2 year self-funded project with FING on the exploration of technologies to support identity construction —and not just protection
- ETTCampus 2.0: a European project exploring the building and control of social reputation on the Internet (eReputation)

P3: University of Nottingham (NOT), United Kingdom

Legal name	**The University of Nottingham**
Acronym	**NOT**
PIC number	**999976978**
Department carrying out the work	**Centre for International ePortfolio Development**
Role in project	**Contribution to architecture, API specification and implementation, Proof of Concept**
Responsible persons	**Sandra Winfield, Tom Kirkham**

The University of Nottingham is one of the top five universities in the UK, and is nationally and internationally renowned for its teaching and research excellence. It was recently ranked 75th in the world by QS-World University Rankings.

The Centre for International ePortfolio Development is part of the Information Services Division in the University and was established in 2003 to carry out externally-funded research projects into how ePortfolios support learning, transitions and collaborations between institutions and between learning and work, Widening Participation, and Information, Advice and Guidance. Centre projects seek to maximise the efficiency of information flow, supporting stakeholders including SMEs and large business in access to seamless ICT services and quality information. The Centre is running a number of projects funded by the UK Joint Information Systems Committee (JISC) and is a partner in the TAS3 project.

Sandra Winfield has been Project Manager at the Centre for International ePortfolio Development since 2004, following a portfolio career including commercial publishing, teaching in schools, work as an open learning manager and a period working in computer services in the UK public sector. She holds an MSc in Computer Science from the University of Hertfordshire. She has run a number of successful JISC projects for the Centre and is currently managing the UK employability demonstrator for TAS3.

Dr Tom Kirkham holds a PhD in Distributed Computing from the University of Wales, Bangor. His main research experience is in the field of Dynamic Virtual Organisations, Trust and Security, Grid Computing, Semantic Web, SOA business integration, and the integration of legacy systems into SOA. He has worked on a number of UK and EU projects including Akogrimo and SOCRADES. He is currently working on the audit infrastructure, policy aggregation and the UK employability demonstrator for TAS3.

P4: University of Reggio Calabria (URC), Italy

Legal name	**The University of Reggio Calabria**
Acronym	**URC**
PIC number	**997224894**
Department carrying out the work	**DIMET**
Role in project	**WP2, WP3, WP5, WP6, WP7**
Responsible persons	**Francesco Buccafurri**

The **Mediterranea University of Reggio Calabria** is one of the four calabrian universities and the main university of Reggio Calabria. It is joined with the Mediterranean Universities Union (UNIMED), and it has undertaken over the years the development of international cooperation through the creation of stable and productive links in teaching and research fields, with a keen interest in the Mediterranean basin. The Mediterranea University is also committed to higher educational training through master degrees, in cooperation with international partners, and through the innovatory contents of the courses, the excellent reputation of the teaching staff and the level of the invested funds.

The **Department of Computer Science, Mathematics, Electronics and Transportation (DIMET)** was established in 1993 and currently consists of 48 researchers, mainly operating in the Information and Communication Technology, Industrial Engineering and Civil Engineering fields, and 17 research laboratories are activated inside it. It is has been involved in a high number of national and international projects and it has activated several research collaborations with public and private institutions, achieving significant results in terms of research excellence. In the high-formation area, it organizes several PhD courses.

Francesco Buccafurri is a full professor of computer science at the University "Mediterranea" of Reggio Calabria, Italy. In 1995 he took the PhD degree in computer science at the University of Calabria. In 1995 he was visiting researcher at the Information System Department of the Vienna University of Technology, Austria, where he joined the data base and AI group. His research interests include deductive-databases, knowledge-representation and nonmonotonic reasoning, model checking, information security, data compression, histograms, data streams, agents, P2P systems. He has published several papers in top-level international journals and conference proceedings. He serves as a referee for international journals and he is member of a number of conference PCs.

Gianluca Lax is an Assistant Professor of computer science in the Department of Computer Science, Electronics, Mathematics and Transportation (DIMET) at the University Mediterranea of Reggio Calabria, Italy. In 2000, he took the Laurea degree in Electronic Engineering at the University Mediterranea of Reggio Calabria. In 2005, he took the PhD degree in computer science at the University of Calabria. Since November 2005, he is Assistant Professor at the University of Reggio Calabria, Faculty of Engineering. He is also responsible of a number of computer science courses within Master courses. His research interests include P2P systems, user modelling, information security, e-commerce, data reduction and data streams. He has published in top level international journals and conference proceedings and he has served and serves as a referee for international journals and conferences.

Domenico Rosaci is Assistant Professor of computer science in the Department of Computer Science, Electronics, Mathematics and Transportation (DIMET) at the University Mediterranea of Reggio Calabria, Italy. He took the Degree "Magna cum Laude" in Engineering in 1994 and the PhD in Electronic Engineering in 1999. His main research interests are in the areas of Distributed Artificial Intelligence, Intelligent Agent Systems, Recommender Systems and Semantic Web. He is author of about 80 papers published in conference proceedings, books, and outstanding scientific journals, including ACM Transactions on Information Systems, VLDB Journal, Information Systems, Computational Intelligence, etc. He is in the editorial board of

the Open Cybernetics and Systemics Journal and he is member of the program committee of the IEEE AINA Conference, ARES Conference and International VLDB Workshop on Ontologies-based techniques. He served as referee for several international journals and conferences as the IEEE Transactions on Human, Man and Cybernetics, International Journal of Human Computer Studies, Knowledge and Information Systems, Information Sciences, User Modeling and User Adapted Interactions etc.

Giuseppe M. L. Sarnè is an Assistant Professor of computer science in the Department of Computer Science, Electronics, Mathematics and Transportation (DIMET) at the University Mediterranea of Reggio Calabria, Italy. In 1988, he took the Laurea degree in Engineering at the University of Calabria in Arcavacata (CS). Since November 2002, he is Assistant Professor at the University of Reggio Calabria, Faculty of Engineering. He is also responsible of computer science course within Engineering courses. His research interests include cooperation in multi-agent systems, agent technologies and models for e-commerce and adaptivity, reputation systems and neural networks. He has published in top level international journals and conference proceedings and he has served and serves as a referee for international journals and conferences.

Domenico Ursino received his Laurea Degree in Computer Engineering from the University of Calabria in July 1995. He received his PhD in System Engineering and Computer Science from the University of Calabria in January 2000. From October 2000 to January 2005 he was an Assistant Professor at University Mediterranea of Reggio Calabria. Currently he is an Associate Professor at the same University. His research interests include multi-agent systems, personalized and device-adaptive e-services, knowledge extraction and representation, scheme integration, semi-structured data and XML, Cooperative Information Systems, Folksonomies, Social Networking and Social Internetworking. He has published many papers in top level international journals and conference proceedings and he has served and serves as a referee for international journals and conferences.

P5: Forge Rock (FRK), Norway

Legal name	**ForgeRock**
Acronym	**FRK**
PIC number	
Department carrying out the work	**Research and Development**
Role in project	
Responsible persons	**Lasse Andresen**

ForgeRock is a global software company with bases in the USA, UK, France and Norway, ForgeRock is committed to continuity of innovation and service for the existing and new open source interaction, identity, and integration software found within the I3 platform.

Lasse Andresen. A powerhouse of tireless can-do enthusiasm, Lasse brings a unique blend of business, technical and people skills to leading Forgerock. His twenty-plus years of experience in the software industry include leadership roles at both Sun Microsystems and Texas Instruments, most recently as CTO for Sun Central and Northern Europe. His passion and vision combine to ensure ForgeRock is always ready to execute and deliver. 2000-2003 Co-Founder and CTO of www.gravityrock.com Lasse has played keyboards in several bands. Specialties: Entrepreneur, the network is the computer (cloud computing), identity and access management, web 2.0, infrastructure software, open source, distributed organisations, leadership

Victor Aké is Identity and Federation Architect. His core competences are Access Management and Federation of Identities (SAMLv2 and Liberty) and Web technologies. He has 22 years of experience in the IT industry, working with several IT companies like IBM, 3Com, Sun Microsystems and ForgeRock. He has focused in the Identity and Federation management technologies during the last years and was involved in federation projects in European countries for both private and governmental institutions.

P6: TB·Solutions (TBS), Spain

Legal name	TB·Solutions Advanced Technologies S.L.
Acronym	TBS
PIC number	998828983
Department carrying out the work	Research and Development
Role in project	Use case, trust architecture, API, access control and privacy, implementation
Responsible persons	Mayte Hurtado

TB·Solutions Group is comprised of the parent company TB·Solutions Advanced Technologies, S.L. which is located in Pamplona (Navarra) and its subsidiary TB·Solutions Technologies Software, S.L., whose share capital is 100% owned by the parent company located in Zaragoza. Moreover, it has branches in Barcelona, Madrid, Valladolid and Seville, and Miami (USA), Mexico, Colombia.

TB·Solutions offers generic software and security solutions for the public and private sectors, and specific solutions for the Public Administration, Financial Entities, Insurance Companies, and e-Health, its main research efforts being in digital signature and PKI products, global security services, both software and embedded systems.

Moreover, the TB-Solutions Group has strongly been committed since its start in 1987, under the business name Intercomputer, S.A., in investing resources in R&D and technological innovation not only at a national, but also at international level, by participating in National and European programmes, which have allowed the company to work jointly with some of the most important technological companies and organisations.

Relevant projects within the scope of the Project:

- **e-Confidential**: Aimed to the establishment of a trusted security platform providing secure information and identity interchange among users, applications and services.
- **TSC**: aimed in developing a family of HW/embedded SW silicon components enforcing secure and trusted computing in Consumer, Computer, Telecommunications and Wireless areas
- **M·POWER**: Defines and implements an open platform to simplify and speed up the task of developing and deploying services for persons with cognitive disabilities and elderly.
- **BRITE**: Provides interoperability between registries in different countries along with their different organisations and architectures.
- **REALTH**: Defines an integrated architecture taking over much of the required security requirements such as authentication or authorisation based on identity technologies (SAML / XACML).

Jesús Gómez is Computer Systems Engineer from University of Zaragoza. His research work is in the e-Health and embedded systems taking part in the analysis and integration of ubiquous services over SOA platform. Moreover, he has experience in the usage, analysis and design of secure environments based on encryption algorithms, digital signature and PKI.

Juan José Gracia is Telecommunications Engineer from University of Zaragoza. He works in the R&D department in the development and integration of services over SOA platform for international mobility and e-Health projects. He is knowledgeable in smart information systems, role and identity management based on PKI.

Carlos Bricio has a Informatics Degree from the University of Zaragoza. Currently he is analyst and Project manager in the R&D department. He is an expert in security technologies, varios programming languages and participates investigating and developing in both national and international projects.

Antonio Bermejo is Telecommunications Engineer from the University of Zaragoza and has post-graduate in Telecommunications' Infrastructures He is analyst and Project manager in R&D department working in radio communications, secure embedded systems, security tecnologies, audio and video streaming national and international projects.

David Montejo is Informatics engineer from the University of Vitoria. He is analyst-programmer in several R&D projects, such as secure embedded systems, TPM, security applications form DTT, mobiles.

