SEVENTH FRAMEWORK PROGRAMME

STRATEGIC RESEARCH AGENDA

EDITORS
Amardeo Sarma, Daan Velthausz, Arthur Leijtens

CONTRIBUTORS
Ronny Bjones, Caspar Bowden, Sonja Buchegger, Stefan Bumerl, Jacques Bus, Hugo Jonker, Jens Fromm, Jac Goorden, Mathieu Goudsmits, Pieter Hartel, Sascha Hauke, Mireille Hildebrandt, Jaap-Henk Hoepman, Gus Hosein, Leena Kuusniemi, Pia Kristine Lang, Xavier Larduinat, Petteri Leiviskä, Víctor Izquierdo Loyola, Sead Muftic, Jean-Pierre Nordvik Aljosa, Pasic Milan Petkovic, Reinhard Posch, Steve Purser, Peter Racsko, Kai Rannenberg, Mark Ryan Jon Shamah, Corinne Sieux, Andrew Tokmakoff, Ross Tsagalidis, Claire Vishik

TDL | Trust in Digital Life

DATE
March 26th 2012

Executive Summary

As in the real world, establishing trust and trustworthiness in digital life is essential to release the full potential of an information-based economy. At the same time, protecting privacy and other fundamental human rights of future citizens must apply as much in the digital world as it does in the physical world. While these aspects need to be addressed and even guaranteed by lawmakers within an improved legal framework, technical solutions should enable more than just the legal minimum. Beyond only enabling what is required by law, technology can add more capabilities for trust and privacy, possibly coupled with consequences on transparency, cost and business models. One concrete approach whose potential should be examined is the *transparent payment for trust* scheme towards a fair treatment of privacy and trust needs.

The technological baseline has become a fast moving target, reflecting a changing environment that brings in completely new players and interests, while citizens and policy makers are becoming aware of new threats. This calls for new approaches combining technological options with legal requirements, societal needs and business opportunities to handle and manage trust in this changing world.

One significant change in the technological baseline is the move to the Cloud and “things” attached to the Cloud, which has created major new *research and innovation challenges*. This document identifies the Trust in Digital Life[1] community’s view on the innovations and research required to address these challenges. It also assesses the *impact* that such innovation and research could have on business and society and how this matches European policy making and values. The document addresses the expected *economic and social impact* and defines a generic portfolio of *possible projects*.

Five application domains will guide us, providing complementary requirements on privacy and trust, understanding that privacy may be needed for trust. These are:

- Privacy of individuals in online life
- Logistics and Transport
- Medical environments and healthcare
- Financial environments and financial transactions
- Telecommunication

The document concludes by providing recommendations to stakeholders in government, legislation, industry and research.

[1] The Trust in Digital Life community is an open innovation community with leading industry partners, institutes and user organisations with the goal to accelerate the adoption rate of trustworthy ICT by

Contents

1. Introduction and Context

This document addresses central challenges around establishing trust in digital life and moving towards a vibrant future economy that protects privacy and other fundamental human rights of citizens in society. The relevant timeframe is horizon 2020 of the European Union. The backdrop compared to FP7 is:

- Trust erosion caused by both opportunistic and organized cybercrime, with increasing impact and frequency, as well as privacy threats to citizens and society with numerous incidents of breaches of trust and privacy, all leading to more visibility of trust, security and privacy problems,
- Higher level of awareness of citizens and policy makers related to privacy and trust, which is reflected in new legal initiatives, such as in EU policy making,
- At the same time, paradoxically, a shift of social and personal behaviour, in which things are accepted online that we would never accept in a physical world,
- New technologies and solutions which are constantly changing the technological baseline, with the move towards cloud computing and the Internet of Things introducing new challenges to security and privacy,
- The changing technological and business environment brings in completely new players, such as many more small providers and so-called ‘pro-sumers’ requiring new “broker” roles, with new interests beyond monetary rewards, such as social rewards, that have to be taken into consideration.

Using a simple definition[2], trust comprises the intention to accept vulnerability based on positive expectations of the intentions or behaviours of another. In practice, trust often boils down to users of services who evaluate the expected benefits against the perceived risk, noting that this may not necessarily correspond with the actual benefit and risk. The TDL community mainly addresses the potential vulnerability through the exposure of the parties and their perceived behaviour rather than risks that the use of the services may have themselves, which may vary considerably. Within this context of vulnerability, we divide risk into two categories – risk associated with security and risk associated with privacy, as the economic models for security and privacy are different. Trust also needs to be evaluated according to its constituent components accountability, transparency, anonymity and traceability.

[2] based upon D. M. Rousseau, B. S. Sim, R. S. Burt, and C. Camerer. Not so different after all: A Cross-Discipline view of trust. Academy of Management Review, 23(3):393-404, 1998.

Trust is involved when interacting with various elements of the digital world. Devices that should be safe, service and product providers should guarantee sufficient protection, and actions should be transparent and not breach privacy. There should also be safeguards against purposeful or accidental misuse by governments, oneself, malware and in general 3rd parties that may be involved, perhaps even without legitimate parties knowing. In order to ensure trust, the complex effects of the possible combinations of these elements should be kept in mind, including emergent effects beyond mechanical combinations.

Trust has consistently been identified by organisations and industry leaders as a major enabler of digital life[3], the lack of which could be a show-stopper. For example, services requiring financial transactions in a cloud-based environment with a number of providers require a particularly high level of trust because of the assets involved. Both a user (for payment) and a start-up service provider (for delivery of services) would need to understand each other's trustworthiness. Beyond this, trust could play an important role when other real or perceived assets are concerned, including one's own private data. The level of perceived trust may make the difference between whether a contact between two parties is successfully made, both in the private and commercial arena. Making trust transparent and believable in the digital domain is essential.

Ensuring trust in the future digital life with the advancement of cloud computing and the Internet of Things (IoT) leads us to major new *research and innovation challenges* to be addressed, both to achieve technological and scientific excellence as well as to enable business and global prosperity. We identify the *impact* that such research could have on business and society and indicate how this matches European policy-making and values. The expected *economic and social impact* will help define this strategic research agenda. We cover fundamental and applied research, pilots and deployment, as well as a generic portfolio of *possible projects*.

To incorporate trust as an essential component of digital life, one approach is to have a well established and understood "chain of trust", both for services linking to some trusted authority and for devices linking to some physical trusted anchor for full transparency and accountability, as well as the protection of citizens from threats. Another could be incorporating reliable reputation-based systems that provided a distributed alternative to the centralised "chain of trust" approach. This document outlines a roadmap for a Trustworthy ICT environment, which includes a defined research agenda with clear objectives that need to be fulfilled within a defined schedule.

[3] See an extensive report in the ITU document digital.life: www.itu.int/osg/spu/publications/digitalife/

In addition to the shared issue of privacy of individuals in their online life, more comprehensive issues related to basic human rights including freedom of speech, transparency and openness, and democracy also need to be considered. Transparency and the ability to make informed choices will be central. For this document, instead of covering all possible domains, we have chosen the following application domains that reflect a wide range of relevant requirements:

- Services for closed groups, such as family members or members of a club
- Logistics and Transport
- Medical environments and healthcare requiring reliability and confidentiality of data
- Active and Healthy Aging
- Financial environments that have trust requirements for financial transactions
- Telecommunication (currently forced to strengthen privacy according to Directive Telecom package Art. 13a)

In addition to the above, we need to consider additional requirements imposed by the trend towards Cloud computing and an explosive increase in the number of objects that need to be handled in digital life. Though these application domains are far from exhaustive, they will help guide this document to define the research and innovation challenges (Section 2), the research and innovation needed (Section 3) and the expected impact (Section 4).

The document further proposes an approach to trust, called the 'transparent payment for trust' model. It consists of three pillars: payment (business aspect), transparency/awareness (social aspect), and legislation (legal aspect) with the technology needed to provide solutions. In taking this viewpoint, the TDL community expects to gain further insight into the overall problem, even if the proposed model meets with barriers.

TDL's viewpoint

There are different viewpoints and approaches to investigating the future of trustworthy ICT solutions; one is focused on the paradigm shift where 'transparency and payment' are included from a business perspective, the other is more focused on enforcement by law and regulations.

From a business perspective, taking into account that the TDL community represents a substantial number of industry players in this field, the natural point of departure is to focus on 'transparency and payment' rather than focusing on legal issues. The work carried out in this community since 2010 shows that focusing on legal issues has not sufficiently contributed to raising user awareness of issues related to trust, security and privacy. Following the 'transparency and payment' approach might give novel insights that we would not have gained otherwise. Although the TDL community cannot directly influence regulation and law enforcement, this viewpoint is also addressed by the SRA.

2. Challenges Faced

2.1 Business Challenges

Services in the future will need to cater for a wider range of interests, where social rewards have become an important factor in addition to monetary rewards for many people. Additionally, social networks and services are being mixed with more conventional service offerings, such as for marketing and sales. Organisations and companies have begun to invest in such forms of social trust.

Beyond this new development, business needs to invest in compliance and to fulfil a number of legal requirements related to trust and data protection. All of these expenses need to be recovered to maintain a viable business.

While there are many expenses that can be recovered in general payment schemes, trust, just like privacy and security, often remains the last thing that both consumers and service providers think about. There is often little incentive to pay for (or invest in) trust. As with Trust, people don't expect to pay for (many) services, as shown by the popularity of the "free" social networks. This is not just a European or US phenomenon. For example, in Africa, even electricity is considered by some to be free. This situation makes it an uphill task to change user perception around the need to pay for services and the investment associated with trust and privacy. Enterprises want to keep their prices down and also don't invest because the negative effects associated with the lack of trust (or privacy) are often felt very much later, such as when a major incident leads to a loss of revenue.

Trust clearly plays a decisive role in the acceptance of some Internet services. In e-government, e-banking and other business applications, security and privacy are taken for granted. The 'price' for security is however hidden or included in the taxes paid to the government or account-keeping fees. In other domains, such as social networking, online games or free smartphone apps, the service appears to be free, however, users do pay indirectly for privacy and security. They either have to accept some side effects (such as advertising), or accept – knowingly or inadvertently – that the providers' costs are covered by "selling" or otherwise benefiting from the customers' data.

The reason for a lack of investment in security[4] is that business drivers, such as being first in the market or excelling in offered functionality, are negative incentives to invest in security or privacy. Security and privacy often stand in the way of functionality.

[4] see several articles of Ross Anderson on www.cl.cam.ac.uk/~rja14/

Because of the lack of transparency, users cannot easily compare the security properties of different products and usually expect adequate security and privacy in the products without having to pay for it. Indirectly, service providers understand that their reputation and how customers trust them may be adversely affected if customers' expectations of security and privacy are not fulfilled. Such dangers are, however, often ignored as the negative effects come a lot later.

A number of approaches need consideration here. One is to provide the transparency that users are in fact paying, either with money or their data, and that they should have a choice on "how" to pay. Long-term dangers may be covered by making liability transparent, such as introducing mandatory insurance cover, which would be far more costly if adequate precautions to guarantee the customer's privacy have not been taken. Furthermore, trust may be fostered by regulatory demands on transparent privacy and trust requirements to be fulfilled, with fines due when the regulatory requirements are not met. These are but variants of the *transparent payment for trust* scheme, which does not necessarily mean that the customer pays the provider with money, which may not suffice on its own.

Overall, we need business models and environmental (e.g. regulatory) conditions that permit at least a cost-neutral business case for the development and provision of trustworthy modules or systems.

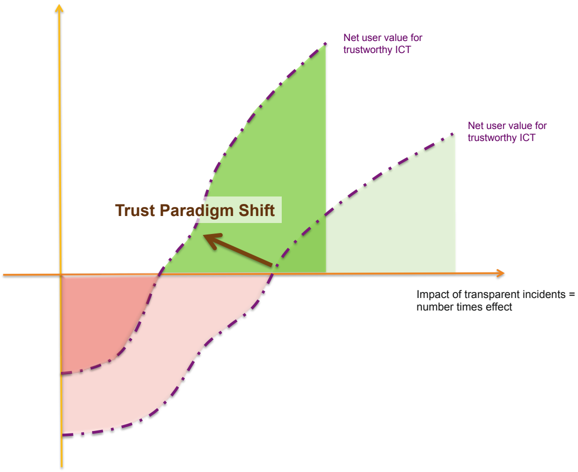
Factors that enable a change in thinking are:

1) awareness and transparent impact of incidents and multiple (mis)use of provided/gathered (user) data
2) perceived user's need for trustworthy ICT solutions
3) realisation that security and privacy are business enablers
4) preparedness/willingness to pay for trustworthy ICT solutions
5) regulations: enforcing privacy and security by design

The relation between these factors will determine the perceived price level for trustworthy ICT (see Appendix A for a detailed explanation). The 'net user value' for trustworthy ICT is the result of the preparedness to pay and the actual pricelevel of trustworthy ICT. The steepness of the net user value is an indicator for the adoption rate of trustworthy ICT; the steeper the curve the faster the adoption.

Based on the preparedness of users to pay, there are two scenarios: a positive scenario with a possible positive net user value for trustworthy ICT solutions, and a negative scenario where the net user value remains negative. The net user value for trustworthy ICT graph (see figure 2.1) shows areas where the net value is negative (where trust is seen a burden and needs to be subsidized to increase the adoption), and where the net value is positive (where trust is seen as a benefit and is self-propelling).