P7: University of Saint-Etienne (UST), France

Legal name	**University of Saint-Etienne**
Acronym	**UST**
PIC number	**TBD**
Department carrying out the work	**Research**
Role in project	**TBD**
Responsible persons	**Jacques Fayolle**

Telecom Saint-Etienne is an engineer school of the University of Saint-Etienne (Université de Lyon) and is member of the French Telecom Institute. The research team SATIN works on the global scientific field of adaptive systems for telecom. This field includes (but is not limited to): - adaptation of remote graphical user interface of devices - adaptation of data to the network (next generation network, quality of service vs quality of experience) - adaptation to the media (hypermedia adpative systems) The data adaptation paradigm encompasses the need to address the information security issue, and especially the authorisation and authentication of the entities involved. It explains why the SATIN team has a part of its works dedicated to the identity management in open environment like the Internet, and has been involved in research project as FederID.

Jacques Fayolle is the head of the SATIN research team. He is also the development director of the Telecom Saint-Etienne engineer school. Jacques Fayolle manage research project on adaptative systems for a better integration of the human interactions in information systems. His personal scientific research fields are distributed architecture over the Internet and the use of semantic information to increase the pervasivity of information systems.

A specific doctoral position will be open for this project. The student will be drived by Jacques Fayolle. The PhD student profile includes skills on information technologies, security management, ubiquitous and pervasive computing, XML languages, and obviously, Internet architectures and network facilities.

P8: Kynesim (KYN), United Kingdom

Legal name	**Kynesim**
Acronym	**KYN**
PIC number	**TBD**
Department carrying out the work	**Research**
Role in project	**TBD**
Responsible persons	**Richard Watt**

Kynesim is a small technology consultancy firm based in Cambridge, UK with strong links to the University of Cambridge, for which some of our staff routinely teach.

We provide top-flight hardware and software development services to a variety of clients in the UK start-up, SME and public sectors, specialising in IPTV, home automation and energy monitoring.

Many of us were originally members of SJ Consulting and we have a good track record of delivering challenging technology to solve hard problems on tight deadlines.

Past projects we have been involved in include:

- Development of a novel ATSC video decode system for the US cable market and a novel IPTV STB concept for the UK.
- Video surveillance work for the UK public sector.
- Hardware and software development for advanced scientific imaging devices.
- Development of the Norton SD STB for VNL Ltd - one of the UK's first IPTV VoD deployments.
- Low power radio systems based on the Ember EM250/260 Zigbee chipset.
- Clean-room re-implementation of the JFFS2 flash filesystem.

Richard Watts has over ten years' experience in the technology sector in Cambridge; he has been a product manager for Metafaq, Transversal's flagship knowledge management product, worked for SJ consulting for three years on a variety of projects including WMA and VC-1 decoders and a hardware H.264 decode accelerator and recently completed two years' at Amino Communications building software for their award-winning line of Linux-based STBs and managing their Cambridge development office. Richard holds an MA and PhD in Computer Science from, and is a bye-fellow of, Selwyn College, Cambridge. His research interests include compilers, programming languages, operating systems and user interface design.

Gareth Bailey is a graduate Software Consultant; he has worked on various projects including innovative browser-based VoD prototype systems, accelerated 3-D graphics, and Windows Media DRM. Gareth holds a B.A. in Computer Science from Selwyn College, Cambridge.

John Cox is a Senior Software Consultant with many years experience developing video codecs and IPTV systems on x86 and TI 6000-series DSPs and Davinci chips. He has written H.264 decoders and MPEG-4 part 2 encoders and decoders.

Steve Wiseman is a Senior Hardware Consultant; among other things, he has worked on Dyson intelligent vacuum cleaners, VNL's Norton MPEG-2 STB and Balloon - a multi-use open hardware development board.

P9: Kuppinger Cole (KUP), Germany

Legal name	**Kuppinger Cole**
Acronym	**KYN**
PIC number	**TBD**
Department carrying out the work	**Analyst Group**
Role in project	**Specification and dissemination**
Responsible persons	**Martin Kuppinger**

Kuppinger Cole, founded in 2004, are the only European analyst group dedicated to provide expert advice on GRC, Identity and Access Management, IT security, Cloud Computing and other core IT issues as well as independent and critical evaluation of products and solutions in the realm of their research areas. Kuppinger Cole stands for expertise, opinion leadership and a vendor-neutral view of the extended Identity Management market and other growth sectors within the IT-market. This comprises subjects like classical Identity and Access Management (IaM), Governance, Risk Management and Compliance, Information Rights Management (IRM), Identity Risk Management, digital certificates, cards and tokens, Single Sign-On, Auditing, Federation, user-centric Identity Management, Identity 2.0, Cloud Computing, Virtualization and other areas.

Kuppinger Cole is constantly analysing the market and in touch with all important manufacturers as well as end-user companies. The results are provided in Kuppinger Cole´s newsletter, through webinars, reports and studies, in keynote addresses and events.

Kuppinger Cole´s continued research covers more than 200 companies in the Identity Management and GRC market alone, with a global focus that keeps track of small suppliers as well as the key players. This allows Kuppinger Cole to consult on decisions for quick solutions to specific problems as well as deliver a longer-term vision for strategies and roadmaps.

As an independent analyst group Kuppinger Cole also organises conferences, seminars, workshops, management briefings and webcasts on IAM issues.

Kuppinger Cole advises manufacturers and users, evaluates market opportunities for products and systems and makes in-depth market analyses available to the various segments of the identity sector.

Martin Kuppinger, born in 1965, is the author of more than 50 IT-related books, as well as a widely-read columnist and author of technical articles and reviews in some of the most prestigious IT magazines in Germany, Austria and Switzerland. He is also a well-known speaker and moderator at seminars and congresses. His interest in Identity Management dates back to the 80ies, when he also gained considerable experience in software architecture development.

Kuppinger Cole will most include some other analysts in the project if required and appropriate, depending on the type of work to be done:

Tim Cole, co-founder, author of many IT- and Business Management books, journalistic background.

Prof. Dr. Sachar Paulus, full-time professor at the FH Brandenburg and former Chief Security Officer of SAP AG.

Sebastian Rohr, former Chief Security Advisor of Microsoft Germany, strong background in strong authentication and related areas.

Mike Small, senior expert with long term industry background, focused on IAM and Cloud Computing

Projects in line with the scope of the project

- Ongoing research on all relevant vendors and standards initiative in that space. One outcome of this are the European Identity Awards, awarded by KuppingerCole. These

awards included several of the specs relevant for this project during the past years, proving the affinity of KuppingerCole with this topic.

- Participation in the Think Trust Working Group 2 within the Riseptis project (Prof. Dr. Sachar Paulus and Martin Kuppinger).
- Advisor to many companies in the relevant market segment, including Fun Communications, one of the founding members of the
- German chapter of the Information Card Foundation (ICF).
- Member of Kantara initiative.

Associate Partner AP1: Levelview (LLV), Portugal

Legal name	**Levelview, Lda.**
Acronym	**LLV**
PIC number	**971278461**
Department carrying out the work	**Research**
Role in project	**Architecture board, TAS3 knowledge transfer and liaison, FI-CP liaison, API, exploitation**
Responsible persons	**Susie Chua (administrative), Sampo Kellomäki (technical)**

Levelview is a Portuguese startup (SME) that aims at bringing to the market a commercial grade product suite (based on the reference implementation) for TAS3 trust and security technologies. Levelview also provides professional services, such as installation, training, and IdM architecture consulting to support deployments based on TAS3 trust and security technologies. Availability of such commercial products and services is an important enabler for adoption of both TAS3 and ICI technologies.

Contribution. Levelview's contribution will be three fold:

1. To facilitate adoption of TAS3 technology by ICI. This happens mainly via architecture board.
2. Harmonization of APIs. This will happen mainly via Levelview's participation in Kantara Initiative on the forums where ICI also participates.
3. Finally as Levelview plans to exploit TAS3 technology, there is scope to exploit ICI technology as well.

Sampo Kellomäki is the chief architect of TAS3 (Trusted Architecture for Securely Shareable Services with Privacy - www.tas3.eu), a FP7 funded project that will be leveraged by the present proposal. He is also the lead developer of ZXID.org open source project that is the reference implementation of TAS3 core security architecture.

Sampo's business interests include Levelview, Lda, a company focusing on exploitation of TAS3 technology and Wizi SA, a mobile social networking company (Wizi connection will be outside ICI).

Sampo has been on the forefront of identity management and federation technologies for last 10 years, acting as the architect of Symlabs directory and federation products, participating from start in Liberty Alliance, SAML, and XACML standardisation. Several Liberty Alliance specifications were authored, in editor capacity, by Sampo. He is a frequent speaker or panelists in IdM related industry events. Sampo holds an MSc/CS degree from Helsinki University of Technology.

Daniel Gomes is developer in employ of Levelview, productizing ZXID, focussing on IdP and identity mapping aspects. He holds MSc from Instituto Superior Tecnico, Lisbon.

Pedro Magalhães is developer in employ of Levelview, focusing on PDS aspects of ZXID. He is working towards his MSc from Instituto Superior Tecnico, Lisbon.

Susie Chua is the administrative contact of Levelview. She has extensive experience from organisation and administration of previous FP7 projects, such as TAS3. She holds MBA from University of Singapore.

Associate Partner AP2: The Kantara Initiative (KAN), USA

Legal name	**The Kantara Initiative**
Acronym	**KAN**
PIC number	
Department carrying out the work	**The European Working Group, the User Managed Access Working Group (UMA WG) and other working groups**
Role in project	**Architecture design, adoption, dissemination, licensing**
Responsible persons	**Fulup Ar Foll**

Kantara Initiative was announced on April 20, 2009, by leaders of several foundations and associations working on various aspects of digital identity, aka the Venn of Identity". It is intended to be a robust and well-funded focal point for collaboration to address the issues we each share across the identity community: Interoperability and Compliance Testing; Identity Assurance; Policy and Legal Issues; Privacy; Ownership and Liability; UX and Usability; Cross-Community Coordination and Collaboration; Education and Outreach; Market Research; Use Cases and Requirements; Harmonization; and Tool Development.

The mission of the Kantara Initiative is to foster identity community harmonization, interoperability, innovation, and broad adoption through the development of open identity specifications, operational frameworks, education programs, deployment and usage best practices for privacy-respecting, secure access to online services

Vision: Ensure secure, identity-based, online interactions while preventing misuse of personal information so that networks will become privacy protecting and more natively trustworthy environments.

Kantara goals are:

- Accelerate marketplace adoption through clear messages, defined processes, and open community collaboration that brings vendors, deployers, individuals, and organisations together
- Bring together technical, business, legal, and policy experience to achieve holistic & trusted identity management solutions
- Establish an open and democratic governance model with no financial barrier to participation
- Implement an operational structure with nimble processes, procedures, and oversight, and a viable financial model
- Commit to open standards and encourage interoperable implementations from both the COTS product and open source development communities
- Foster positive dialogue across all relevant organisations to assure coordination, harmonization, and re-use of all applicable open content (specs, policy, etc.)
- Establish programs with strong branding for technical and operational output to promote interoperability, compliance and/or conformance

Kantara Initiative Trustee and Regular Members

Trustees
British Telecommunications
Computer Associates
Fidelity Investments
Internet Society
NeuStar, Inc.
NRI
NTT
Oracle

Members
AARP.org
Anakam
AOL
Josep Bardallo
Gerald Beuchelt
BIPAC
John Bradley
Dr. Hellmuth Broda
John Bullard
Center for Public Management and eGovernment
Dan Combs
Connecting.nyc Inc.
CSC
Salvatore D'agostino
Danish Biometrics
Danish National IT
Data Portability Project
Deutsche Telekom AG
Brian Dilley
Direct Marketing Association (DMA) (MNP)
Drummond Group
eHealth Ohio
Eduserv
ElfEL
Entr'ouvert
Ericsson
Fischer International
France Telecom
Frazier-McElveen, Myisha
Fraunhofer Fokus
Fraunhofer SIT
FuGen Solutions, Inc.
Fun Communications GmbH
FSTC
Stefanie Geuhs
Global Patient Identifiers, Inc.
Government of Canada
GSA
Thomas Hardjono
Helsinki Institute of Physics
HIMSS
Rainer Hoerbe
Andrew Hughes
Identropy, Inc.
Indiana University
Information Card Foundation (ICF)
Internet2
Gershon Janssen
Kantega
Kuppinger Cole
Colin Mallett
MEDNETWorld.com
MyDex
National eNotary Registry
New Zealand Government, Dept of Internal Affairs
NHK
OpenID Society
PayPal
Ping Identity
Probaris Solutions
RedIRIS
Mary Ruddy
SAFE Bio-Pharma Association
Andrew Shikiar
Signicat AS
Smart Card Alliance
SPIKE
SUNET
Surescripts
Swisssign AG
TAS3
TERENA
The Boeing Company
tScheme Limited
Paul Trevithick
Ubisecure Solutions, Inc.
UNINETT
University of Namur, Belgium
University of Washington
UPM
Visiti AS
Mike Waddingham
XDI.org

Contribution. Kantara Initiative's contribution will be:

1. Provide a network and an organisation (working groups etc.) to contribute to the design of ICI architecture
2. Provide a public platform for the dissemination of ICI outcomes and contribute to the success of the call for tenders to explore the capacity of ICI to be adopted
3. Provide a legal framework for making the outcomes of ICI securely available under open source, royalty-free licenses[3]

Projects in line with the scope of the project

eGovernment WG The eGov work group focuses on international issues particularly focused on governments. Multi-national participants contribute to this group from Asia, European Union and North America.

Federation Interoperability WG The Federation Interoperability WG focuses on the tools that will link federations so they can share meta-data securely at varying levels of assurance.

Health Identity Assurance WG This group focuses purely on issues pertaining to health care and health care systems. There is special focus on patient privacy and secured data exchange around patient records and information.

Identity Assurance This group manages the Identity Assurance Framework, its components and profiles. This group is at the forefront of managing the documentation that the Kantara Initiative Assurance Accreditation and Certification Programmes abide by.

ID-WSF Evolution WG This group manages the ID-WSF specification set in its matured lifecycle.

[3] One of the strong point of the Kantara Initiative is its ability to face unscrupulous actors that would attempt to patent a technology developed by ICI

Information Sharing WG This group focuses on contract models and scenarios where information must be shared. They are developing contracts which would provide or outline details around how and with whom information is shared.

Interoperability WG Interoperability WG directly supports the technical interoperability certification programme developing test plans and documentation.

Privacy and Public Policy WG Also known as P3WG, this group is under taking the development of a Privacy Framework. With input from multi-national communities and industry this Framework would be adopted by the Kantara Initiative Assurance Certification program for testing.

Telecommunications Identity WG With strong participation from Asia and Europe this work group focuses on issues related to Telecommunications and deployment of federation in Telecommunications systems.

Universal Login Experience WG This group is building mock-ups for a method which would enable all users to have the same login experience regardless of Identity Providers or Management Systems.

User Managed Access WG This group is defining how a User would be empowered to manage access to their information and records.

B.2.3 Consortium as a whole

The ICI consortium has a strong and committed team – all consortium members have either an academic or a combined academic & business impact, in Europe and beyond. It is constituted by partners that have a strong and reliable track record in achieving successfully projects related to identity. The choice of creating a consortium dominated by SMEs does not mean that large organisations are not involved: through the Kantara initiative, an associated partner, a number of large organisations will be able to contribute to and benefit from the project activities. Through Kantara working groups the ICI consortium will be able to interact with representatives of large corporations and governments (for a full list of Kantara working groups, see the support letter provided in the annex).

The range of partners covers the whole spectrum of competencies required to achieve successfully the project:

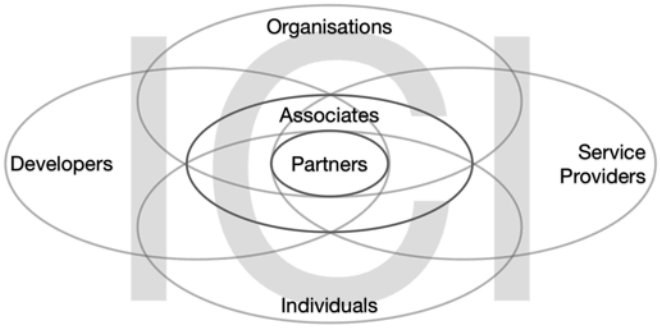
- Project management, including large scale projects
- Large scale deployment of identity and security projects
- Contribution to standardisation processes in the field of identity and access management — several partners were active members of Liberty Alliance and now the Kantara Initiative
- Contribution to open source developments
- Scientific research in the areas of security, trust, user interfaces, mobile devices
- Development and integration of technologies, including mobile devices and set-top boxes
- International recognition: members of the consortium have worked on large scale identity projects in their respective countries, in Europe and beyond and several are recognised leaders.

Collectively the partners are responsible for 4 different open source implementations of SAML: 2 are partners (Entr'ouvert and Forge Rock) 2 are associated partners (Levelview and Internet 2 which is a member of the Kantara Initiative. Moreover, Lasso and ZXID are used in large-scale production environments, and both are certified conformant to the SAML2 standard, a conformance certificate delivered by the Kantara Initiative Consortium.

The consortium also has a successful track record with dissemination. Kuppinger Cole is the organiser of the most influential identity conference in Europe and ADP-IOS (formerly EIfEL) has successfully organised conferences in Europe and beyond on advanced learning technologies.

One of the main strengths of the consortium is a strong common vision and an ability to share it with others, a committed team and a clear governance structure which are the conditions for creating an impact. The ICI consortium meets those criteria – all partners have first hand experience with the problems tackled by the ICI project and are involved in a number of communities, from standardisation bodies, to end users.

Organisation of the extended consortium



The extended consortium is organised in three tiers:

1. **Core Partners**: they are the ICI contractual partners, the consortium per se.
2. **Associate Partners**: not funded by the project, they are organisations committed to contribute to and exploit the outcomes of the project.
3. **Developers and service providers**: 10% of the total budget has been earmarked to cover 2 calls for tenders that will involve additional partners during the *adoption* phase of the

project. Our goal is to involve universities, researchers as well as start-up companies that should find in the ICI consortium valuable resources to achieve their goals.

About ICI Core Partners

ICI core partners bring together the whole range of expertise and experience, from research to integration, standards design to (conformant) software design integrated in a variety of hardware, from architects to developers and dissemination specialists. Several of the partners are recognised as leaders in their domain. To the exception of TB-Solutions, all partners are SMEs, universities and NGOs.

Entr'ouvert has a strong technical expertise, as well as in project management. They have demonstrated their architecture design, development and integration competencies in a number of large scale identity projects. Entr'ouvert is also a recognised contributor to the Open Source community and an expert in the implementation of OASIS (SAML) and Liberty Alliance (IDWSF) standards. Entr'ouvert is also a contributor to the work of the Kantara Initiative on identity specifications.

ADP-IoS is a brand new not-for-profit organisation born out of ElfEL, an organisation recognised internationally for its work on learning technologies, in particular ePortfolios, a domain of choice for an Identity Centric Internet. It brings a strong expertise in leading innovative projects in the domain of learning and employment technologies. ADP-IoS (Association de Préfiguration de l'Internet of Subjects) was created with the goal of making an Identity Centric Internet a reality: the Internet of Subjects. ADP-IoS staff was involved in the TAS3 project.

Nottingham University: hosts the Centre for International ePortfolio Development a department established in 2003 to carry out externally-funded research projects into how ePortfolios support learning, transitions and collaborations between institutions and between learning and work; The Centre is running a number of projects funded by the UK Joint Information Systems Committee (JISC) and is a partner in the TAS3 project where they are developing a prototype of a personal data store.

University of Reggio Calabria is recognised for its scientific contributions in information system security with a number of publications in refereed journals. An other dimension of its work is social networks.

ForgeRock is a recognised expert on OASIS SAML and Liberty Alliance ID-WSF specifications. It brings to the project strong competencies in software design and development in the field of identity and access management.

TB-Solutions is a large organisation (the largest of the consortium) with extended experience in the integration of large projects security and identity management. It will bring to the project an experienced team of software architects and developers.

University of St Etienne brings to the project its scientific expertise in user interface, ontologies and cross-organisational identity management.

Kynesim has an extensive experience with interface for mobile and smart-phones as well as set-top boxes. It is a recognised specialist in integration and multimedia data processing. Kynesim has also some experience on security systems —project in the UK public sector. An other domain of expertise is DRM, something that might raise interesting discussions in the consortium :-)

Kuppinger Cole brings the expertise of the leading analyst group dedicated to provide expert advice on GRC, Identity and Access Management, IT security, Cloud Computing and other core IT issues. Organiser of the European Identity Conference, a landmark for the professionals working in that field, Kuppinger Cole regularly publish newsletters and organise webinars.

About ICI Associate Partners

Once the project launched, one key activity of the Dissemination and Adoption WP will be the recruitment of associate partners in order to extend the reach of the project.

We have already two fully committed partners: Levelview (Portugal) and the Kantara Initiative (USA, with a European chapter in the process of being created).

Levelview is a Portuguese startup (SME) that aims at bringing to the market a commercial grade product suite (based on the reference implementation) for TAS3 trust and security technologies. Levelview also provides professional services, such as installation, training, and IdM architecture consulting to support deployments based on TAS3 trust and security technologies.

The **Kantara Initiative** is a not-for-profit organisation with the goal to accelerate marketplace adoption of identity and access management solutions. It is committed to open standards and encourages interoperable implementations from both proprietary solutions and open source development communities. The ICI project will be able to exploit the Kantara Initiative's work groups and community to contribute to the design and exploitation of the ICI architecture.