The business challenge is to increase the net user value for trustworthy ICT solutions and thus the adoption rate, see figure 2.1[5]. In addition to positive effects of enforcement by law and regulations, this can be achieved by actions that decrease the costs development and maintenance of trustworthy ICT, thereby increasing the perceived need for trustworthy solutions and increasing preparedness to 'pay' for it. Paying does not automatically mean that ICT will become trustworthy.



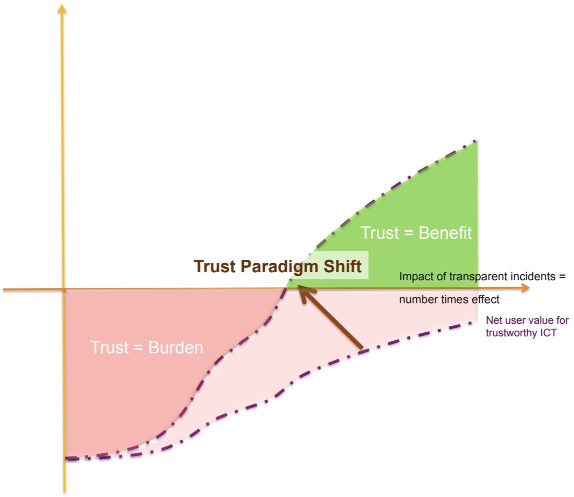


Figure 2.1a: visualisation of the trust paradigm shift in the positive scenario: interventions shift the tipping point, increasing the trust as benefit, i.e. speeding up adoption and increasing value for the user.

Figure 2.1b: visualisation of the trust paradigm shift in the negative scenario: interventions will shift from trust being seen as a burden to trust being seen as a benefit.

The target of the Trust Paradigm shift is to enable a transparent payment scheme involving various players, leading to an overall gain for users (consumers and business users), providers and society as a whole. Transparent payment can be direct, but also indirect, via suppliers, service providers, or even enforced by regulations requiring

[5] The illustrations used are intended to indicate the effects and are by no means reflecting hard measurable predictions. The x-axis represents the impact is of transparent incidents (being a combination of the number of incidents and the effect of the incidents). The y-axis represents the Net user value of trustworthy ICT; a negative value implies trustworthy ICT is seen as a burden, a positive value implies trustworthy ICT is seen as a benefit.

certain trust levels in specific domains to operate a (trustworthy) service. Regulations and enforcement by law can strengthen and speed up the paradigm shift.

2.2 Societal Challenges

Recent years have seen a change in behaviour with respect to the digital world, which has started serving a number of social needs related to communication and recognition. With an increasing proportion of the population participating in digital life, including children, cybercrime has become more attractive. This is also because these new digital citizens are not aware of the risks and dangers that await them. People entrust the digital world with things they would never do in the physical world. These challenges, which legislation is now increasingly aware of, need to be addressed.

Depending on particular application domains, the social issues faced will vary. Several, possibly conflicting requirements, such as preventing misuse of data and the protection against loss of data need to be tackled. We look at these in turn and then address challenges in the Future Internet, Cloud, and Internet of Things context. From a societal perspective, transparency will be empericial, such as disclosing information about a provider's security policy regarding the gathering and usage of data, clarifying what protection is built into a service or product and providing information about potential issues related the device used to access the service. It should also always be possible to maintain anonymity while using services, even allowing for payment schemes that work without revealing the identity of the user.

In the future digital society, technologies are needed to transparently build trust, also towards improved business opportunities for new and existing providers. While the "negative" trust component of the users' assets not being misused (such as a breach of expected behavior related to privacy) is of major importance, trust also requires approaches to support the positive aspect of whether the provider actually delivers what is expected. On the whole, this touches the aspect of fairness: Is the user actually getting a fair deal or not? From a societal viewpoint, solutions will be needed that enable users to make wise and informed choices in the digital world, transparently making clear what the user gets and what the user pays for, whether in monetary form or otherwise. The challenges addressed here should be seen as requirements that need to be addressed by technical solutions.

Understanding that informed user consent including transparency and accountability of actions will be a prerequisite for privacy, the TDL community has identified the following common challenges for privacy of individuals in online life:

- Enforcing policies users expect to be in place,

- Providing users with a) an understanding what is going on, and b) the ability to deal with privacy issues themselves,
- For children, their inexperience should be considered and compensated,
- Because of the scale of gaming, e.g. money involved that makes gaming lucrative for criminals, methods that counteract these are needed,
- A means to indicate trustworthiness of data, products and services (e.g. web sites),
- Protection of data including generated data (e.g. with regard to location),
- The right to be forgotten, which coincides with minimizing collected data, i.e. limited to what is essential for the service.

Central points for *Medical environments and healthcare* are trustworthiness and reliability of data, as well as data protection. Examples of functions required are:

- Advanced access and usage control (e.g. break-the-glass in emergencies or for care personnel),
- Reliability and trustworthiness of data used for diagnosis and in decision support for physicians and care personnel (e.g. data collected by the patient or different health and well-being services),
- Privacy-preserving data mining of EHRs and anonymisation for research and scientific purposes.

In regard to *Logistics and Transport*, we obtain a different set of requirements:

- Tracking of location with differentiated access to the data,
- The user should be able to choose and track the changing handlers of goods and data (e.g. based on reputation).

Financial environments that have trust requirements for *financial transactions*

- Associating trustworthiness of a service or transaction with financial value, perhaps as a range,
- Ensuring enforcement, auditing and rollback in case of failure.

Telecommunication

- Strengthening privacy,
- An ability to choose between different levels of trust and privacy,
- Limiting the collection of data to what is needed to deliver the service.

In addition to the above, it is important to keep in mind that the different legal and societal environments associated with different countries may lead to differences in requirements, also requiring trust solutions to take these aspects into account.

2.3 Technical Challenges

A big technical challenge faced is to create an environment where it pays off to invest in trust, both from the point of view of the enterprises and organisations, and from consumers and citizens. In addition to creating awareness of the problem and getting the required legal framework in place, we need to make digital life more trustworthy. From a technological point of view, this implies the ***development of technologies and methods to make trustworthiness, privacy and security measurable, visible and controllable by stakeholders***. In the context of a chaotically developing digital infrastructure augmented by an un-countable number of attached objects (i.e. The Cloud and the Internet of Things), we need to do so in an increasingly hostile environment. This includes taking account of:

- Disrespect of ownership or co-ownership of data,
- Privacy protecting measures at a high layer are thwarted because of (stray) use of identifiers at a lower layer,
- Retention or copying of data that is communicated or generated without consent or knowledge of concerned parties,
- The growing ability to compromise end-user devices and other equipment by malicious users (or through carelessness), leading to hitherto unthinkable attacks,
- Reliably informing the user of the current level of security/trust/privacy over hostile channels and possibly semi-hostile equipment, allowing the user to exert a reasonable level of control through such channels and equipment.

More specifically, this will need specific actions to handle challenges related to different technical solutions.

Devices, platforms and services:

- Protecting end-user devices, networks and servers from malware, including mobile devices that so far, have not ben targeted very much,
- Visualizing the level of trustworthiness of devices, platforms and services as a component of overall trust,
- Controlling trustworthiness levels of a used end-user device including the ability to switch between different levels reliably,
- Providing trust metrics and signals by assessing trustworthiness, privacy, and security mechanisms of a service (e.g. interpretation of privacy policy, assessment of security, reputation, certification, etc.)
- Measuring risks and benefits offered by a service.

Identities:

- Protecting credentials while achieving a maximum level of security, privacy, mobility, costs and usability, understanding that in some scenarios there are trade-offs that will need to be considered. In these situations, the reasons and options should be transparent to the user,
- Assuring unlinkability.

Information and attributes:

- Privacy of information (privacy preserving data mining, operations on encrypted data)
- Controlled disclosure of attributes and information
- Proof of attributes and validity of information (data provenance, origin authentication)

While solutions are provided by technology, mechanisms for monitoring and certification are essential to ensure that solutions and services (possibly composed of different subservices) are compliant with legislation.

2.4 Legal Challenges

When developing solutions, we need to start at a non-technological level, such as the need to provide end-users with means to delete information and finding technology solutions to facilitate this. Regulations, such as those related to privacy, need to be technology-agnostic.

The law provides an incentive structure for business: legal notions such as contracts, trade secrets, intellectual property law, but also effective remedies for a series of fundamental rights determine the framework within which businesses, consumers and other stakeholders can create and enjoy added value. Whoever wants to do business in the EU will need to comply. See Europe vs Facebook[6], and the pillars proposed by Commissioner Reding[7] and the recent published audit report on Facebook by the Irish Data Protection Commissioner[8].

To incorporate trust as an essential component of digital life, we need a well-established and understood “chain of trust” for full transparency and accountability, as

[6] see http://europe-v-facebook.org/EN/en.html

[7] see http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183&format=HTML&aged=1&language=EN&guiLanguage=en

[8] see http://www.europe-v-facebook.org/Facebook_Ireland_Audit_Report_Final.pdf

well as an in-built protection of citizens from potential threats. It should be clear to the players involved where the “root of trust” lies, and why and to what extent they should trust the root. In technical terms, the chain of trust for a service may end with an authority that is trusted, or in the case of devices, may end with a trusted component in a computer or mobile phone. Besides the chain of trust approach, alternative, “softer” and more distributed approaches, such as using reputation schemes may be considered. Here, a single anchor is replaced by many. This corresponds, for example, to making choices based on the recommendations of friends and family.

The challenge is to protect the stakes and interest of all the involved parties in a well-balanced manner, including:

- Private citizens should have a means to compare offerings; to make adequate choices and have adequate remedies,
- Service and technology providers, i.e. to have possibilities to evaluate the consequences of actions and omissions of actions; to deal with liability (chains) and costs,
- Authorities, i.e. to have sufficient means to verify, audit and intervene.

The TDL community has identified actions (including remedies) that would improve end-user trust in online services:

1. Protection regardless of location and liability regardless of location
    - Since online services do not follow country borders, customers must enjoy the same legal protection regardless of the service provider(s) location,
2. Joint and several liability of service providers
    - Similar to the sale of goods, end-users should be able to make claims against relevant parties that participate in offering the service
    - Especially in cloud-computing, if end-users can only make a claim towards the immediate interface (i.e. where it would be well-known that, for example, a data-breach was due to failure by another service-provider in the cloud), this could lead to unfair consequences if the immediate interface is unable (either technically or financially) to cover its liabilities based on the agreement or applicable law,
3. Law change to also include services offered for “free” to be protected by similar warranties and liabilities, when in fact “free of monetary payment” is replaced by payment in other values, such as exploiting user’s personal data
    - In some member countries consumer legislation is stricter on “sale” of goods or services compared with those offered free-of-charge.

  - Business models are increasingly reliant on exploitation of the data that end-users provide when using the service (subject to the applicable privacy policy).
  - It can therefore be argued that such data is a mean of payment to benefit from the service, and consequently the service is not provided free-of-charge.
  - Such services should be subject to same legislation as those paid for with money, giving consumers the same level of protection.
4. In summary, consumer rights should be the starting point, because strong consumer rights mean strong consumer trust.

Given the nature of international online services the following challenges should be taken into account:

- Complexity of services and systems,
- International aspects of contract governance,
- Jurisdiction, EU coverage and protection against claims coming from outside, such as legal interception,
- Criteria for sufficient quality level,
- Liability: consumer liability (in case they ignore security measures and risks) and Service Provider liability,
- Enforcement of the regulatory framework.

At the moment, the unfortunate truth is that stakeholders and in particular, end-users, cannot understand the consequences of their actions or omissions according to the law, since the question of which laws are applicable is unclear in many countries. Furthermore, it is quite pointless to have a perfect framework of laws and regulations that cannot be effectively enforced.

3. Research and Innovation towards Horizon 2020

The identified technical, social, business, and legal challenges of chapter 2 describe the main issues that need to be addressed to achieve the future-intended end-2-end trust landscape. To realise the Trust paradigm shift, we focus on the most relevant research and innovation building blocks (see section 3.1) and identify the core (long and medium term) research questions (see section 3.2). We define a portfolio of possible future projects (see section 3.3 and Figure 3.1) with roadmaps for different stakeholders that drive the trust paradigm shift.