B.2.4 Resources to be committed

Describe how the totality of the necessary resources will be mobilised, including any resources that will complement the EC contribution. Show how the resources will be integrated in a coherent way, and show how the overall financial plan for the project is adequate. In addition to the costs indicated on form A3 of the proposal, and the effort shown in section 1.3 above, please identify any other major costs (e.g. equipment). Ensure that the figures stated in Part B are consistent with these. (Maximum length for Section 2.4 – two pages)

	KYN	IOS	FRK	URC	TBS	UST	NOT	ETO	KUP	ICI Project
Indirect cost rate 20 or 60%	60%	60%	60%	60%	20%	60%	60%	60%	60%	
RTD										
Funded at 50 or 75%	75%	75%	75%	75%	50%	75%	75%	75%	75%	
Total personnel cost Funded	222,793	107,837	366,667	143,780	108,533	196,845	144,679	258,500	156,300	**1,705,934**
Total equipment	5,000	5,000	8,000	8,000	3,000	5,000	5,000	4,000	5,000	**48,000**
Total travel	11,100	5,100	12,000	12,000	11,000	9,300	7,200	14,100	4,000	**85,800**
Other Costs	0	0	6,000	6,000	6,000	0	6,000	6,000	0	**30,000**
Total other costs	16,100	10,100	26,000	26,000	20,000	14,300	18,200	24,100	9,000	**163,800**
Total Direct Costs	238,893	117,937	392,667	169,780	128,533	211,145	162,879	282,600	165,300	**1,869,734**
Total Indirect Costs	143,336	70,762	235,600	101,868	25,707	126,687	97,728	169,560	99,180	**1,070,427**
Total Costs	382,229	188,699	628,267	271,648	154,240	337,832	260,607	452,160	264,480	**2,940,161**
Requested EC Contribution	**286,671**	**141,524**	**471,200**	**203,736**	**77,120**	**253,374**	**195,455**	**339,120**	**198,360**	**2,166,561**
MGT										
Funded at 100%										
Total personnel cost								66,000		**66,000**
Total other costs										
Total Direct Costs								39,600		**39,600**
Total Indirect Costs								105,600		**105,600**
Total Costs for the partner								105,600		**105,600**
Requested EC Contribution	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**105,600**		**105,600**
OTHER (dissemination)										
Funded at 100%										
Total personnel costs	30,107	272,763	73,333	38,280	21,707	33,055	24,522	38,500	99,769	**632,036**
Call for tenders								500,000		**500,000**
Total travel	1,500	12,000	2,400	3,900	3,000	1,500	1,200	8,700	10,000	**44,200**
Conference	2,000	4,000	0	4,000	0	2,000	2,000	2,000	2,000	**18,000**
Other costs								14,000		**14,000**
Total other costs	3,500	16,000	2,400	7,900	3,000	3,500	3,200	524,700	12,000	**576,200**
Total Direct Costs	33,607	288,763	75,733	46,180	24,707	36,555	27,722	563,200	111,769	**1,208,236**
Total Indirect Costs	20,164	173,258	45,440	27,708	4,941	21,933	16,633	337,920	67,061	**715,059**
Total Costs	53,771	462,021	121,173	73,888	29,648	58,488	44,355	901,120	178,830	**1,923,295**
Requested EC Contribution	**53,771**	**462,021**	**121,173**	**73,888**	**29,648**	**58,488**	**44,355**	**901,120**	**178,830**	**1,923,295**
Total personnel Costs	252,900	380,600	440,000	182,060	130,240	229,900	169,201	363,000	256,069	**2,403,970**
Total Direct Costs	272,500	406,700	468,400	215,960	153,240	247,700	190,601	885,400	277,069	**3,117,570**
Total Indirect Costs	163,500	244,020	281,040	129,576	30,648	148,620	114,361	613,080	166,241	**1,891,086**
Total Cost	**436,000**	**650,720**	**749,440**	**345,536**	**183,888**	**396,320**	**304,962**	**1,458,880**	**443,310**	**4,969,056**
Requested EC Contribution	**340,443**	**603,545**	**592,373**	**277,624**	**106,768**	**311,862**	**239,810**	**1,345,840**	**377,190**	**4,195,456**
EC Contribution Average rate	*78%*	*93%*	*79%*	*80%*	*58%*	*79%*	*79%*	*92%*	*85%*	**80%**

In the budget presented in the table above 500 k€, 10% of the total budget, are earmarked by Entr'ouvert, the coordinator, to feed in the call for tenders, which is a pivotal part of the project which is geared towards studying the conditions of *feasibility* and *adoptability* of an Identity Centric Internet.

Each country representative will also receive 6k€ to fund the renting of servers to create conditions of a distributed network of IC-Agents hosts, initially for testing, then to support the adoption phase and eventually a reference implementation of the IC architecture.

Part B. Section 3. Impact

B.3.1 Expected impacts listed in the work programme

Describe how your project will contribute towards the expected impacts listed in the work programme in relation to the topic or topics in question. Mention the steps that will be needed to bring about these impacts. Explain why this contribution requires a European (rather than a national or local) approach. Indicate how account is taken of other national or international research activities. Mention any assumptions and external factors that may determine whether the impacts will be achieved.

The objective of ICI is to provide every individual with the means to fully control their personal data, from creation to exploitation by themselves and third parties. The main challenge is primarily human, not technological: to educate and convince the designers of information systems and users of services exploiting personal data.

The potential impact of the ICI project is very considerable, in the following key areas:

- ICI will provide individuals with a clear vision of their personal sphere and how their personal data is being used and how it could be exploited to their benefit
- ICI will provide individuals and communities the means to dynamically create and control social spheres where individual will have full control over the use of his personal data within a circle of trust
- ICI will provide businesses with a trust architecture that will improve business relationships and create new opportunities for European business
- ICI will provide an integrated approach to security and trust that enables consistent end-to-end privacy assurance in open and distributed environments.
- ICI will address the societal implications of wider ICT integration to the Human Right to privacy, by highlighting policy and regulatory as well as technical innovations needed.
- ICI will identify and contribute towards the inclusion of security and trust policies in standards applicable to web services in all domains

It is by making trust visible and tangible to the end-users, through the ICI dashboard, that we will create the conditions for further innovation. Providing citizens with a dashboard to control and manage the exploitation of their personal data will have an impact on:

1. Technology: this will put a pressure on service providers to be more transparent in the use of personal data.
2. Economy: new business services will emerge that will change the relationships between stakeholders (B2B, B2C and C2C). For example, VRM (Vendor Relationship Management) systems will be representative of another relationship than what CRM (Customer Relationship Management) had to offer
3. Lifelong learning and employability:
4. Health-care: with the ability to visualize one's personal data, patients will be empowered to share their personal health records and other relevant data with services (e.g. Patients Like Me) supporting the management of their health.
5. Social practice and citizenship: by allowing anonymous search of personal data, like the type of heating system, consumption, mode of transport etc. this can lead to new types of services facilitating the change of behaviour required to reduce our carbon emission.

Expected impact in the call	**Impact of the ICI project**
impacts on markets in 5-10 years	The ICI architecture is designed with the perspective of transforming business relationships, exploiting the power of VRM and '*user chain management*'' through novel services made possible by the liberation of personal data, in a trust environment
impact of ICT on social behaviours	Giving everybody the opportunity to have a tangible and autonomous representation of themselves will be a powerful empowerment mechanism
impact on industrial competitiveness and on addressing socio-economic goals	The ICI architecture creates the conditions to move from an economy of ''push'' to an economy of ''pull''. In doing so billions of Euros can be saved by reducing the costs of planning decision on obsolete information and associating users and consumers to the design of services by moving from the model of ''supply chain management'' to that of ''demand chain management''.
impact future industrial ICT research agendas.	Pervasiveness of digital appliances collecting and exploiting personal data calls for an identity centric architecture.
Strengthened positioning of European industry in the fields of Future Internet technologies, mobile and wireless broadband systems, optical networks, and network management technologies.	The development of an Identity Centric Internet will give Europe an edge over its competitors. Many of the concepts developed in the project will have to be further translated into lower layers of the architecture, such as routers, set-top boxes etc. Integration of trust technologies within hardware and low level protocols will improve performance and resilience of trust networks.
Developing the technology for the future generations of the European high-speed broadband and mobile network infrastructure.|	Mobiles telephones might become the ubiquitous device used to present credentials
Increased economic and energy efficiency of access/transport infrastructures (cost/bit). Contributions to standards and regulation as well as the related IPRs, with a predominant role for Europe in standardisation bodies and fora.	One key ICI associated partners is the Kantara Initiative, through which a number of outcomes will be made accessible under royalty-free license. One on the indirect outcomes of the project should be the creation of a European chapter of the Kantara Initiative, giving Europe a stronger voice in the design of standards related to identity management and trust.
Emergence of European interoperable clouds contributing to an internal market of services in the EU whilst providing very significant business opportunities to SME's; improved trust in cloud-based applications and storage for citizens and business.	ICI will considerably lower the access barriers to new entrants on a market. With ICI it will be possible for an entrepreneur to find in one click ("I feel lucky") the investors, partners, staff and clients.
Fast innovation cycles in service industry, e.g. through the use of Open Source development model.	The outcomes of the ICI project will demonstrate how an open source approach to trust can create fast adoption of a disruptive technology.
Improved European industrial competitiveness in markets of trustworthy ICT, by: facilitating economic conditions for wide take-up of results; offering clear business opportunities and consumer choice in usable innovative technologies; and increased awareness of the potential and relevance of trustworthy ICT.	The ICI project is gears towards creating the conditions for rapid adoption of a trust infrastructure. The ambition of the pilot is to reach 1 million users, individuals and organisations. If we reach that goal, that will demonstrate the value of an IC-Agent-based trust infrastructure, and if we fail, data collected will be valuable to improve our approach or open new research and development activities.
Adequate support to users to make informed decisions on the trustworthiness of ICT. Increased confidence in the use of ICT by EU citizens and businesses. Increased usability and societal acceptance of ICT through understanding of legal and societal consequences.	The ICI project will design a personal/privacy dashboard that will provide individuals with the means to make informed decision in a trustworthy environment. Individuals (and organisations) will be able to attach policies to their data, and these policies will be enforced as they will be exploited by parties represented by IC-Agents with an embedded Policy Enforcement Point.

Demonstrable improvement (i) of the trustworthiness of increasingly large scale heterogeneous networks and systems and (ii) in protecting against and handling of network threats and attacks and the reduction of security incidents.	The pilots will (try to) demonstrate how a large scale heterogeneous network of autonomous IC-Agents is improving the security and privacy of personal data and transactions. Such an architecture will, of course, create new type of threats, but they should be much more fragmented than when a hacker (or a malevolent insider) attacks the NHS database containing dozens of millions of personal health records.
Significant contribution to the development of trustworthy European infrastructures and frameworks for network services; improved interoperability and support to standardisation.	ICI will provide a framework for a highly scalable trust architecture. This work will inform standardisation bodies through the Kantara Initiative, the international body at the forefront of identity and access management standards.
Demonstrable usability and societal acceptance of proposed handling of information and privacy.	The pilots should demonstrate that there is an alternative to existing, proprietary social networks, and (one of) the ICI challenge (s) will be to understand what the incentives for leaving/ quitting proprietary social networks (initially, keep them but move the control to the IC-Agent.
Improved coordination and integration of research activities in Europe or internationally.	The ICI project involves associated partners beyond Europe and one of the outcomes of the project should be the creation of a European legal entity of the Kantara Initiative (this is not listed as a deliverable as it is not directly related to the objectives of this call). This should give Europe a stronger voice in the international identity community.