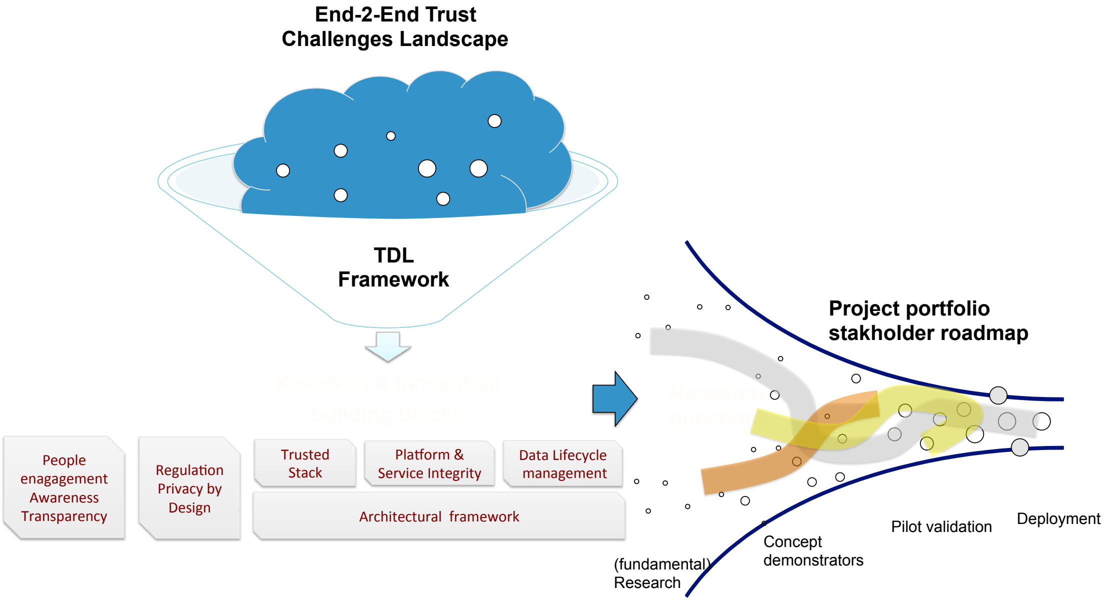


Figure 3.1: Overview of the used approach

3.1 Research Framework

The TDL Research Framework determines the research and innovation building blocks of the Strategic Research Agenda. The Trust in Digital Life research framework has been created through many interactions by best in class researchers and multidisciplinary experts from the Trust in Digital Life community.

The following were identified as central to the approach:

- Trusted data management over the whole data life-cycle: For example, there is strong pressure to reduce the cost of healthcare, such as through process automation. This has been delayed due to the absence of relevant legislation, for example on how related pieces of patient data should be managed and handled. Another example is the financial industry, where online transaction fraud is on the rise but consumers do not have appropriate solutions.

- Trusted Platforms and Services that ensure integrity and transparency to make users willing to pay for services. Value for money is key, and, if consumers are expected to pay for Trustworthy ICT solutions as commercial products and services, it must be clear what the product and service is and what the consumers receive in return. Guarantees and accountability to protect consumers are prerequisites.

The Figure 3.2 below shows the building blocks related to the ‘transparent pay for trust’ paradigm shift that we expect to play a role in addressing the technical, social and legal challenges of the future.

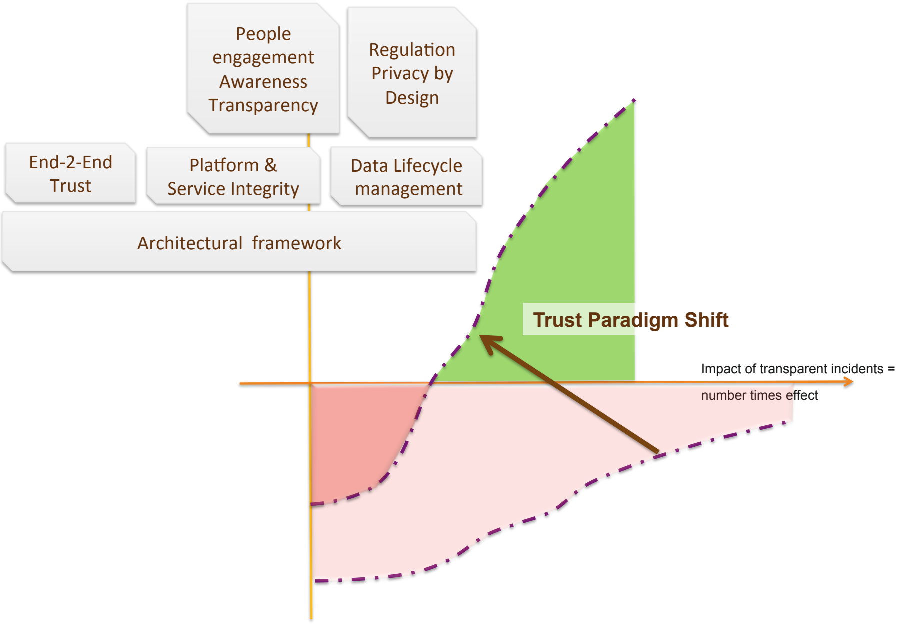

People engagement Awareness Transparency
Regulation Privacy by Design
End-2-End Trust
Platform & Service Integrity
Data Lifecycle management
Architectural framework
Trust Paradigm Shift
Impact of transparent incidents = number times effect

Figure 3.2: Impact of building blocks on the trust paradigm shift

Applying the TDL research framework leads to the following research and innovation building blocks:

- Architectural framework for trust in digital life,
- Data management over the whole data lifecycle,
- Platforms and Services ensuring integrity and transparency,
- Trusted Stack with intermediate infrastructures that guarantee trust,
- Raising awareness and providing transparency,
- Regulation for privacy by design.

As TDL focuses on technical innovations and solutions, only the architectural framework and technically-related building blocks will be described in further detail.

3.1.1 New Architectural Framework

An important ingredient of the overall architectural framework for trust in digital life is identity management and the authentication architecture. The TDL white paper "*Architecture serving complex Identity Infrastructures*"[9] sets out a some fundamental principles:

1. Composable Architecture
2. Open to Technology and Standards evolution
3. Attributes remain with the source of the data
4. Informed User Consent
5. Privacy
6. Correctness and accountability

These are principles that must be considered when designing a large scale authentication architecture. In the future these principles will not fade away. The architectures built in 2020 will have to address the same kinds of principles. Due to social and technological evolutions there might be a few additional principles needed to protect users against further challenges raised at that time.

As the architectural framework is a generic research topic, the TDL community is taking a first step towards an overall framework by looking into the interoperability and utilisation of different existing identity management solutions. For this purpose, the TDL community has specified an example of a trustworthy e-authentication architecture framework which examines how to design a large scale authentication architecture, as shown in Figure 3.3.

[9] see www.trustindigitallife.eu/documents-faq/tdl-publications.html

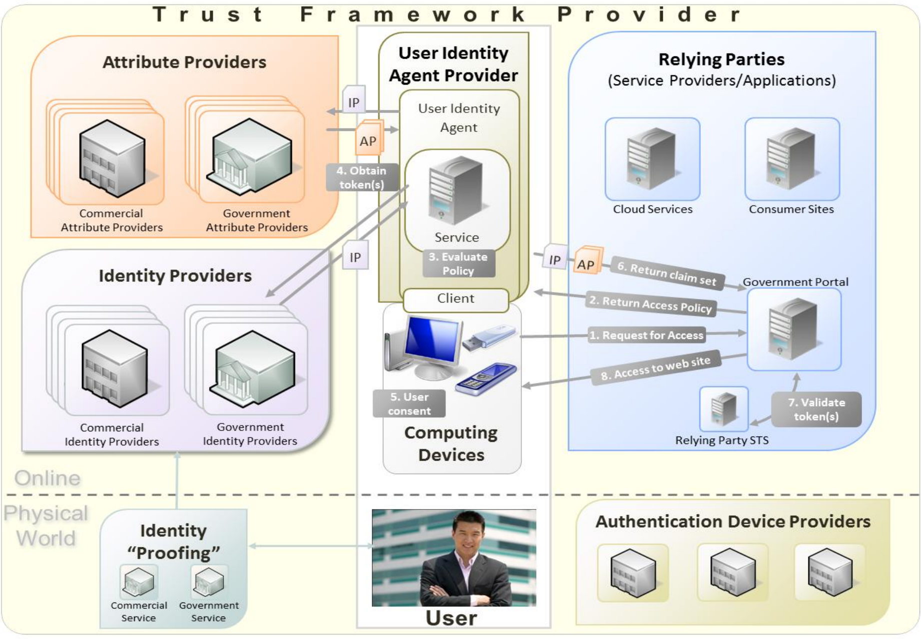


Figure 3.3: Example of future trustworthy architecture framework

This architecture specifies core building blocks needed for large scale architectures that remain stable even when technologies, protocols and devices change. The underlying principles go beyond traditional Internet transactions into the physical world, and include not only payment, but also access to buildings and vehicles, and support the exchange of contact information (business card scenario). This architecture has the potential to become the de-facto standard in IT infrastructures.

Identity User Agent

A user agent represents us in the physical and digital world. It may be a part of mobile devices and act on behalf of the user via policies that users can express. Users can list trusted entities to which agents can automatically reveal claims. Privacy thus plays an important role in such scenarios. There will be a need for new protocols that allow users to only reveal those claims to trusted entities.

User agents will also be instrumental in anonymous micro payments, for example in the case of payment of road tolls and can be authorized to pay without revealing the identity of user, whilst keeping accountability in place in case things go wrong.

Comprehensive Trust

Often, too much trust is placed in single components. Identity providers can impersonate users by creating credentials in our name without user intervention. Reducing the trust we need to put in each of these components while still having an overall trustworthy system will be a key research theme for the future. User consent should steer the generation of user credentials.

User Friendliness

Intelligent components need to cooperate to facilitate smart, complex transactions with the user at the centre. Even non-savvy computer users need to be able to understand the decisions they make to ensure safe transactions. User friendly interfaces for security and privacy will be a key future innovation.

3.1.2 Data life cycle management

Consumers are often reluctant to put their critical assets, such as files, profiles and activity logs, in the Cloud and may prefer to keep these assets local despite higher costs[10]. Such critical assets can be files, credentials, identities, profiles, activity logs, etc. People know their material assets in the physical world and are uncomfortable with digital versions of such assets, despite the convenience, speed and security offered by e-services.

A complete set of Data Life Cycle Management solutions is needed here, leveraging existing technologies and filling in gaps with missing technology building blocks. This includes technologies from secure authentication, access control, secure storage and revisions management to data archiving and data termination.

The goal is to “port” into the Digital world all of the key attributes of assets in the physical world that people like and build their trust upon. Protecting identities, assets and transactions are TDL’s three pillars of a trustworthy eco-system where people can feel comfortable and which also offers scope for business development.

One aspect is user-controlled management of identities (Ids) and identifiers (IDs) with privacy-friendly and selective disclosure of personal data for transactions and the secure storage and termination of identifiers. Since the personal data which constitutes an identity is, generally speaking, distributed over multiple partial identities and identifiers, devices, and identity service providers, one major challenge to be addressed is the development of a consistent (single) user interface for access and management of identities and identifiers.

R&D efforts must further be directed towards solving critical issues for secure storage, execution, deletion, and revisions management. Applications leveraging cloud computing today lack these qualities and should be central for future research programs.

[10] see also http://www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf

3.1.3 Platform and Services Integrity

Thanks to the increasing success of online Application Stores (like Apple's for iOS and Google's for Android), software is becoming a convenience good. However, the exploding variety of interacting applications creates a kind of digital chaos where it is still impossible to prove the integrity and the safety of running software on platforms. Personal data is exposed and risks being compromised by commercial or criminal motives. Potential threats in the context of "The Internet of Things" with a multitude of networks and devices further aggravate the situation.

TDL's service integrity approach includes a chain starting from creation by the application developer, to running on the target platform (e.g. a smartphone) and its interaction with a networked server. Although each element of this chain (such as storage or data transfer) can be secured rather easily, the combined safe and secure service offering is a much bigger challenge.

Platform integrity requires, amongst other things that:

- the platform works as intended and in a trusted manner,
- the platform assists the user in a user friendly manner to adjust policies based for example on user behaviour ideally, offering solutions where users are not required to manage policies but instead, they trust that policies are implemented as they are declared[11], and
- user acknowledgements of policies are straight-forward and transparent, while enabling monitoring of functions and auditing.

Currently, execution platforms are short of adaptability and current service provision value chains are flexible. Depending on the platform being used and the security model that has been implemented (e.g. regarding the controlled usage of device capabilities by applications) there is different degree of control over what (potentially dangerous) application elements may be installed onto mobile devices.

To solve these issues, TDL proposes:

- to define and develop a Trusted Mobile Platform[12] that uses existing components based on standards or specification of fora offering:
  - a secure/trusted execution environment capable of isolating applications and preventing unauthorized modifications on applications;

[11] there is a fundamental tension between "automating security policies" and making sure that the user is able to enforce a policy that suits his/her needs. This is a difficult research problem that needs to be addressed. Current extremes are either very simplistic "one-size-fits-all" types of policies or policy configuration that is too daunting for users so that only a few users ever change the default.

[12] e.g. building on projects like Trust4ALL (www.hitech-projects.com/euprojects/trust4all/)

  - different execution environments depending on the risk level of an application;
  - requirements for a user interface, that prevents manipulation of users and helps them to make policy decisions, e.g. regarding privacy;
  - a trusted path between the user interface and the trusted execution environment;
  - remote attestation of the state of execution, e.g. to authenticate running applications (e.g. signed software as a pre-conditon for execution) and building on existing security mechanisms.
- to define and develop a deployment model:
  - which integrates trust mechanisms, such as trusted third parties and reputation mechanisms,
  - where an agent running in the trusted execution environment (e.g. a Secure Element), acts as a trust reverse proxy and can automatically reject or accept new applications as a function of trust metrics, user profile and configured policies.
  - where the execution platform (OS, application) is capable of adapting the isolation constraints as a function of the criticality level of the selected application. Trustworthy services should rely on a trusted stack.

3.1.4 Trusted stack

The Internet has transformed the way we live. Social networking has become the new town square, blogging has turned citizens into journalists (mobile devices with integrated still/video camera functionalities further enhance this and make blogging/personal newscasts ubiquitous and instant), and e-commerce sites have revolutionized global competition in the marketplace.

However, along with the Internet's phenomenal growth, computer and network related crimes have exploded as well. Criminal activity ranges from consumer threats, such as malware, botnets and ID theft, via enterprise threats, such as stealing sensitive information, economic espionage and denial of service attacks, to government threats, such as information warfare. Creative, adaptive, and sophisticated adversaries are mis-using the Internet and sometimes creating havoc.

TDL assumes that we might need to "change the rules of the game". This starts by building a 'trusted stack' with suitably strong authentication of hardware, software, people, and data. The intention is to improve auditability of events which in turn enables accountability. People need to be in control of their personal information, and be given tools to manage their online reputations. The trusted stack, combined with better mechanisms to protect privacy, will enable End to End (E2E) Trust. This in turn provides people, devices, and software the means to make informed decisions about who and what to trust throughout the ecosystem.

3.2 Research Questions

The identified research and innovation building blocks lead to a number of important mid-term and long-term research questions. Here we list (fundamental) research questions which relate to the technical, business, legal and societal challenges. The main underlying question in this SRA is **"How to achieve the Trust paradigm shift?"** and **"What are the bottlenecks and how to overcome them?".** See Appendix C for a detailed overview of the research questions.

3.2.1 General research questions

What are the most important factors that influence trust and which can be used to model and evaluate trust? What are the expectations of European citizens regarding trust in digital life? What are the dominant application areas within digital life that shape their perception of trust? What are expressive indicators of trustworthiness?

A simple definition of trust (as used in Chapter 1) is: "Trust is comprising the intention to accept vulnerability based on positive expectations of the intentions or behaviours of another". According to wikipedia[13], one party (the trustor) is willing to rely on the actions of another party (the trustee); the situation is directed toward the future. The trustor (voluntarily or forcedly) abandons control over the actions performed by the trustee and is uncertain about the other's actions. The uncertainty involves risk of failure or harm to the trustor if the trustee does not behave as expected.

What are the expectations of European citizens regarding trust in digital life?
For European citizens to embrace digital life in all fields of life, such as commerce, culture, government, and healthcare, they must have confidence in the trustworthiness of digital services. Beyond the purely technical properties of ICT (such as encryption or attestations that declare a system as dependable), social, cultural and legal aspects also need to be considered.
The trust of a relying party is based on an expectation of the intentions and future behaviours of that other party. Researchers, policy-makers and implementers thus need to understand what citizens expect from a trustworthy digital environment.
Questions to be addressed are:

- What concerns of citizens drive or inhibit the acceptance and adoption of services?
- How do legal, social, cultural and technical mechanisms contribute to the formation of trust in digital life?

[13] source http://en.wikipedia.org/wiki/Trust_%28social_sciences%29

- How can the trustworthiness of particular services be made apparent to citizens?

Which dominant application areas within digital life shape the perception of trust?
Trust is subjective and situation-dependent, and the requirements on trust depends on the application. The most relevant application areas of digital life need to be assessed regarding the requirements citizens have to feel safe with these digital services. Beyond privacy and IT-security, social norms and legal regulation are involved. Trustworthiness needs a clear definition and metrics. The level of vulnerability accepted by users for services such as on-line banking is high, because of the liability that the banks cover in case of incidents, often defined by the law. However, the situation for services, such as social networks and online games are much less transparent. An independent European 'trustworthiness' measurement and evaluation methodology could significantly help expand trust-related Internet services.

What are expressive indicators of trustworthiness?
Trust is often seen as subjective. Users have to decide whether or not to trust a particular service on a case-by-case basis. Information is needed about features that a potential service partner possesses and of the attitude of the user. One method of trust building in computational settings is feedback-based reputation which helps to estimate future behaviour. This simplistic approach needs to be extended, such as by contextual sensing and machine-learning. We need to identify features that are strong indicators of the trustworthiness of the partners, modelled as when citizens establish trust in the real-world, and subsequently evaluated. Such a system has to capture user intentions, be usable and seamlessly integrate with the core functionality of applications.

3.2.2 Research questions related to architectural framework

What future architectures are needed to establish and maintain end-to-end trust?
What are the best architectures for complex authentication/identification systems?

The trend to outsource data, computations and even computing platforms "into the cloud" carries a great potential to increase productivity and cut cost. With new roles emerging and the roles of existing digital service providers changing, many assumptions are being questioned. We need to accommodate, for example, Facebook logins to authenticate other services. We need to re-visit and re-evaluate the assumptions underlying current architectures. Users may end up in an undesirable state, such as more-than-expected personal data being revealed. Also, can businesses trust the cloud?. Data and processes need to protected from competitors, rogue system administrators, and (naturally) the service providers used. In short, the cloud must be trustworthy.

New research is needed on issues, such as how minimal disclosure of sensitive data can be enforced, how the impact of a rogue administrator be minimized, how trust can be handled over multiple parties, and notification and revocation are handled.

3.2.3 Research questions related to Data life cycle management

How can we ensure *trusted data life cycle management* in information systems ensuring that the risks of data creation, access control, sharing, usage, storage, archiving, back-up, and termination of data are all manageable by all parties involved?

Mobility and cloud computing have become an unavoidable part of everyday life. Data no longer resides on physical storage isolated “securely” from the rest of the world. Open and interconnected systems pose new challenges for security technologies. Threats from cyber-criminals have grown, and are an obstacle to the widespread adoption and utilization of the new technologies, such as e-commerce. The risks of the whole cycle of digital data management from data creation to data termination must be made manageable.

Important building blocks of trusted data lifestyle management are still missing. How do we model and determine data authenticity, reliability and provenance? How do we ensure data confidentiality, and data minimization? How do we know that the data is used for legitimate purposes? How are operations on encrypted data made possoble? How do we provide transparency and methods for the consumer to objectively measure the risks of putting his data in the cloud? How can data be securely deleted and how to guarantee the right to be forgotten?

3.2.4 Research questions related to platform and service integrity

How to compose platforms and services of multiple people/sources, e.g. adaptive heterogeneous complex service composition, and enhance trustworthiness?

Trustworthiness must be transparent and different trust-creating and manifesting (trust-descriptive) solutions can help in this, such as those cumulating end-user feedback on e.g. certain Internet services (online stores etc.). Proper management of user identities as well as service identities plays a central role. New ways of strengthening authentication and sophisticated identity verification of users and services are needed. Interfaces between different platforms and services should be designed with security and trust in mind. Independent authorities need to be able to evaluate and certify (verify) trust between different sources, communities (people), services and platforms. This includes ensuring application and system level trust.

3.2.5 Research questions related to trusted stack

How do we make the trustworthiness of an end-user device transparent to the user? How do we model the 'health' of devices and components? How to increase the assurance on the "health state" of endpoints, and how can unhealthy and hacked devices be instantly spotted? What "stethoscope" can we apply to these devices?

Making trustworthiness of devices transparent to the user.
Users have little technical knowledge to be able to understand the trust level of the device, and may not even be able to differentiate between the trust level of the application and the device. The user should get an indication of the trust level of the whole stack leading from the device to the application in question to feel safe. This should cater for different levels of trust needed, such as for financial transactions and simple surfing of the Internet.

Modeling the health of devices and components.
Techniques are needed to identify the health of devices, for which models are needed to check the health level, i.e. possible compromise of the ideal behaviour of devices and the software running on them. Beyond current kinds of malware, this should also involve unexpected changes of behaviour of devices that may result from regular software, which may cause unexpected behaviours, such as allowing a more promiscuous access to possibly sensitive data.

Enhanced detection services for compromised devices.
In addition to providing security within devices, the future opens new opportunities to provide detection or 'stethoscope' services for devices that can indicate the trustworthiness and health levels of devices. These can both be web based, as a new kind of software as an add-on, or even a part of the basic operating system of devices. Such 'meters' make trustworthiness more transparent to the user.

3.2.6 Research questions related to social and economic impact

What are the driving factors of security and privacy perception of consumers and business? How to strengthen the acceptance of trustworthy technology and the Internet? What is the business value of trust? How does a trustworthy Internet impact overall employment and the ICT services market in the EU? What are the incentives and barriers for the deployment of trust models?

Driving factors of security and privacy perception of consumers and business.
Security and privacy are important factors in a customer's perception of trust in services. Most service providers make their privacy and security policy publicly available, but many customers do not understand the details of these statements. Perception of security and privacy are subjective, and depend on factors such as the legal liability of the provider, quantity and impact of publicized security/privacy

incidents of the service, opinion of friends and trusted people and business partners. Explaining the correlation between the subjective perception of 'hard' security and privacy measures and the 'soft' perception will help in establishing trust in the Internet services.

Strengthen the acceptance of trustworthy technology and Internet
The "ease of use" of trust is one of the most significant factors in accepting or rejecting useful Internet services. The Technology Acceptance Model TAM)[14] from economics is a strong method for studying the statistics of consumer behaviour towards new technologies. In the case of Internet services, trust is added to the perceived usefulness as input factors to the TAM model. For proper evaluation, a considerable amount of statistical data is needed.

The business value of trust
Security, privacy and trust are significant factors in both consumer and business decisions regarding the use (or not) of online services. However, providers will only invest what they see as really necessary in security and privacy, often just enough to comply with the regulatory requirements. It is, on the other hand, not known how many new customers would use services and how much is the business value they represent for the provider if security, privacy and the perceived trust increases. A cost-benefit analysis will help in definition of the business value of trust as a "product".

The expected impact of a trustworthy Internet on employment in the EU
Future Internet, cloud computing and a trustworthy Internet will have a complex impact on the labor market of the world and the European Union. With the outsourcing of ICT operations to the cloud, some ICT employee functions will become redundant. At the same time, more ICT professionals will be employed or re-skilled e.g. by cloud providers to counter the negative effect. A restructuring of the ICT labor market is likely. There are a few indirect effects of the new technologies on the employment:

- Large companies save on ICT operations due to the new technology and can invest more in their core business, thereby creating job opportunities
- The threshold for using ICT systems becomes very low and SME's can utilize them to expand their business, resulting in new job opportunities.

A comprehensive job market research will help understanding the impact on employment.

[14] Bagozzi, R.P. (2007), "The legacy of the technology acceptance model and a proposal for a paradigm shift.", Journal of the Association for Information Systems 8(4): 244–254.

3.3 Implementation Model via Future Projects

This section defines the roadmaps of possible future projects for the identified technical building blocks (i.e. Trusted stack, Data lifecycle management and Platform and Services Integrity). Different projects and relevant topics have been identified. The roadmaps are in a generic form for the 2014 – 2020 time range, and indicate the overall TDL strategic research programme Per project proposal relevant research questions and innovation issues have been identified for the different types of stakeholders, i.e. industry, government and research organisations. See Appendices B1-B3 for the detailed roadmaps.

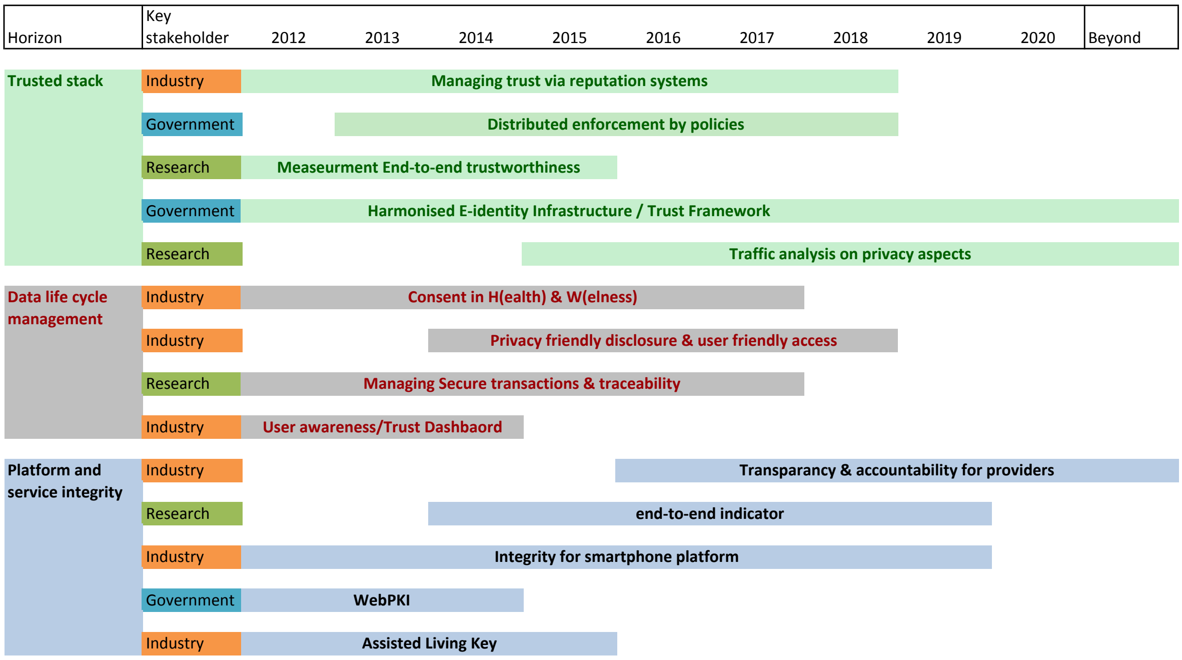


Figure 3.4: Roadmap for Horizon 2020

4. Social and Economic Impact

Trust often influences the acceptance of the Internet services, especially when assets that may be lost or compromised are involved. In e-government, e-banking and other business applications people and organizations take security and privacy for granted. In these areas “price” for the security is included in the taxes paid to the government or in the cost of the products and services. In other applications, as social networking services, online games, free and paid Internet and smartphone apps, the users do not pay directly for privacy and security. The service providers’ costs for development and operations of the systems are covered by “selling” the consumers’ data mostly for personalized or location based marketing. The number of users of some on-line gaming, social networking services, Internet and free smartphone apps is measured in billions. The users pay for the ‘free’ service with personal data.