B.3.2 Dissemination and/or exploitation of project results, and management of intellectual property

Describe the measures you propose for the dissemination and/or exploitation of project results, and how these will increase the impact of the project. In designing these measures, you should take into account a variety of communication means and target groups as appropriate (e.g. policy-makers, interest groups, media and the public at large). For more information on communication guidance, see http://ec.europa.eu/research/science-society/science-communication/index_en.html. Describe also your plans for the management of knowledge (intellectual property) acquired in the course of the project.

Dissemination strategy

Principles of ICI Dissemination Strategy

There are already a number of solutions to the problems addressed by ICI, but these solutions suffer from a number of flaws that are:

- **architecture**: existing solutions do not transform the Internet into an Identity Centric architecture —based on the recomposition of existing components, ICI builds a new and open ID-Centric architecture (*** careful here: "open ID-Centric" vs. "OpenID Centric". Personally I do not subscribe to OpenID as it is an identity preservantion hostile technology.)
- **adoption** —there are a number of different solutions, but their level of adoption is low, and fragmented, without any impact on the real fragmentation and lack of control of personal data

The objective of the dissemination strategy is more than simply make the deliverables of the project known to the relevant stakeholders, but to create the conditions for wide adoption of the ICI architecture. We have set the goal of one million users of the ICI architecture by the end of the project.

Adoption of an Identity-Centric Internet, where individuals are in full control of their personal data will be easier for some stakeholders than others. In the field of commerce, it means that we are moving from a relationship reified into a customer-relationship management system (CRM) to one defined by a vendor-relationship management system (VRM) a concept coined a few years ago by Doc Searl at Harvard Law School. Moving from CRM to VRM means that vendors trust more their prospects and clients to keep up-to-date their profiles than the person in the marketing department or the information collected by Google, Facebook, Microsoft and others that spend all their energy in spying on our activities.

Adoption of a trust architecture requires much more than just convincing a person or an organisation that it/she can have trust in the technology. The ICI architecture is a disruptive architecture: it allows to do business differently, to establish relationships differently. Mainly it allows for the first time in history to provide the means for individuals to have a sense of agency on the Internet, and not just stay at its periphery, behind a browser or a client application. In order to disseminate the message that a disruptive technology (what really are the outcomes of the project) is at our disposal and that it is an opportunity to do things differently, ICI will organise a public campaign in direction of key stakeholders.

Why one million users?

The objective of one million users has been set in order to verify whether the ICI architecture is easily adoptable or not, whether new and existing businesses and services find the cost/benefit of adopting this new architecture is worth it. After all Facebook got its first million user in less than one year...

The main problem with the adoption of trust architectures is not so much technological than human: end users, system architects, business owners etc. still live and think within the old Internet paradigm where identity management parks individuals at the periphery as users or consumers and not are autonomous entity. Many also believe, despite witnessing what

happened recently with social computing, that change is slow, or if it is rapid, it only addresses marginal activities or business areas.

To move into the modern world of identity management, there are two main options today:

- adopt a solution providing a low level of trust, but easy to adopt as it does not ask any real reengineering of identity policy management — e.g. OpenID, as simple single sign on mechanism
- adopt a solution providing a high level of trust but more difficult to adopt as it requires a proper reengineering of identity policy management — e.g. SAML

We believe that there is a third option:

- adopt an architecture providing a high level of trust which is easy to implement because the burden of ID management and trust rests on an independent, open and public architecture and do not require heavy reengineering — the goal of ICI

We believe that providing such architecture, should lead to a rapid adoption by individuals, organisations, businesses and service providers. If ICI provides an architecture where it is possible for anyone to operate as they operate today when they create a web site, or an online shop, while providing the extra service of *trust relationship management*, if for existing services, entering into a highly reliable trust federation is just as easy as adding an OpenID login mechanism, we will have created the conditions for rapid adoption.

Can we reach the one million users goal?

Most innovative activities, by definition, must fail. Otherwise, they are not truly innovative or exploring the unknown. But value comes from that small proportion of activities that are able to make significant breakthroughs, as well as identifying what can be learned from *failures*.

Does it mean that we do not really want to achieve that goal? Yes, we want to do everything within the means of the project to reach that goal, to record and report all the data collected in the course of the project, so if we 'fail' following projects will have useful data to be exploited.

Moreover, all the dissemination activities will have raised the level of awareness of a number of stakeholders that will have an impact beyond the end of the project.

What targets?

Even starting with the assumption that the ICI team has been able to produce the best possible architecture, easy to implement, there is no guarantee that the ICI architecture will be adopted. Managers of legacy systems might not see the real benefits of empowering users, as it will reduce their power. Similarly with a number of businesses that have striven on the privatisation of personal data to their profit.

The iconic figure ICI is aiming for is the **'21st century worker**' (not just the *knowledge worker*)

According to 2009 Eurobarometer Survey on Entrepreneurship, 45% of all Europeans would like to be self-employed while 49% would prefer working as an employee. In the USA the preference for self-employment has decreased from 61% to 55%. However, the share of US citizens who would like to be an employee has remained almost unchanged at 36% (vs. 37% in 2007).

In the report *Entrepreneurship in the EU and beyond* (2009) the European Commission reports that four percent (20 million) of EU 501 million citizens (831.4 million, using a definition which includes the whole of the transcontinental countries of Russia and Turkey) were currently in the embryonic phase, i.e. taking the necessary steps to start up a business, 3% (15 millions) were running a new business and 6% (30 million) were running an established business. In total, 12% (60,1 million) of EU citizens were currently involved in entrepreneurial activity.

One growing component of entrepreneurship is *social entrepreneurship*. According to the European Commission (http://ec.europa.eu/enterprise/policies/sme/promoting-entrepreneurship/social-economy/), a significant proportion of Europe's economy is organised to make profits not only for investors. Social economy enterprises represent 2 million enterprises (i.e. 10% of all European businesses) and employ over 11 million paid employees

(the equivalent of 6% of the working population of the EU): out of these, 70% are employed in non-profit associations, 26% in cooperatives and 3% in mutuals. Social economy enterprises are present in almost every sector of the economy, such as banking, insurance, agriculture, craft, various commercial services, and health and social services etc. Membership of social economy enterprises is much wider than the 11 million jobs, with estimates ranging as high as 160 million. Millions of members therefore depend on such enterprises in areas such as healthcare.

How shall we find 1 million users for the ICI architecture ?

The target population we need to reach first is the population that would most benefit from the ICI architecture, in particular its ability to be present on the Web simultaneously as service consumer or provider, employee or employer. While some large organisations and businesses might be sympathetic to the ICI architecture —a number of large organisations that are Member of Kantara are actively present in groups working on similar paths, like UMA WG User Access Managed Working Group led by a representative of PayPal— very few are agile enough to try-out novel ideas, even if they might lead to taking a leadership position.

This is why, we will focus most of our attention, without neglecting the other opportunities, to groups of organisations and people that would gain a quick win by exploiting the features of the ICI architecture.

The groups identified are

- Software developers, open source and proprietary
- Small and medium enterprises, in particular start-up
- Individuals looking for self-employment opportunities (nearly 50% of the European population

Building the community of ICI developers and service providers

In the early phase of the architecture development, the developers community, open source and commercial, interested in the ICI architecture will be invited to attend workshops and code-bash sessions where the first components of the architecture will be tested. The open source community will be also involved in the developments, initially through comments on the requirements and initial architecture, but rapidly in the development of the ICI components themselves —some of the developments will simply be an adaptation of existing components to ICI requirements or APIs.

There are already open source and commercial developers who are committed to an Identity Centric architecture, like Mahara and PebblePad, two ePortfolio platforms, one open source, the other commercial.

Call for tenders

In order to provide an incentive for developers to contribute to the developments or plug-in their developments to the ICI architecture, the project will organise a call for tenders. A reasonable financial prize will be offered to the laureates and should cover two main categories:

- direct contribution to the developments of open source components for the ICI architecture
- connecting proprietary services to the ICI architecture

The practice of financial rewards has already been used with success by the Kantara Initiative and a number of other initiatives regarding the exploitation open data for new services (e.g. Rennes, in France).

Approximately 10% of the budget has been earmarked for call for tenders.

Remark: there is a more fundamental incentive that should mobilise a number of developers: as sole traders, many should appreciate the value of an architecture where they will be able to establish trust relationships as service *user* as well as *provider* —e.g. be visible to prospects and find projects and partners.

The ICI partners are already in contact with a number of open source and developers communities. Details for reaching them and the organisation of the ICI Awards will be developed in the Dissemination and Adoption plan.

What we might achieve by the end of the project is establish a model for a *service app* where users will be able to connect their IC-Agents.

European citizens looking to be self-employed, self-employed and entrepreneurs

45% of European citizens are considering self-employment as an option, unfortunately, access to the information that would make this option a reality is difficult. Existing services like Linked-in or Monster.com are built on a paradox: hiding contact information in order to make a profit from the connection requests in order to pay for the service provided. But this is a fool's bargain, as the reality is that by privatising information, LinkedIn and alike hinders the potential for innovation that would be possible if data was accessible by the services of one's choice. There is no place in LinkedIn where it is possible to say: I want to create a business on business idea xyz, find me the people I need to create it, and just like with Google search, have a 'I feel lucky' button that will bring me the 5, 10 or 20 CVs I need to create this type of business. Such service can be build, but to make it efficient, i.e. to find in the whole Europe or world those 5 people, the service provider needs to have access to profiles of hundreds of millions of people —that are able to trust such service... This is what ICI can do, and the discovery mechanism is one of the first mechanisms that will be implemented in the architecture.

How shall we reach this population?

We will of course use existing social networks, such as LinkedIn, Viadeo, but also Facebook and the others. We will do so by organising groups to support the campaign **'free our data now**', calling for the separation between the storage of personal data from the services exploiting them. In parallel to this awareness raising campaign we will invite people to create an IC-Agent that will help them control of their data in LinkedIn, FaceBook etc. and explore the benefits of a unified interface and the ability to use the ICI architecture to establish trust relationships.

There are a number of people who are willing to leave Facebook and are looking for alternative solutions, like the Diaspora initiative in the USA and Turbulences in France. The ICI architecture will provide a framework for those wishing to be emancipated from existing social networks and be able exist on the Web without having to wear the Facebook or linked straightjacket — ICI will make it easy for people who wish to continue to stay on existing social networks, while exploring the benefits of ICI.

In order to make the connection of existing accounts to ICI, ICI can not just provide a trust architecture with no services. What the Open Data movement has taught us is that it is impossible to anticipate the depth and breadth of services developers have been able to create. To exploit developers ingenuity, the ICI project will use the ICI Awards as means to get innovative services.

'The ICI partners will co-design a set of small applications (applets) that will exploit the unique properties of the ICI architecture for the

- **100 million European citizens considering self-employment**
- **20 million of European citizens starting a business**
- **15 million running a new business**'

Our objective is that ICI will create the conditions that the 60 million EU citizens currently involved in entrepreneurial activity will grow significantly, in particular in the field of social enterprise that represents today 10% of all European businesses (2 million) and that a significant number will achieve their dream of self-employment.

"Free our data now!"

Free our data now! is the central campaign around which all the other dissemination activities are being organised. This campaign will be managed in cooperation with partners beyond the ICI partnership. A public site will present the outcomes of the campaign, invite people and

organisations to sign a petition, join seminars, workshops and bash-code parties where we will demonstrate how it is possible to regain control of our data using the ICI architecture.