A factor that is strongly associated with trust in a service is perceived risk, defined as the combination of perceived security and privacy. Further on, trust in this section will be mainly considered as a business challenge to achieve the ‘pay for trust paradigm shift’.

Trust as a personal and business value

One of the challenges in the digital landscape is that many consumers are not aware of the risk levels of the services they use. There are a number of recent security incidents that significantly affect the consumer market reaction:

- The Blackberry email service stopped on 12th October 2011 for 3 days, and it affected about half of the 70 million users. Thousands of companies started to move to alternative solutions.
- In July 2011 the Dutch government had to revoke certificates used for all its secure online transactions, because hackers broke into a web security firm in the Netherlands and issued hundreds of bogus security certificates that could be used on important government and business websites. *Economical aspects of trust in e-banking and e-commerce.*

In the e-banking domain the consumers perceive this Internet application as secure and trust the situation. The price of security is included in the fees paid for the e-banking. After an incident, i.e. where consumers are able to get access to banking accounts of other customers, consumers are aware that the application is not secure and the consumer trust level is damaged. Consumers become concerned and unsatisfied. They expect that the bank will solve the problem and not using the banking Internet service is not a preferred option. Still the (theoretical) question remains: Would consumers in this case be prepared to use and pay for a service that on top of the bank application guarantees 100% (reimbursement) security? We think the answer is “no”, it is expected that banks and e-commerce sites provide a 100% guarantee without additional payment.

Economy of trust in “free” services

A recent example is the security breach of the PlayStation network causing economical damage for Sony and global loss of reputation[15]. The PlayStation manufacturer was responsible for data security and privacy (at least in the EU) as a data processor. The damage caused by the loss of trust as in the above examples is not limited to the users of the specific service, but impacts the whole Internet community. It works as a negative network externality. The service providers however are legally not liable for the loss of trust (and business) in the whole Internet. One might think of Internet security “pollution” as a form of environmental pollution, which is extensively penalized.
Social networking services providers earn money from selling personal data – even if it is restricted by legal restrictions and the EULAs. In a recent study - An Information Flow Tracking System for real-time Privacy Monitoring on Smartphones[16] showed that of 30 apps studied, 2 sent the phone number, International Mobile Subscriber Identity, and IC Card Identity to a remote server, 7 sent the device ID to content servers and 15 sent location data to advertisement servers. In no case was the user’s consent obtained either explicitly or implicitly.

Social impact of trust can be well illustrated using a number of use cases that have been investigated by the TDL[17]. These use cases illustrate typical interactions of users with IT in futuristic but realistic scenarios. As such, they act as a means to uncover concerns, potential threats to security, and potential pitfalls undermining user trust.
Child safety:

- This use case revolves around a young family, whose youngest daughter is the victim of cyber bullying and (in a different scenario) abduction. The use case highlights the impact of the integration of digital communication technology into the everyday life of a family.
- Online Fraud auction: describes a scenario in which criminals meet in a digital exchange of criminal services, such as the sale of user credentials, or a reputation system for online criminals. In the end, innocent and honest end users and intermediaries are (ab)used to defraud an online seller of goods.

[15] e.g. see http://www.guardian.co.uk/technology/2011/may/19/sony-playstation-network-hacking-password

[16] William Enck, et al. 2010. Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI)

[17] see TDL use case overview, www.trustindigitallife.eu/documents-faq/tdl-publications.html

- Online Gaming use case examines various forms of online multi-user games, and the threats that can undermine user trust. Both “hardcore” and “casual” gaming are considered.

4.1 Modelling Impact

Obviously, there exist consumers who will never request for trustworthy ICT solutions nor pay for provided solutions. Another set of consumers doesn’t take security aspects into account during their use of services. The following Technology Acceptance Model (TAM)[18] based on Theory of Reasoned Action (TRA) is designed to describe the variety of behaviours of the consumers (see Figure 4.1). The model can be quantified and tested by standard questionnaire research on a representative sample.
Introduction of trust results in a dynamic structure of the model, as trust can not only be earned, but also lost. The negative feedback impacts the attitude toward usage’ parameter.

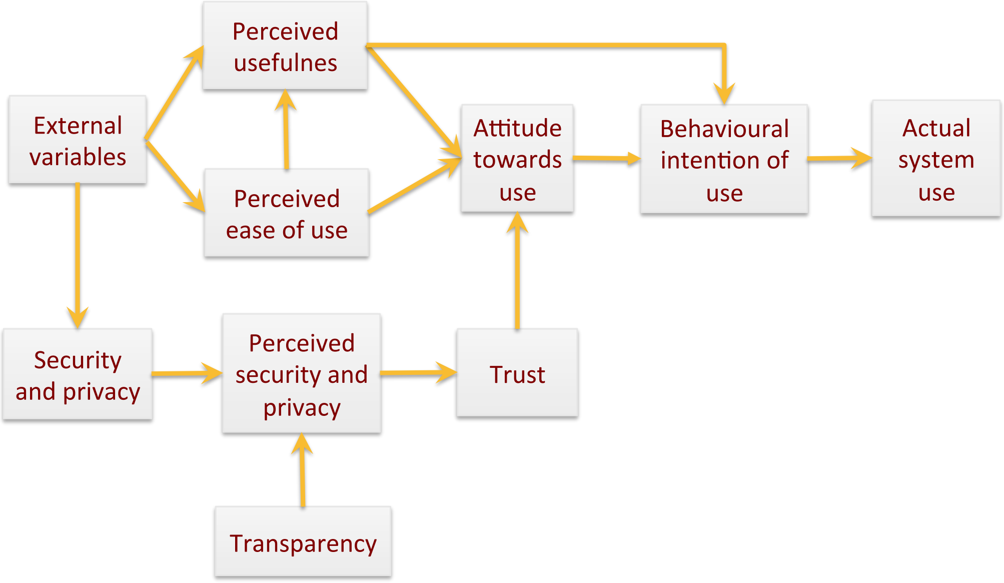


Figure 4.1: The modified Technology Acceptance Model

In the TDL community, we will test the hypotheses on consumers’ willingness to pay for different application areas. The hypotheses tested will be a statistical proof of the consistency of the paradigm shift. An impact model for trustworthy ICT solutions will be included as part of the TDL impact analysis later on in this chapter.

[18] Bagozzi, R.P. (2007), "The legacy of the technology acceptance model and a proposal for a paradigm shift.", Journal of the Association for Information Systems 8(4): 244–254.

For quantification of the amount of people willing to pay for a trustworthy service the "privacy calculus"[19] method can be deployed.

4.2 Impact of Implementing this SRA

Consumer awareness and market behaviour
A general assumption is that the market ramp-up of Internet services is being hampering by a lack of trust by consumers. Many consumers are not aware of the trust levels of the services they use and have made a more-or-less conscious choice to trust service providers/businesses that trade their information and personal details. A question that remains is: "what are the mechanisms to influence market behaviour by increasing consumer awareness?"

The dynamics of consumers' attitude towards acceptance of a given service (and services in general) in relation to gaining or losing trust in services will be modelled by the user state transition model shown in Figure 4.2.

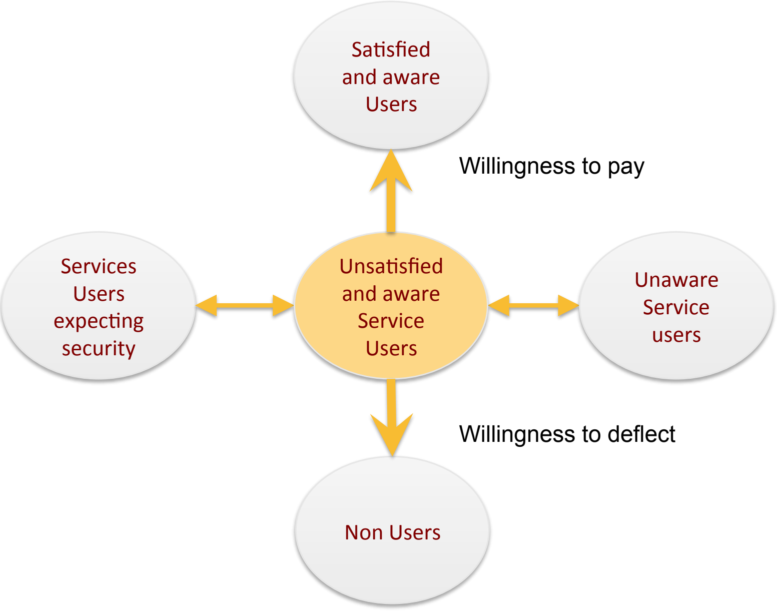

Satisfied and aware Users
Willingness to pay
Services Users expecting security
Unsatisfied and aware Service Users
Unaware Service users
Willingness to deflect
Non Users

Figure 4.2: User state transition model

Clearly, a loss of trust will increase the willingness to defect so the rate of churn is higher (abandonment of the service, as indicated by the downward arrow). In that

[19] Tamara Dinev, Paul Hart (2006) An Extended Privacy Calculus Model for E-Commerce Transactions Information Systems Research 17(1), pp. 61–80

case, the service provider's business case for retaining service users determines the premium for trustworthy ICT solutions.

A market for trustworthy ICT

The challenge we face today is that many companies state that there is no profitable business case for security and privacy features in their services. As a result they lower or terminate their investments in R&D. To stimulate companies to increase their investments in trustworthy ICT instead, means that the market for trustworthy ICT has to be actively developed. The government can play an important role with legislation and economic stimulation in different phases (e.g. research, precompetitive procurement). But, in addition, parties like TDL should identify the technology that will change customer behaviour and should provide means to industry parties to develop profitable business cases.

Generic calculation models describing the market- and technology trends for each of the three innovation lines (described in chapter 3) will be developed to benchmark the business cases of individual projects with a reference project portfolio. Instruments such as scenario analysis are provided to improve individual business cases. With these models we will be able to estimate the market value of the three innovation lines. And if we succeed in collecting the input of approximately 50 individual business cases for trustworthy ICT projects, we can use the models to estimate the macro economic and social impact.

Methodology

The hypothesis is that we can build a generic calculation model that uses market- and technology trends that are very uncertain and that we can estimate reliable forecasts for parties to verify their own investments in R&D. The model for cloud computing is built to test the hypothesis. The outcome is used to list the principles for the generic trust model to measure economic and social impact. The generic trust model is used to make a first portfolio analysis of the economic value of the three innovation lines.

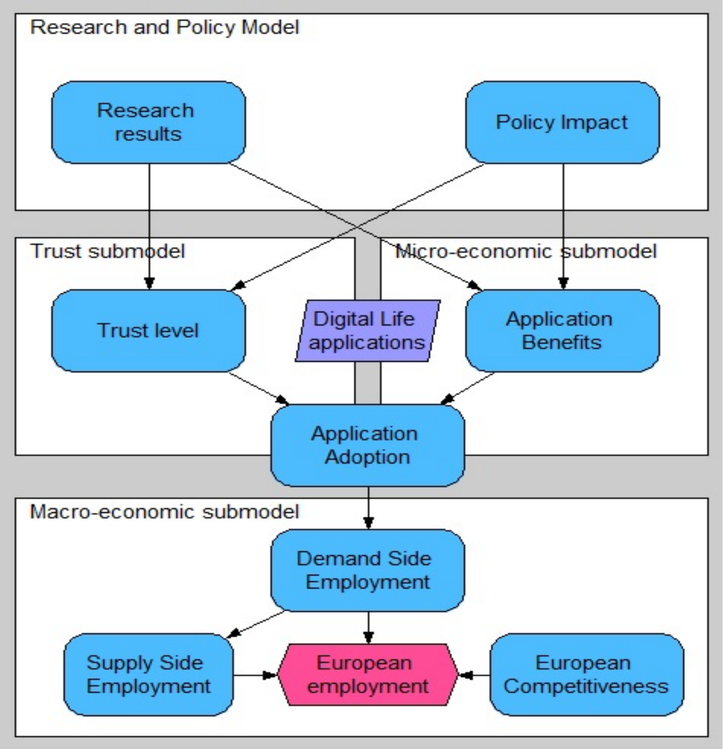


Figure 4.3: Trust in Digital Life impact model

In general flow, this model can be read top-down, where the research and policy themes identified in this SRA indicate the impact on benefits and trust level. The main impact of trust is on the speed and scope of adoption of Trustworthy Internet applications. If people and businesses don't trust in the content and services, they simply will not use them and Future Internet will not work as thought.
For the adoption patterns of consumer applications, we use the technology adoption model as presented in section 4.1. For the macro-economic sub model, we accumulate these application adoption patterns into an effect on the cumulative demand for new ICT services and solutions.

Corresponding to this growth in demand, employment impact is two-folded:

- Reduction of employment due to increased efficiency (typically ICT-related jobs).
- Increase of employment due to growth from increased competitiveness (jobs in primary process).