A campaign committee will be created at the beginning of the project and the campaign will start M+3

IPR

The management of IPR in the project is based on *Kantara Initiative Intellectual Property Rights Policies*. What follows is only an extract of this policy. A more detailled version will be provided in annex of the consortium agreement.

Background IPR

The background IPR of individual partners will be safeguarded and made freely available for the project purposes.

It is possible that for testing purpose or for the implementation of a specific use case it will be necessary to exploit proprietary or non-royalty-free systems, as it is in the nature of ICI to propose an architecture open to all actors, exploiting open/proprietary free/paying technologies. In that case, the Partner will grant a royalty-free license to ICI partners for the duration of the project and for the purpose of the project only. Any exploitation beyond the ICI project of such license will be in violation of the agreement.

Foreground IPR

Unless stated otherwise, by default, ICI partners are guaranteed to be *free to implement and use* the outcomes of the project. In particular, there will be *royalty-free* patent licensing for all those that contributed to the technology as well as the consortium members. It will be possible to extend the license outside the consortium, to third parties wishing to implement and use the ICI architecture.

Unless produced by a single partner, all IPR generated in the course of the ICI project will be considered as having joint ownership. All joint ownership foreground that has potential industrial or commercial application will be protected by means of IP rights such as patents, designs. When produced by a single partner, foreground IPR will be solely owned by the partner who has developed it within the project. This will encourage partners to bring appropriate background IPR to advance the project quickly, whilst enabling core developers to exploit their work outside the project. In other words, it is not because a background IPR is modified by the project that the status of the IPR changes: it remains to its initial owner.

Each ICI Partner shall retain ownership (including, but not limited to, the right to publish or distribute without any obligation of confidentiality) of any of its Licensed Materials that such Participant offers for use in the development of or for inclusion in any output of the ICI project, as well as of such Participant's implementations of the ICI architecture. Where two or more Partners jointly develop Licensed Materials or intellectual property appurtenant thereto (such as copyrights or patent rights) as part of their work in ICI, such Participants shall jointly own any such Licensed Materials and intellectual property, without any obligation of accounting to each other or to the other Participants.

To the extent to which an ICI deliverable constitutes a copyrightable work distinct from any Participant's copyright interests in Licensed Materials included as part of such output or from which they are derived, the copyright of the outputs of a work package shall be transferred to the Kantara Initiative.

Patents will be applied for on a joint basis through organisations like Kantara or the Oasis Group in order to benefit from a legal framework protecting IPR from attempts of privatisation of common goods.

Copyright: unless agreed otherwise, all public documents will be made available under Creative Commons Attribution Share Alike option

Licensing: Each joint owner of the foreground IPR is free to grant non-exclusive licenses to third parties. As long as licenses are non-exclusive, there is no restriction on the type and number of licenses.

Right to sublicense: licensees have right to sublicense, subject to the terms of their license. Sublicensees also have right to sublicense, subject to the original license terms.

Non-exclusivity: The license granted shall be non-exclusive and with condition that any sub-license shall also be non-exclusive.

Part B. B.4 Ethical Issues

The ICI project will involve two ethical issues:

- **Informed consent**: Does the proposal involve Human data collection? Yes *
- **Privacy**: Does the proposal involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)? Yes

In fact, ICI is working on providing the means for all individuals to improve the level of privacy and their ability to give an informed consent for the exploitation of their personal data. The whole architecture is focused on the opportunity to 'open' access to personal data while improving the level of security, privacy and anonymity.

A privacy officer will be appointed and report to the coordinator to ensure that privacy policies are being properly implemented and deal with the complaints when they emerge.

Informed consent compliance

Informed consent is a phrase indicating that the consent a person gives meets certain minimum standards. In the case of ICI, do the criteria related to the collection of personal data meet those standards?

The goal of ICI is precisely to give individuals the means to give an informed consent in the exploitation of their personal data. ICI as such has no interest in the data collected, but in the ability of the person to control who has access to what and under what conditions.

Nevertheless, as it is a pilot project it is not possible to be 100% sure that the system will have no flaws and will not be hacked successfully by a malicious party. So the consent should address the risks inherent to the storage of data online and the fact that this is a project under development. We will have to ensure that the information given is accurate, understandable by all readers and really reflects a voluntary decision.

NB: ICI does not 'collect' data, but participants 'publish' their personal profile and it is the services that 'collect' data in order to provide a service.

Elements of the consent form

when signing-up for creating an IC-Agent, users will be asked to state that they have read and agreed with the information relative to the risks linked to the project.

the list of all major risks will be clearly presented and made explicit, including with the use of graphics, on the first page, while more detailed explanations will be made available in the following pages.

participants will be immediately notified by email in case of a problem has occurred

Privacy compliance

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data lays down a series of rights.

It is precisely the mission of ICI improve privacy to a level never experienced before. The users will the the co-designers and implementors of this new privacy and trust architecture.

The improvement of privacy rights are:

The right of access to own personal data —all data will be under full control of the person

The rights of erasure, blocking or rectification of the data, which do not comply with the provisions of the Directive, are incomplete or inaccurate —all data being under the person's control, it is easy for her to rectify any data

The right to be informed of all relevant details relating to the data processing and the rights granted to self -- the dashboard provides the person with an accurate view of where data is exploited and how.

The right to a judicial remedy for any breach of the above mentioned rights — the person will have the means to collect evidence of any wrongdoing, and present this evidence in court.

The person creating an IC-Agent will be the only one deciding who can see what. Even in the case of a sysadmin trying to access personal data, the IC-Agent user will be notified and will have to give consent for accessing data —a breaking the glass procedure, known to the owner, will be available in case of extreme circumstances.

The main foreseen problems with privacy are not linked to the architecture itself but with the risks inherent with projects under development and pilots —and unforeseen problems that require contingency plans!

How will ICI ensure data protection & confidentiality?

The objective of ICI is precisely to ensure data protection and confidentiality, and this will be achieved, partly, by associating all the stakeholders to its definition and governance.

The main parties that will have to deal with private data during the pilot phase (to be distinguish with the risks in a *normal* deployment):

Who	Identified risk	Impact	Probability
IC-Agent owner	disclose involuntarily private data to third parties	low to high	medium
software developers	reveal private data accessed when debugging a component of the architecture	low	low
system administrators	access to private data as *super user*	medium to high	low
service provider	collecting data against its owner's will	medium to high	low
search engines, metadata harvesters	providing non anonymised data to third parties or sets of anonymised data that can be desanonymised	low to high	low to medium
hacker	collecting data against its owner's will	high	medium to high

All the partners involved in the ICI project are highly sensitive to privacy issues and will take the necessary steps to respect privacy. Systems will be in place so that sysadmins and developers will not have access to personal data in a human readable format —except when required, e.g. to debug encoding mechanisms. Service providers and developers working outside of the direct partnership will have to sign a charter by which they agree to do their best to enforce the policies defined by users. They will also agree not to exploit a system flaw and to report it if they find one. As all the actors will interact through IC-Agents, it will be possible for a privacy officer to inspect an audit trail.

For the end-users, the dashboard of the IC-Agent will provide an indicator on the level of security and trust provided by the ICI architecture. With a low level of security (low by ICI standards, means in fact high by current standards!) users will be invited to only store non-sensitive data. As the level of security will increase, the indicator will tell users that it is safer to store other types of personal data.

Security

ICI will use state-of-the-art technologies for secure storage, delivery and access management of personal information: redundant storage, saves, databases, firewalls, network security, encryption, authentication, authorisation etc.

One of the strong points of ICI, which is the discovery mechanism, i.e. the ability to find a specific profile, will be studied in great detail in order to avoid the risk of disanonymisation, which is relatively trivial to perform in exploiting sets of anonymised data. As users will have

the same tools as service providers, we will be able to use their collective intelligence to establish best practices — and best technologies.

As a research project, we will produce reports and statistics on the user profiles and behaviour in order to inform current developments and future research. All these reports will be produced using anonymous data and users will have the right to refuse to have their IC-Agent harvested for specific or all types of data. In that case we will indicate the number of harvested and non-harvested IC-Agents.

If in the course of the project there is a need to poll users, the individual results of the poll will stay in the IC-Agent, so the responses could be used by other actors (trusted by the users). In order to collect the data, the users will have to accept as *trusted service* the *ICI polling service*. The individual responses will be kept in the 'personal locker' of the respondents (if they wish so, if not they can erase the data), while the synthesis of the responses will be stored in ICI locker with no possibility to trace back the responses to the respondents.

Ethical issue table

		Page
Informed Consent		
• Does the proposal involve children?	no	
• Does the proposal involve patients or persons not able to give consent?	no	
• Does the proposal involve adult healthy volunteers?	no	
• Does the proposal involve Human Genetic Material?	no	
• Does the proposal involve Human biological samples?	no	
• Does the proposal involve Human data collection?	yes	
Research on Human embryo/foetus		
• Does the proposal involve Human Embryos?	no	
• Does the proposal involve Human Foetal Tissue /Cells?	no	
• Does the proposal involve Human Embryonic Stem Cells?	no	
Privacy		
• Does the proposal involve processing of genetic information or personal data (eg. health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)	no	
• Does the proposal involve tracking the location or observation of people?	no	
Research on Animals		
• Does the proposal involve research on animals?	no	
• Are those animals transgenic small laboratory animals? • Are those animals transgenic farm animals?	no	
• Are those animals cloned farm animals?	no	
• Are those animals non-human primates?	no	
Research Involving Developing Countries		
• Use of local resources (genetic, animal, plant etc)	no	
• Benefit to local community (capacity building i.e. access to healthcare, education etc)	no	
Dual Use		
• Research having direct military application	no	
• Research having the potential for terrorist abuse	no	
ICT Implants		
• Does the proposal involve clinical trials of ICT implants?	no	

I CONFIRM THAT NONE OF THE ABOVE ISSUES APPLY TO MY PROPOSAL

Annex

References & Bibliography

[ATE2009] Ates, M.: Digital Identities, User Centric and Privacy-Respectful Cross-Organizational Identity Management, PhD thesis, Université de Lyon, SATIN Team, DIOM Laboratory, Telecom Saint-Etienne, University of Saint-Etienne, 2009

[BHA2006] Bhargav-Spantzel, A., Camenisch, J., Gross, T., Sommer, D., User centricity: a taxonomy and open issues. In: DIM '06: Proceedings of the second ACM workshop on Digital identity management, New York, NY, USA, ACM, 1–10, 2010

[BRA2000] Brands, S.A., Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy, MIT Press, Cambridge, MA, USA, 2000

[CAH2010] Cahill C.P., Liberty ID-WSF Advanced Client Technologies Overview, Liberty Alliance Project, 2007

[CAM2002] Camenisch, J., Lysyanskaya, A., A signature scheme with efficient protocols, International Conference on Security in Communication Networks, Lecture Notes in Computer

Science, Volume 2576, 268–289,2002

[CAN2005] Cantor S., Metadata for the OASIS Security Assertion Markup Language (SAML) v2.0, OASIS, 2005

[GID91] Giddens A., Modernity and Self-Identity: Self and Society in the Late Modern Age, Cambridge Polity Press, 1991