This demand is related to a supply of these services and solutions, from which the corresponding European share of this supply side growth is derived based on Europe's supply side competitiveness (vis-à-vis competitive providers from e.g. North-America and Asia-pacific region).

With the Flightmap portfolio management tool, we are able to estimate the impact of the choices in this SRA. We have implemented a basic impact model for trust in digital life, and have entered the key data of two sets of projects to forecast their impact:

- the base case set of currently running trust-related projects (including Stork, TClouds, ABC4Trust, PICOS, TAS3, etc.);
- a selection of the the newly proposed set of roadmaps (see also section 3.3), i.e. Trust Framework, WebPKi, E2Etrus, Consent I Heath & Wellbeing, Trust Dashboard, Assisted Living key. The selection is based upon the priorities of the members of the TDL community AND the availability of reliable market data to be model the expected outcomes accurately. The selection of four projects provides a first impression for the impact of implementing all proposed projects in this SRA.

The results of this impact analysis are illustrated by screenshots of the tool used (figures 4.4, 4.5, 4.6 and 4.7). In figure 4.4 on overview is given of all project propsals with their impact on trust. In figure 4.5 the expected trust impact of the selection of the proposed projects of this SRA is shown.

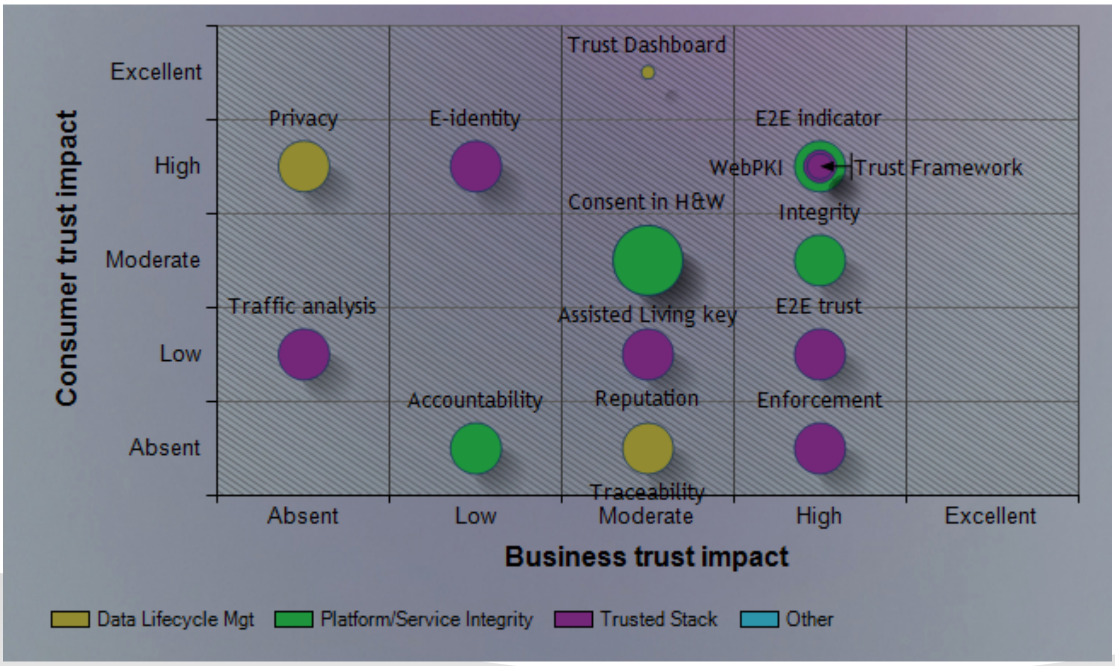


Figure 4.4: Ilustration of all project ideas shown per innovation line, with their impact on trust for businesses (horizontally) and consumers (citizens) vertically.

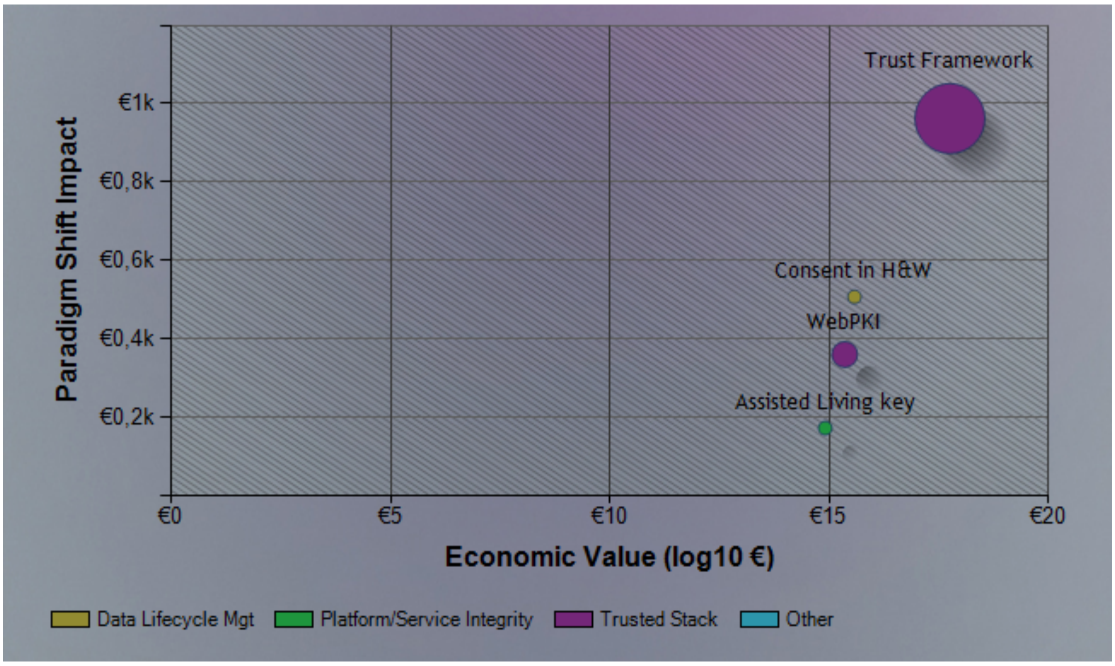


Figure 4.5: Trust impact of the selected projects and proposals. Societal Impact (as contribution per citizen to the Trust Paradigm Shift) and Economic Impact (relative order of magnitude) for the selected project ideas.

In figures 4.6 and 4.7 the result of successful execution of this proposed roadmap indicates a positive contribution to the realisation of the Trust paradigm shift. In Figure 4.6 a low trust future is assumed in the underlying model, while in Figure 4.7 a high trust future is assumed.

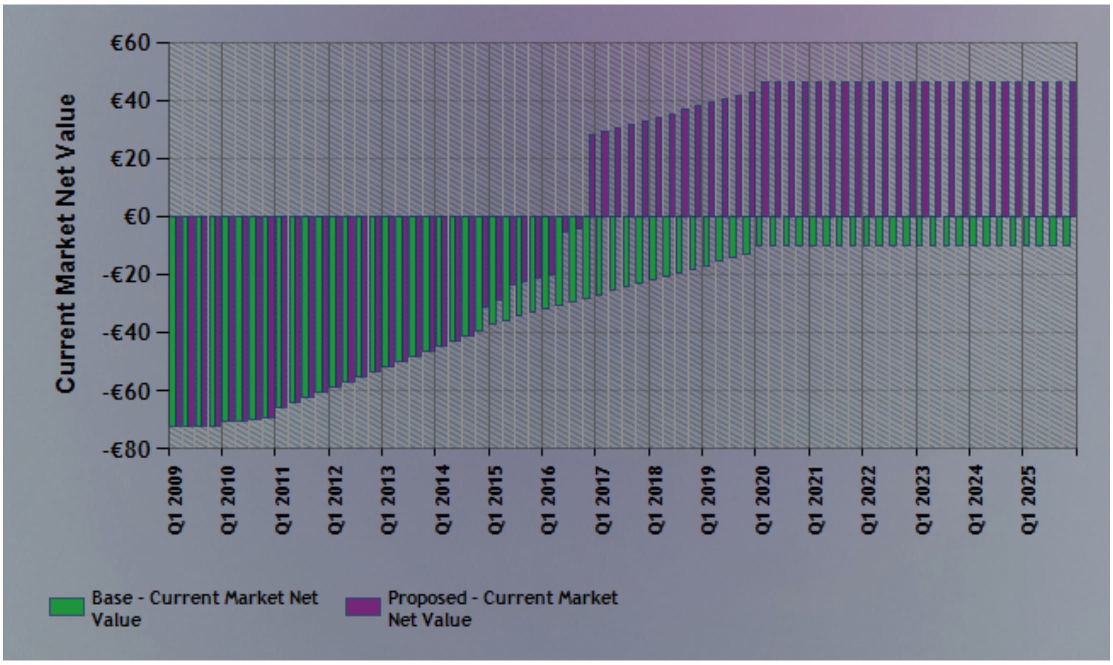


Figure 4.6. Illustration of the paradigm shift where a low trust future is assumed in the underlying model. The Y-axis shows contribution to the paradigm shift per European citizen (per year). Positive contribution to the trust paradigm shift as result of a successful execution of the proposed roadmaps, leading to an increase of the net user value (purple bars) when compared to the base case (green bars) without execution of the proposed roadmaps. If all proposed projects deliver according to the planned timelines with the expected increase of net user value, reduction of price levels, and acceleration of adoption this will result in in a positive net value in 2017.

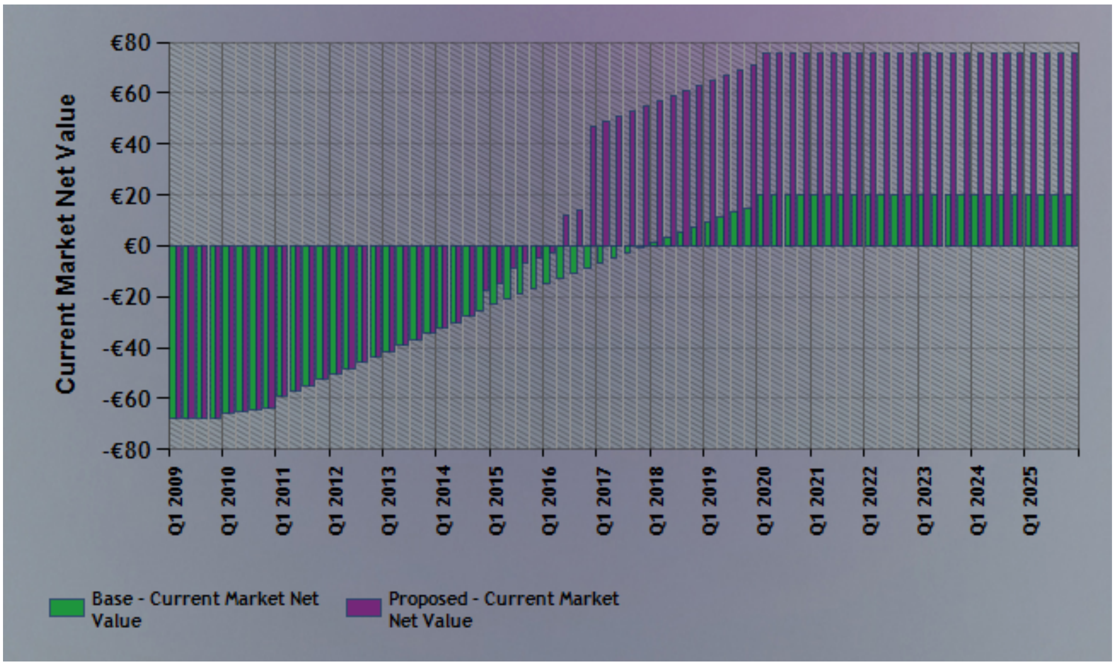


Figure 4.7. Illustration of the paradigm shift where a high trust future is assumed in the underlying model. The Y-axis shows the contribution to the paradigm shift per European citizen (per year). In case of a positive scenario, the increase of the net user value (green bars) will eventually become psotive even without the execution of the proposed roadmaps, however, execution the proposed projects in the SRA (assuming if all proposed projects deliver according to the planned timelines with the expected increase of net user value, reduction of price levels, and acceleration of adoption) will speed up the uptake of trustworthy ICT by several years.

5. Conclusions

Based on a radically changed environment, this document has identified the challenges faced for trust in digital life, the innovations needed, and how we expect these factors will impact our future. A differentiated approach based on the amount of trust needed is expected, and we envision that in some cases, users and enterprises will be willing to pay for a higher level of trustworthiness. One advocated approach is the *transparent payment for trust* scheme.

In the future, development of technologies and methods to make trustworthiness, privacy and security measureable, visible and controllable to stakeholders will be crucial. This is not only to safeguard the rights of users and the assets of players, but also to create an environment that generates new business opportunities. Although it is not the only enabler, trust will be key. In some cases, where critical assets are concerned, it may make the difference between that success and failure of business propositions.

The most important recommendations for stakeholders are:

- ***Governments*** should provide a legal basis that ensures the rights of its citizens in the digital world, while at the same time, providing an attractive environment for business to thrive, thereby enabling the building of trust and protection of privacy. Governments should see European values related to trust and privacy as differentiators that enable business, even beyond the borders of Europe.
- ***Legislators*** *should create a level playing field that safeguards core values of the rule of law, and provides for effective remedies in case of breaches.*
- *The* ***Research Community*** *should provide the technical solutions for increased privacy and security, such as developing technologies that implement and test the transparent payment for trust scheme for higher levels of both trust and trustworthiness.*
- ***Industry*** *should promote research in this area and participate in programmes that create new solutions, while ensuring that the output of European research is transferred to business. The need for a trustworthy infrastructure should be recognized, as consumer trust will be a critical asset in the future. Industry should take practical initiatives towards this goal.*

As a consortium of leading industrial and research players in the area of trust, we will utilize this Strategic Research Agenda to guide our efforts in shaping our common future Digital Life with the appropriate support of trust, privacy and security.

Appendix A: Trust Paradigm Shift

The perceived price level for trustworthy ICT see Figure A1[20]) depends on several factors mentioned in section 2.1 (The X-axis (of all figures in this Appendix) represents the impact of transparent incidents (being a combination of the number of incidents and the effect of the incidents). The Y-axes differs per figure.
The relation between perceived need and preparedness to 'pay' for trustworthy ICT solutions is illustrated in Figure A2, where the preparedness to 'pay' for Trustworthy ICT solutions may be very limited.

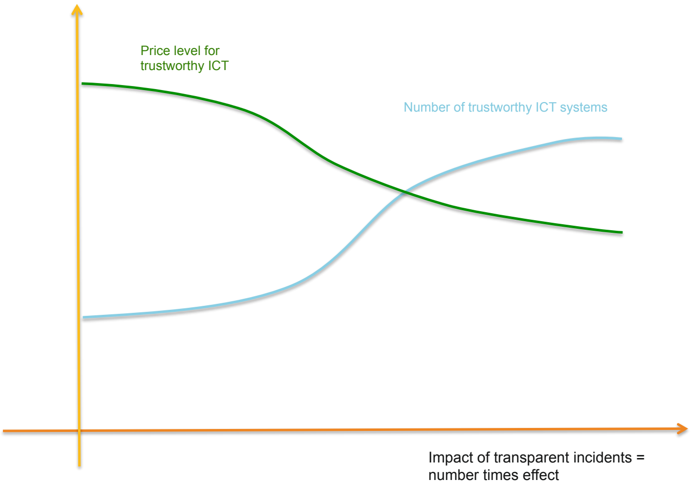


Figure A1: Price level for trustworthy ICT decreases when there are more solutions as a result of higher impact of incidents. The Y-axis represents the price/cost level for trustworthy ICT.

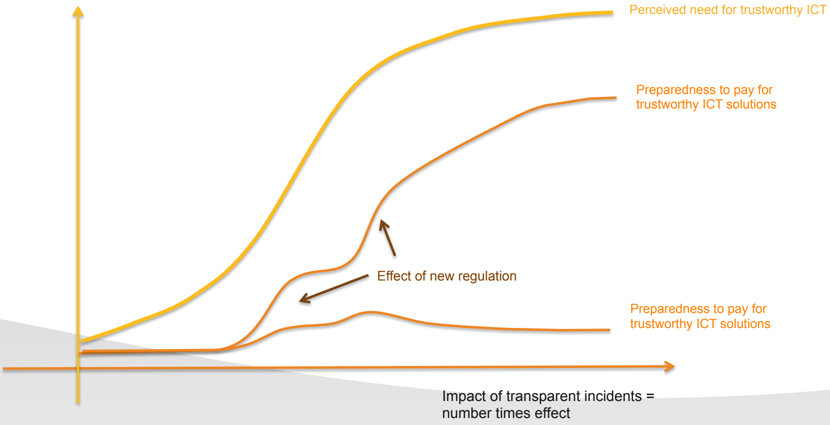


Figure A2 Perceived need and preparedness to 'pay' for trustworthy ICT solutions increases when the impact of transparent incidents increases. The perceived need for trustworthy ICT is upper-bound for the preparedness to 'pay' for trustworthy ICT

[20] The illustrations used in this paragraph are intended to indicate the effects and by no means reflect hard measurable predictions.

solutions and regulation can boost preparedness to ‘pay’. The lower line is related to a domain where people are not really prepared to ‘pay’. The Y-axis represents the perceived need (orange line) / preparedness to ‘pay’ for trustworthy ICT (brown lines).

The ‘net user value’ for trustworthy ICT is the result of the preparedness to pay and the actual price-level of trustworthy ICT. Based on the preparedness of users to pay, there are two scenarios: a positive scenario with a possible positive net user value for trustworthy ICT solutions and a negative scenario where the net user value remains negative, see figure A3. The steepness of the net user value is an indicator for the adoption rate of trustworthy ICT, the steeper the curve the faster the adoption.

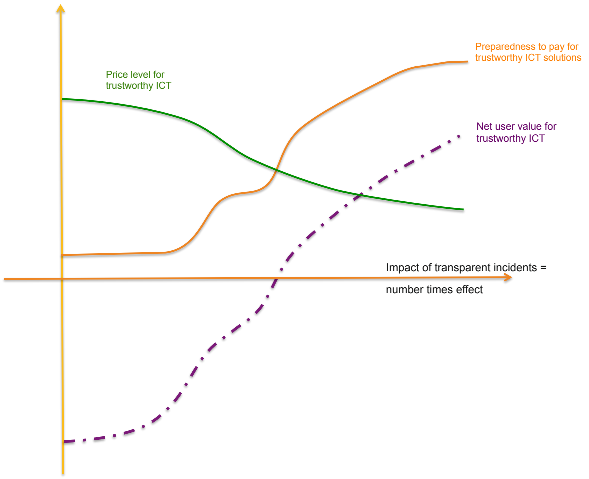


Figure A3a: Positive scenario: the net user value for trustworthy ICT (the dashed line) will become positive. The Y-axis represents the price level for trustworthy ICT (green line) / preparedness to ‘pay’ for trustworthy ICT (brown lines) / net user value for trustworthy ICT (dotted purple line).

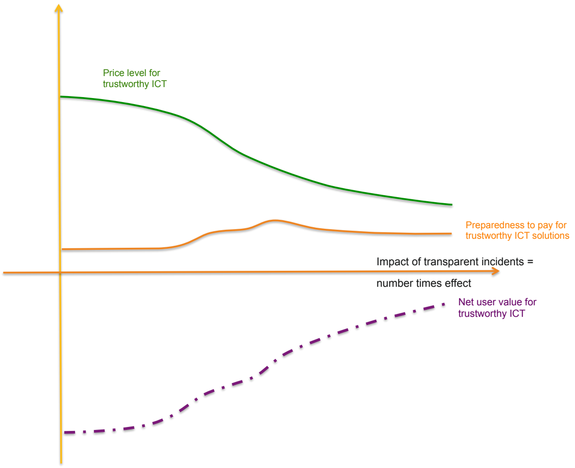


Figure A3b Negative scenario: the net user value (the dashed line) remains negative as a result of low preparedness to pay.

The graph of net user value for trustworthy ICT shows areas where:

- the net value is negative: trust is seen a burden and needs to be subsidized to increase the adoption; and
- the net value is positive: where trust is seen as benefit and trust is self-propelling, (see Figure A4).

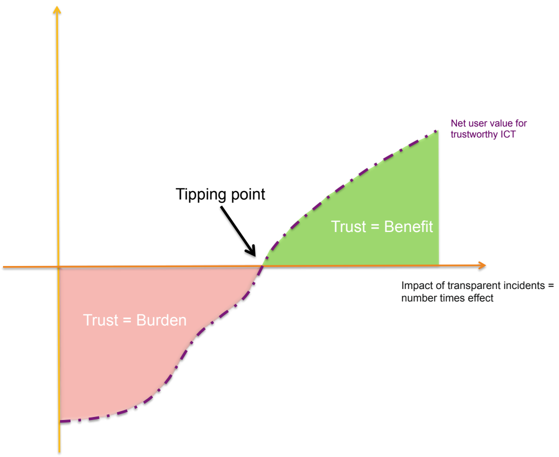


Figure A4a: Positive scenario:
the net user value for trustworthy ICT with a tipping point in the middle between trust being seen as benefit and trust being seen as a burden. The Y-axis represents net user value for trustworthy ICT (dotted purple line).

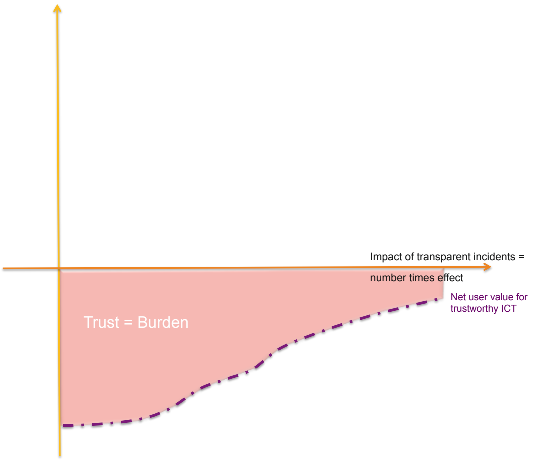


Figure A4b: Negative scenario:
trust will be seen as burden for a domain where the preparedness to pay is very low. The Y-axis represents net user value for trustworthy ICT (dotted purple line).

The key business challenge is to increase the net user value of trustworthy ICT solutions and, thus, the adoption rate (see figure A5). In addition to the positive effects of law enforcement and regulations, this can be achieved by actions that:

- decrease the costs associated with the development and maintenance of trustworthy ICT,
- increase the perceived need for trustworthy solutions, and
- increase preparedness to ‘pay’ for it. Paying does not automatically mean that ICT will become trustworthy.

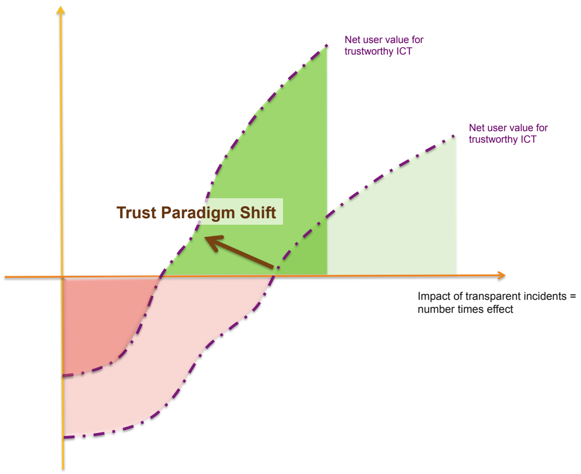

Net user value for trustworthy ICT
Net user value for trustworthy ICT
Trust Paradigm Shift
Impact of transparent incidents = number times effect

Figure A5a: visualisation of the trust paradigm shift in the positive scenario: interventions that can cause a shift, i.e. speed up adoption and increase value for th user. The Y-axis represents net user value fo trustworthy ICT (dotted purple line).

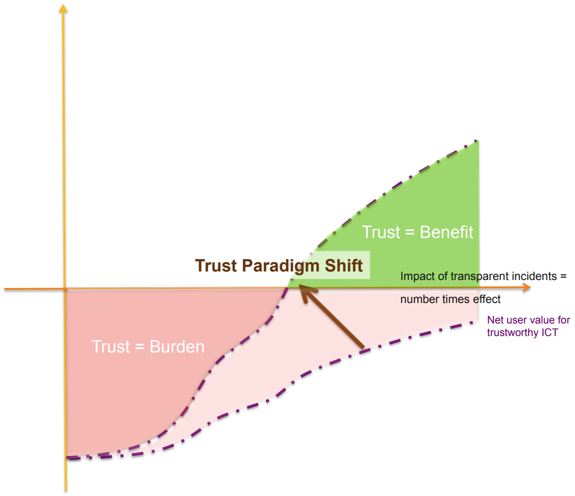

Trust = Benefit
Trust Paradigm Shift
Impact of transparent incidents = number times effect
Trust = Burden
Net user value for trustworthy ICT

Figure A5b: visualisation of the trust paradigm shift in the negative scenario: interventions that will cause a shift from trust are seen as a burden, to trust being seen as a benefit. The Y-axis represents net user value for trustworthy ICT (dotted purple line).