[LAS2008] Lasica J.D., Identity in the Age of Cloud Computing: The next-generation Internet's impact on business, governance and social interaction, ASPEN Institute, 2008

[LAW2009a] Lawrence K., Kaler C., Web Services Trust Language (WS-Trust) v1.4, OASIS, 2009

[LAW2009b] Lawrence K., Kaler C., Web Services Security Policy Language (WS-SecurityPolicy) v1.3, OASIS, 2009

[MAC2006] MacGregor W., Dutcher W., Khan J., An ontology of Identity Credentials - Part 1: Background and Formulation, National Institute of Standards and Technology - U.S. Department of Commerce, 2006

[MAL2009] Maler E., Security Assertion Markup Language v2.0 - Technical Overview, OASIS, 2006

[NAN2008] Nanda A., Jones M.B., Identity Selector Interoperability Profile V1.5, Microsoft Corporation, 2008

[PAQ2010] Paquin, C., U-prove technology integration into the identity metasystem v1.0. Technical report (2010)

[SIE2010] Siegel D., The Power of Pull, Kindle Edition, 2010

[TER2007] Ter Beek M., Moiso C., Petrocchi M.,, Towards Security Analyses of an Identity Federation Protocol for Web Services in Convergent Networks, AICT'07 - Proceedings of the Third Advanced International Conference on Telecommunications, 2007

[TOU2007] Tourzan J., Koga Y., Liberty ID-WSF Web Services Framework Overview, Liberty Alliance Project, 2007

Use cases

For each use case we elicit a need, a possible scenario using the ICI architecture and the unique benefits of the ICI architecture

Use case 1: employment mobility in Europe

In the current architecture of employment services, a person has to duplicate personal data in a number of data silos called public employment agencies or job boards. Moreover, registration to employment services usually happens during a difficult period for the individual (while he/she might have been found earlier by another employer).

Scenario

1. A person makes her profile available on her IC-Agent with the status *make me an offer*
2. A discovery service finds a match with an employer's demand
3. Both IC-Agents are notified -- the prospective employee remains anonymous
4. Employer selects an short-list to organise interview at a distance: notify with a list of time frames

Each prospective employee sends their time frames to the employers IC-Agent that organises the online meetings by solving the constraints

Of course, the IC-Agent of the employer could be that of the employment agency or of a broker, and it will be the solution if they provide real added value service.

ICI USP

Employment data is in one place and one place only, and can be discovered at anytime by any trusted discovery service while preserving complete anonymity.

Use case 2: Self employment

According to the 2009 Eurobarometer Survey on Entrepreneurship, 45% of all Europeans would like to be self-employed while 49% would prefer working as an employee. The objective of this use case it to explore, how the creation of an IC-Agent can encourage European citizens to act out their desire for autonomy and contribute to the growth of social capital. In France, since the adoption of the new status of 'auto-entrepreneur' in 2009, 500,000 people have decided to become self-employed —a large part of this figure is represented by people that would have created a business, even without this new status.

Scenario

1. A person adds to her status *make me an offer* the status *looking for clients*
2. A discovery service finds a match with a potential client with a need for a specific service the person can offer
3. Both IC-Agents are notified -- parties remain anonymous
4. Prospective client selects a short-list of service providers asking for a quote and the right to access testimonials
5. Prospective client access testimonials and can verify that they come from people or organisations she can trust
6. Prospective service providers can access information that their client has disclosed to them to build a relevant offer

ICI USP

Parties can discover each other and can disclose incrementally information about themselves while preserving complete anonymity —if they wish so.

Use case 3: Business creation

In the report Entrepreneurship in the EU and beyond (2009) the European Commission reports that four percent (20 million) of EU 501 million citizens were currently in the embryonic phase, i.e. taking the necessary steps to start up a business, 3% (15 millions) were running a new business and 6% (30 million) were running an established business. In total, 12% (60,1 million) of EU citizens were currently involved in entrepreneurial activity.

Every European company should be able to answer to public calls published on-line providing digital certified data. For this, a trust path must be found between state administrations publishing offers and the certifiers of data of the many countries. A discovery system is necessary to establish trust links through pre-existing trust relationships. For instance, two main state administrations would be trust-linked. Through this link, two sub-organisations should be able to seamlessly discover each other, to agree on legal policies and to establish dynamically a trust relationship.

Scenario

- A person adds to her status *Business in creation*.
- A discovery service specialised in business creation finds a match with a potential investors, partners, employees and clients
- Prospective entrepreneur clicks on "I feel lucky" and receives the CVs of the 10 people, that have indicated in their profile that they are willing to participate in a business creation, the VC the most likely to fund her business, and over all, a list of prospective clients -anonymous but with information useful to build a relevant marketing message

She decides to move forward, create a business in the country with the most potential clients. She does so by going to her local chamber of commerce that will establish a trust relationship with the agency in the target country after paying a subscription fee to the business creation service, she can refine the business proposal by simulating the impact of the different offers on the clients. She can also pole prospective clients —those who have said so in their profile.

ICI USP

In one click the prospective entrepreneur can have a global view on the people who can contribute to the success of her business: partners, venture capitalists, clients, future employees.

Use case 4: 21st century worker

This use case is the synthesis of the three previous ones as, in the 21st century, many knowledge workers (but not only them) will not only have multiple jobs at different times of their lives, but in parallel. And one person might be working as employee for 50% of his/her time, 30% as independent consultant and 20% as social entrepreneur.

Employment services based on the exploitation of personal data store/proxy will allow an individual to simultaneously:

- find potential employers —through brokers or directly
- find potential clients —through brokers or directly
- find potential partners to create/run a business

ICI USP

With an Identity Centric Internet, job seekers do not have to register to multiple services but it is the services that subscribe to one's personal data. Crawling engines collect metadata from all personal data stores in order to feed employment related services. In the ICI architecture, which is a symmetric architecture, individuals can act as potential employers and service providers. The crawling engines build indexes that help individuals to find clients and partners, not just a potential employer.

ICI creates the conditions for taking a global and in depth transformation of employment services in line with the 21st century economy by empowering people to control their lifelong, agile and mobile career.

Use case 5: re-localisation of the economy

When leaving in France and go to the local supermarket to buy garlic, most of the time it will come from China, Egypt or Argentina. Yet, France is the country of garlic (for the Brits, at least!). There is a global movement to re-localise the economy as a means to reduce our carbon imprint and revive local economies and communities. Now imagine that every producer of goods, commercial or not (someone might have a cherry tree that needs harvesting) where all the assets are being described, broker services (another name for discovery services) could offer to organise local commercial and non-commercial exchanges —even use local, non-monetary currencies akin to WIR, an alternative to the banking system...

Scenario

- producers of goods, commercial or not, make the description of their production available through their IC-Agents
- a local cooperative business uses this information to create fresh food baskets that are delivered in the local area
- a social enterprise uses local voluntary workforce to collect unsold and non harvested goods to supply a food bank in the next big town

ICI USP

By making the information available, so it can be harvested by discovery engines, anybody can decide to organise a brokerage to reduce waste and exploit intelligently local resources

Use case 6: Vendor Relationship Management

This use case is a generalisation of the previous one where any service or good provider, instead of keeping their own customer relationship system (CRM) believe that it is better for them, and their clients, to rest on data records maintained by their clients and prospects.

Use case 7: Social networks

A significant proportion of the population of Europe belongs to multiple social networks. The term "belong" is accurate here, since in the actual architecture, for each network, a single organisation hosts the personal data, the links between people, ensure the contact between unknown people and provide a graphical interface. According to the ICI vision, each of these roles should be split across independent entities, just like production and distribution of electricity is being separated.

This division will allow individuals to:

- choose where to host their data, independently from services provider
- use multiple and innovative social network service providers without having to duplicate their personal data

and service providers

- to offer new services directly to prospects and clients without having to be dependent on de facto monopolies or organisations with dominant positions
- enter into a new type of relationship with users, like in vendor relationship management.

Every person will have the ability to create their on-line personal data store and will be able to control access to its own data and delegate some of the rights to chosen members of his/her personal networks. The user will allow trusted services to create anonymous indexes / directories / mailing lists so people sharing similar interests could communicate while preserving anonymity. The personal dashboard will provide individuals with a global

perspective on how their personal data is being exploited and adjust access and distribution rules and policies.

In the ICI architecture, the need for organisations to provide the right to rectify one's personal data is reduced as, personal data is by default on the personal data store/proxy of the individual, the organisation owning simply a pointer and access rights to the personal store/ proxy. So the deletion of personal data from a service provider becomes the suppression of the access rights to the personal repository.

The ICI architecture also reduces the risks associated with the transmission to a non-trusted party: Let's say that A trusts B, B trusts X and A distrusts anybody that is not B, C or D. Then, if B tries to transfer to X data received from A (he can always transfer data 'about' A without A knowing it), then the policy enforcement point will deny the transmission of the data, and if X receives a pointer to data in A's repository, A policy enforcement point will deny access to X.

As each pointer pointing to the same attribute is different (in order to reduce possible correlation across personal proxies) if A gives access to a set of data to B, C and D, then the PEP will be able to: 1) know who tries to access A' data: in a trusted network readers of one's data must be identified 2) know who is responsible for the leak (voluntary or as the result of hacking): the pointer to A repository has B, D or D's signature 3) if necessary deny that this data can be associated to him/her (e.g. the contents of a private conversation with B)

The ICI architecture will do more than just enforce privacy: thanks to the trust network, it will create the conditions for effective intimacy, i.e. the ability to share attributes within a personal circle of trust, while not have to worrying for the risk of disclosion beyond the personal circle of trust —and if disclosion happens, provide the ability to deny access to data source, and cast a doubt on the claim made by the disclosing party.

Use case 8: Demand Chain Management (DCM) and Demand-Driven Supply Network (DDSN)

Demand chain management is to *supply chain management* what VRM is to CRM —it can be understood as the systematisation of VRM across all IC-Agents. It is about the management of upstream and downstream relationships between suppliers and customers based on *customer pull*; it is a*demand driven network* —more than a *chain*. Also referred to as *Demand-Driven Supply Network (DDSN), it is a supply chain management method that involves building supply chains in response to demand signals. The main force of DDSN is that it is driven by customers demand using pull techniques. It gives DDSN market opportunities to share more information and to collaborate with others in the supply chain.*

DCM goes from the collaboration on the specification of new services to the procurement of specific products and services along the supply/demand chain. DCM creates the conditions for active collaboration around the specification, design, implementation and delivery phases. In DCM scenarios networks of employees are created across organisational boundaries through the negotiation and sharing of data in order to achieve the project goals of a demand elicited by the DDSN.

As with VRM, the conditions of existence of DDSN require the ability to harvest metadata from an extremely wide range of prospective customers and participants in the demand chain / network. Such aggregation is only possible if all the members of the demand chain / network can have their demand *data be harvested by DCM services. The ICI architecture creates the conditions (trust) for such harvesting which is the foundation on which DDSN can exist.*

In reality, a DDSN cannot be a single application or service, but the result of the cooperation among multiple agents that are part of multiple networks. Current approaches to collaboration, data management and resource sharing (access to systems) that are done on a step by step basis and a one to one basis cannot create the conditions for DDSN to emerge. A DDSN is complex *(which is different from* complicated*) dynamic system exploiting the outcomes of multiple independent interactions across multiple independent actors.*

The ICI project will address how business to business collaborations can be supported within a DDSN. The ICI approach will tackle the establishment of short term collaborations between

partners in projects by allowing a greater automation of policy negotiation around resource and data sharing. The ICI approach with give organisations a seamless way to establish and monitor agreements about the sharing of resources with individuals from other organisations within specific terms of short term projects.

Scenario

- *a DDSN agent harvests metadata from IC-Agents on a territory, e.g. a district, to elicit a potential supply/demand chain for fresh local products —data is collected from fidelity card records, declared tastes an interests, dietary requirements etc. of potential clients, local stores' lists of suppliers, local farmers and residents with local gardens orchards etc., trucks going through the local area and the opportunity to carry load of goods demanded by local citizens, etc.*
- *all actors in the DDSN are notified of the opportunities —a more sophisticated software would provide information on the opportunities to reduce carbon emission, etc. — and can act on the basis of the information received*
- *at an initial stage, one could expect that the dissemination of this information could create a number of direct relationships across agents and the emergence of local brokerage systems, like the creation of a cooperative.*

ICI USP

By making data searchable, discoverable, ICI creates the conditions for human ingenuity to innovate with new services, contribute to the re-localisation of the economy while encouraging new forms of global business through the chain of interaction across local DDSN —DDSN are like fractal functions, sharing the same characteristics at local and global levels.

Use case 9: Ambient intelligence and pervasive networks of the Future Internet

As mobile and embedded computing systems increasingly pervade our environment, more and more information and content is available throughout our daily surroundings. Pervasive appliances and applications offer new sets of technical and business challenges and opportunities: they are at the same time a major threat to privacy.

Threats: findings by Philippe Golle and Kurt Partridge of PARC (Palo Alto Research Center), demonstrate how anonymized data collected from GPS-enabled devices may not be as anonymous as one may think: knowing someone's general home and work locations can be enough to identify an individual uniquely... The consequence is that it is important to ensure, by default, a high level of entropy on collected data, so anonymity has a better chance to be preserved —entropy that could be reduced after a break glass' policy has been activated.

Opportunities: the combination of GPS-enabled devices and data collected from personal calendars can provide services to reduce carbon emissions, for example by making care-sharing offers or small packet transports (courier) to people, without having to register to a special website. Health monitoring devices could alert neighbours at the same time they alert emergency services by finding the closest person and more likely to provide helpful services.

Opportunities created by enabling mobile and ambient devices to serve as intelligent interfaces to our physical surroundings will only grow within a trusted network where computing environments are transparent to users, starting by providing each user with a personal data store hosting personal (meta) data and attach policies to access it.

Scenario

- Estelle has a studio in Paris she rents on a short time basis. Access to the studio is provided by typing in a changing code that is sent to the client' mobile phone when arriving next to the studio.
- Someone looking for room is notified that Estelle's studio is available, agrees to the terms and conditions, pays online and goes to the studio.

- the cleaning person is notified of the leaving day to clean the room for prospective new clients —access is granted by RFID
- the client arrives next to the studio where he receives the access code to enter the studio —like that, someone can try all possible number combinations without being able to access the studio, as the keypad is only functional when the person is in the vicinity of the studio with a functioning mobile phone
- the second day, the client has forgotten his mobile phone inside the studio, calls a number printed under the access keypad from the closest open café, gives his credential and receives a new code valid for 5 minutes.
- the client takes a shower and after 30 minutes of running the water, the studio monitoring system calls his phone to check that there is nothing wrong. Then calls a neighbour to ask checking if there is a problem. As the client is over 80 years old and has an history of cardiac problems, the neighbour can enter to check further in order to call for emergency services if necessary

ICI USP

By ensuring that all data collected from pervasive appliances, applications and services are fully under user's control, a number of services could be developed to improve the quality of services, create new ones, reduce time to action of emergency services, etc. There is no limit to what can be achieved if we can exist and operate in a fully trusted environment.

Use case 10: "Break glass" policy

Sensor networks can monitor, anonymously, people's health constants in different public and private places (e.g. patterns in home water consumption is one of the best indicators of the state of an elderly or disabled person). In case an anomaly is discovered in the pattern of collected data, emergency services would be notified and the agent in charge would have access to the medical record which is normally only accessible by the patient's GP and the hospital's service where he is treated. Location of the patient would be made available to the emergency team and if a healthcare professional or trained rescuer happens to be in the neighbourhood (*is there a doctor in the assistance* policy) , she would be notified and would receive indications on the patient's condition.

Such *break glass* policy would be also useful in case of missing person, to provide information to all the actors that might be able to have spotted the person based on their location. This policy should be fully under user control as it is perfectly legitimate for a person to decide to *disappear*.

anonymity would be revoked and the access to the personal medical record granted because all the different components are discovered and dynamically trusted; in particular the PDS would dynamically trust and authorise the access because the alert comes from a certified sensor network.

Scenario

As in the previous use case, abnormal water pattern consumption indicates that a person might be in trouble. Helpers, family, neighbours, healthcare professionals could be notified according to the level of risk detected.

ICI USP

The user IC-Agent would be able to monitor accesses in real time or post-facto when the person recovers.

Use case 11: eVoting

In this use-case, we do not address the issue of voting for *regular* elections, but the ability for citizens to organise referendums on subjects of their choice with the constituency of their choices with *good enough* results, i.e. minimising the risks of someone voting more than once or not being part of the chosen constituency.

Scenario

There is a plan to build new high speed rail track. One of the people affected by this new track wants to organise a poll with all the people within a 60 km distance of the track, in order to include those that might have to move as well as those who could benefit from this new service.

Using a search engine she gets the information that 456,322 people match the criteria. With the result of the query, she also receives a handle (a simple identifier) she can use to send a message and a link to the matching profiles to a poll she has created.

In order to reduce system abuse, in order to contact anonymously the 456,322 found in the query through the handle, she is required to get the approval of at least 1,000 people from her community. She does it by acting in the *real* world, asking people to support the poll by adding their name in the *authorise the poll* section. When 1,000 have done so, the poll can become active.

A number of the people contacted send the link to some of their friends in order to influence the vote, but they cannot access the pole as the link is only valid if the voter is part of the community created by the query. A person tries to vote multiple times, but only one vote is counted (a person has the right to change her vote until the poll is closed) as each voter has a unique token to cast a vote.

The organiser of the poll having authorised to see the results in real time, and people to give comments, people can decide to change their vote based on the evolution of the results and the comments.

ICI USP

Providing individuals with a tangible representation on the Internet will create new opportunities for growing in an open society.

Support letter from the Kantara Initiative

November 29, 2010

Partnership with Entr'ouvert toward ICI Project

Dear ICI Representatives,

The Kantara Initiative is pleased to partner with our Member Entr'ouvert in meeting the challenges of addressing the Next Generation of the Internet. The Kantara Initiative has in its mission to collaborate with its members and other organizations to grow markets for Federation systems, to harmonize existing solutions and to foster open source solutions.

The Kantara Initiative infrastructure is specifically focused to enable approved deliverables to be channeled and will make them available world-wide, non-exclusive, and royalty-free under our Intellectual Property Rights (IPR) Option: Creative Commons Share-Alike Attribution. Our goal in collaboration is to promote strong adoption of multi-national project results while ensuring that work develops in a non-profit standards development organization with broad community and industry input.

In our partnership Entr'ouvert would serve as a proxy on behalf of Kantara Initiative while we structure our European based group or chapter. We expect to formalize the partnership toward these projects in the coming weeks.

While the Kantara Initiative is a program of the IEEE ISTO we are currently building processes which will facilitate the creation of jurisdiction based "Chapters" where such "Chapter" organizations wish to form. We expect that there will be commonalities with this work and other Kantara Initiative work groups. The potential overlap with many Kantara Initiative groups will enable broad input toward the success of these projects.

In our first year of operations we have already achieved many milestones which are listed on the following sheets. If you have any questions regarding the Kantara Initiative please don't hesitate to contact me – joni@kantarainitiative.

Best Regards,

Joni Brennan
Managing Director,
Kantara Initiative

445 HOES LANE, PISCATAWAY, NJ 08854 USA
Phone: +1 (732) 465-5817 Email: staff@kantarainitiative.org
WWW.KANTARAINITIATIVE.ORG

Since its launch in mid-2009 Kantara Initiative has:

- formed 15+ Work and Discussion Groups
- been Approved as a US Government Trust Framework Provider
- launched an Assurance Certification and Accreditation Programme
- published Recommendations and Reports
- hosted successful meetings in Europe and North America

15+ Work and Discussion Groups have formed (and more continue to form). Some highlights for more active Work and Discussion Groups are below.

Group	Charter	IPR Policy Option	Mail	Calendar
eGovernment WG The eGov work group focuses on international issues particularly focused on governments. Multi-national participants contribute to this group from Asia, European Union and North America.	charter	Creative Commons Attribution-Share Alike	List	calendar
Federation Interoperability WG The Federation Interoperability WG focuses on the tools that will link federations so they can share meta-data securely at varying levels of assurance.	charter	Creative Commons Attribution-Share Alike	List	calendar
Health Identity Assurance WG This group focuses purely on issues pertaining to health care and health care systems. There is special focus on patient privacy and secured data exchange around patient records and information.	charter	Creative Commons Attribution-Share Alike	List	calendar
Identity Assurance This group manages the Identity Assurance Framework, its components and profiles. This group is at the forefront of managing the documentation that the Kantara Initiative Assurance Accreditation and Certification Programmes abide by.	charter	Patent Copyright and Rand	List	calendar
ID-WSF Evolution WG This group manages the ID-WSF specification set in its matured lifecycle.	charter	Patent Copyright and Rand	List	calendar
Information Sharing WG This group focuses on contract models and scenarios where information must be shared. They are developing contracts which would provide or outline details around how and with whom information is shared.	charter	Patent Copyright and Rand	List	calendar
Interoperability WG Interoperability WG directly supports the technical interoperability certification programme developing test plans and documentation.	charter	Patent Copyright and Rand	List	calendar
Privacy and Public Policy WG Also known as P3WG, this group is under taking the development of a Privacy Framework. With input from multi-national communities and industry this Framework would be adopted by the Kantara Initiative Assurance Certification program for testing.	charter	Creative Commons Attribution-Share Alike	List	calendar
Telecommunications Identity WG With strong participation from Asia and Europe this work group focuses on issues related to Telecommunications and deployment of federation in Telecommunications systems.	charter	Patent Copyright and Rand	List	calendar
Universal Login Experience WG This group is building mock-ups for a method which would enable all users to have the same login experience regardless of Identity Providers or Management Systems.	charter	Patent Copyright and Rand	List	calendar
User Managed Access WG This group is defining how a User would be empowered to manage access to their information and records.	charter	Patent Copyright and Rand	List	calendar
Business Cases for Trusted Federation DG * This very newly formed group will discuss business cases for federation that uses Trust Frameworks (Trusted Federation). It will explore successes and failures with hopes to identify multiple clear business cases for Trusted Federation.	charter	Creative Commons Attribution-Share Alike	Under Construction	