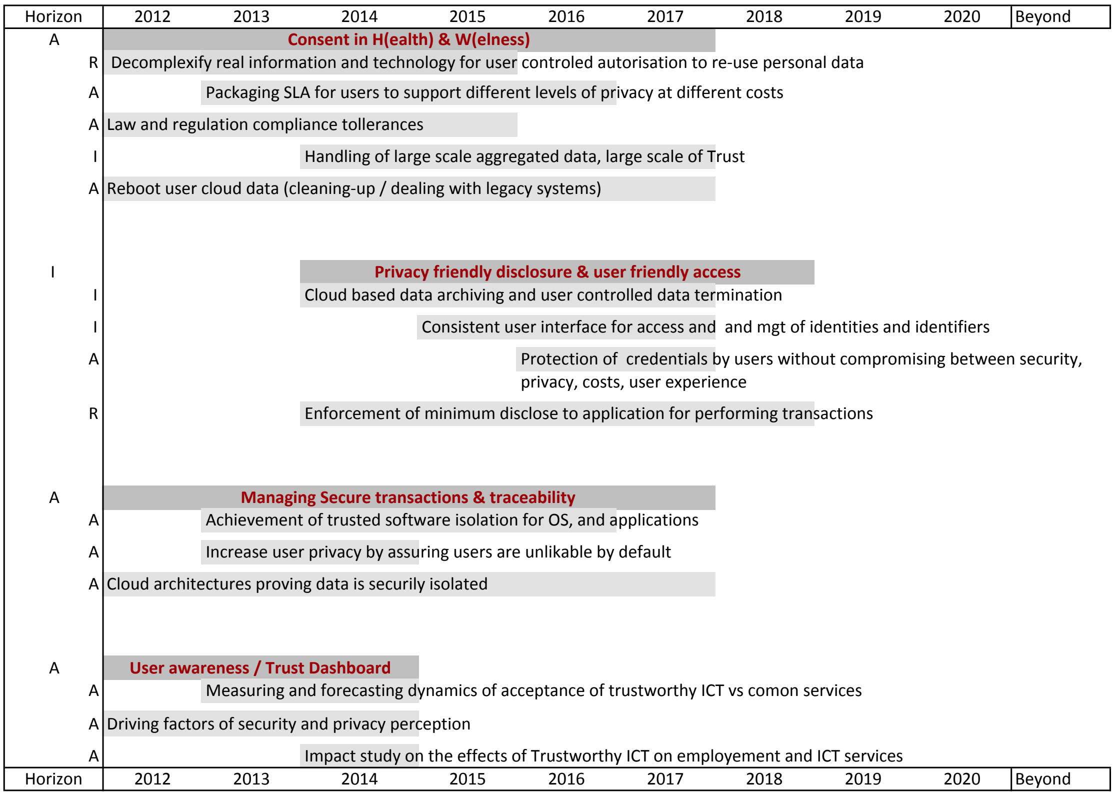
The target of the Trust Paradigm shift is to enable a payment scheme that involves various players leading to an overall gain for users (e.g. consumers and business users), providers and society as a whole. Transparent payment can be direct, but may also indirect (e.g. via suppliers or service providers), or even enforced by regulations that require certain trust levels (in specific domains) to operate a (trustworthy) service. Regulations and enforcement by law can strengthen and speed up the paradigm shift.

Appendix B1: Trusted Stack roadmap for Horizon 2020

Horizon	2012	2013	2014	2015	2016	2017	2018	2019	2020	Beyond
I	**Managing trust via reputation systems**									
R		Protocols and policies to build and maintain trust								
I	EU Protection of citizens									
A		personal risk profile ~ personal risk acceptance level								
			Future architecture to enforce end-to-end trust							
I		**Distributed enforcement by policies**								
I		Mapping of the trust model on legal systems and law protection								
I			Accountability and enforcement of rights in end-to-end trust							
I		Evaluation of trust in distributed systems								
I		Composition of end-to-end trust bесed on network of trusted sub elements								
I	**Measeurment End-to-end trustworthiness**									
I		Health status and protection of the PC / device								
I	Model driven security and consistency of policies integrated in system engineering									
A			Notification and recovation schema's for incidents							
I	Levels of trust and factors that influence trust in context dependency									
R	**Harmonised E-identity infrastructure / Trust Framework**									
R				Information system security for ID federation for heterogeneous domains						
R				Disclosure of of attributed on need to have basis						
R					Optimise accreditation proces for critical components					
R	Claim based E-authentication									
R	Connectivity Stork platform									
R						Automated (legislation) certification service provision				
A				**Traffic analysis privacy architecture**						
I				Increase end user usability of ToR						
A					Risk monitoring and risk assessment tooling for services, devices and platforms					
A				Traffic threat model						
I						Usable anonymizing network				
A				Protection against end-to-end time attacks						
Horizon	2012	2013	2014	2015	2016	2017	2018	2019	2020	Beyond

Impact on paradigm shift
A - Accelerate adoption ~ impact of transparant incidents
R - Reduction of the price level for trustworthy ICT
I - Increase net user value for trustworthy ICT

Appendix B2: Data Life Cycle management roadmap for Horizon 2020

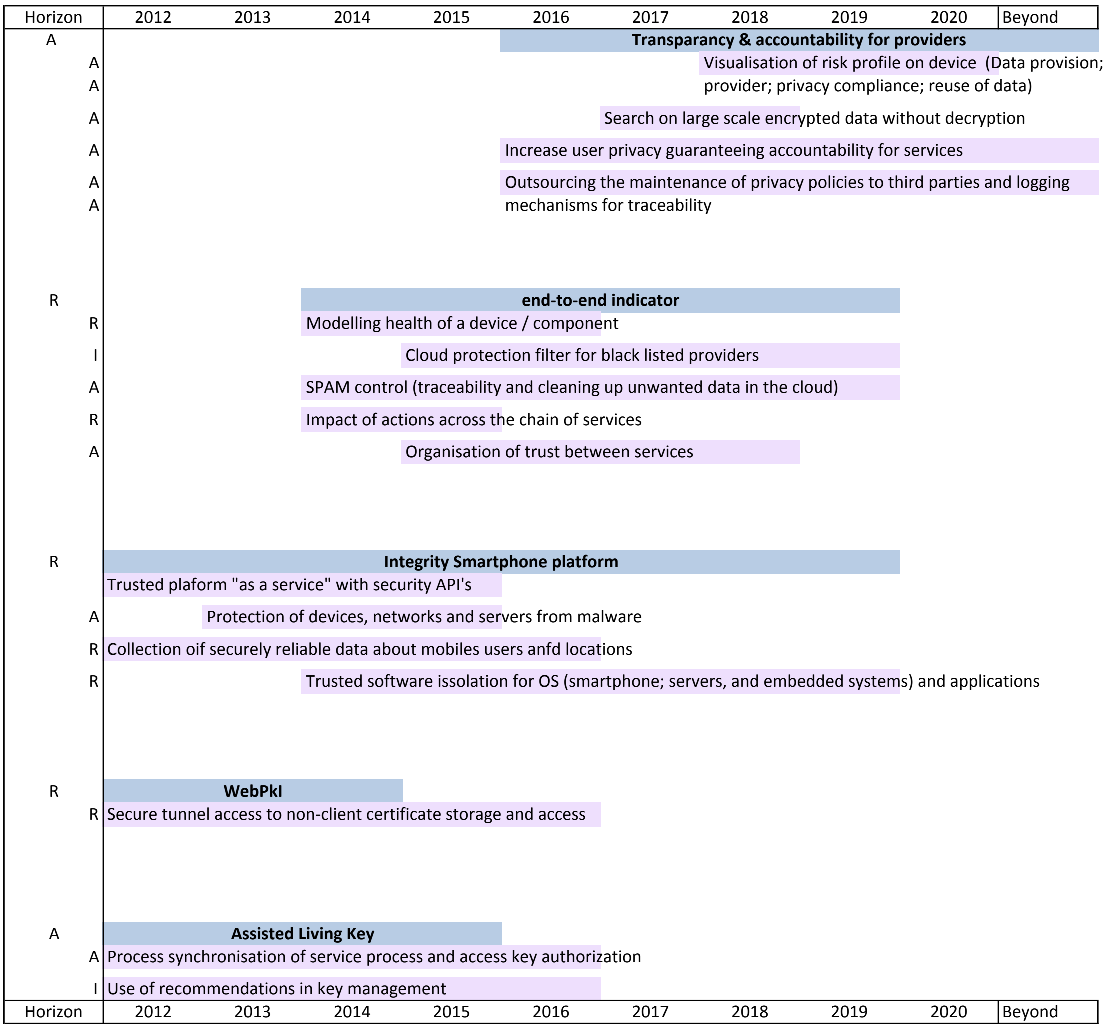


Horizon		
A		**Consent in H(ealth) & W(elness)**
	R	Decomplexify real information and technology for user controled autorisation to re-use personal data
	A	Packaging SLA for users to support different levels of privacy at different costs
	A	Law and regulation compliance tollerances
	I	Handling of large scale aggregated data, large scale of Trust
	A	Reboot user cloud data (cleaning-up / dealing with legacy systems)
I		**Privacy friendly disclosure & user friendly access**
	I	Cloud based data archiving and user controlled data termination
	I	Consistent user interface for access and and mgt of identities and identifiers
	A	Protection of credentials by users without compromising between security, privacy, costs, user experience
	R	Enforcement of minimum disclose to application for performing transactions
A		**Managing Secure transactions & traceability**
	A	Achievement of trusted software isolation for OS, and applications
	A	Increase user privacy by assuring users are unlikable by default
	A	Cloud architectures proving data is securily isolated
A		**User awareness / Trust Dashboard**
	A	Measuring and forecasting dynamics of acceptance of trustworthy ICT vs comon services
	A	Driving factors of security and privacy perception
	A	Impact study on the effects of Trustworthy ICT on employement and ICT services

Impact on paradigm shift

A - Accelerate adoption ~ impact of transparant incidents
R - Reduction of the price level for trustworthy ICT
I - Increase net user value for trustworthy ICT

Appendix B3: Mobile Service & platform Roadmap for Horizon 2020



Impact on paradigm shift

A - Accelerate adoption ~ impact of transparant incidents
R - Reduction of the price level for trustworthy ICT
I - Increase net user value for trustworthy ICT

Appendix C: Research Questions

General research questions related to trust

Main questions:

- What are the most important factors that influence trust and which can be used to model and evaluate trust?
- What are the expectations of European citizens regarding trust in digital life?
- What are the dominant application areas within digital life that shape the perception of trust?
- What are expressive indicators of trustworthiness?

Additional questions:

- What different kinds of trust exist in the information system environments? What are the different levels of trust? What level of granularity is needed for trust?
- What does the European citizen expect from trust in digital life in the long-term? What are the expressive indicators of trustworthiness in digital life?
- What are the most important factors that influence trust (context dependency)? How to model trust in different environments?
- What is the interplay between privacy and trust? How to model privacy? How to make sure that people do not have to give up (too much) privacy when they want or need to gain trust (e.g. in reputation systems)?
- How to compose trusted elements to achieve end-to-end trust?
- How to evaluate trust in a distributed system?
- How to enforce and maintain trustworthy behavior? What policies and protocols are needed? What are the costs of maintaining trust?
- Who is liable/responsible for what in end-to-end trust? How to organize liabilities, and against whom do you need to enforce your rights? How to map the trust model to the actual legal system(s)?
- What are the costs of breaking trust? What is the impact of the price/cost/free nature of the service?
- What is the relation between risk and trust and what mitigation techniques can be applied?
- How can an EU Citizen be guaranteed EU protection? Are there differences when comparing consumer protection for the sale of goods and the sale of e-services? If yes, are there justifiable grounds for that? What would be the impact on trust if submitted personal data would be regarded as a payment?
- How to combine people, process and technology to deliver trust? How can users make informed decisions on which information is needed to be shared to applications?
- What is the incentive for users to protect their privacy/security.

Research questions related to architectural framework

Main question:

- What future architectures are needed to establish and maintain end-to-end trust? What are the best architectures for complex authentication/identification systems?

Additional questions:

- How can we enforce minimal disclosure so that applications only request the sensitive information they require to perform a transaction?
- How can we distribute trust assumptions over multiple parties? How can we reduce the impact of a rogue administrator? How can we avoid the possibility of a rogue administrator impersonating or compromising users being managed?
- What are the notification & revocation schemes when things go wrong?
- How can users protect their own credentials, while not compromising a balance on security, privacy, mobility, costs and user experience?
- How to disclose only the attributes which are necessary for an application? How to prove attributes?
- How can we reduce the dependency on Claims Providers from an availability perspective, and also from a trust perspective?

Research questions related to data life cycle management

Main question:

- How can we ensure trusted data life cycle management in information systems i.e. w.r.t. data creation, access control, sharing, usage, storage, archiving, back-up, and termination of data.

Additional questions:

- How to handle large-scale aggregated data, especially when dealing with trust in the Internet-of-Things (large scale trust).
- How to reduce the complexity of real information and make it useable, transparent and understandable for users?
- How to model and determine the (re)liability of data? How to verify the source of data and the source of service?
- How to prove data is stored and their characteristics, access etc., operations on encrypted data? How to do multi-dimensional data security analysis?
- Identify the missing trust elements when we move from paper to digital data management, i.e. w.r.t. data creation, access control, storage, termination of data, usability of trust management mechanisms
- What are the solutions for usability for identity systems in the Cloud including easy handling and visualization of privacy? How do we handle the identity of objects attached to the Cloud?

- Advanced access control to Cloud resources including policies, enforcement, auditing and ability for users to:
  - track what is going on and intervene (e.g. a Kill button),
  - track what business is done with my data (selling, deletion),
  - select a jurisdiction and the law to be applied.
- How to search efficiently on large scale encrypted data without decrypting it?
- How to achieve a workable framework for cross-border data transfer: towards reconciling workability for businesses and location-(in)dependent user trust?

Research questions related to platform and service integrity

Main question:

- How to compose platforms and services of multiple people/sources (e.g. adaptive heterogeneous complex service composition) and enhance trustworthiness?

Additional questions:

- How to combine services of multiple people/sources, e.g. adaptive heterogeneous complex service composition (incorporating Internet of where many technologies interact with each other, difficult for a user to control data flows in these systems)?
- What is the effect of “outsourcing” the maintenance of privacy policies for services to Third Parties (such as telcos, service providers, friends, peers, etc.). Consider also the “transfer of responsibility” and its limits and interpretations. Consider cloud computing as a prime environment example.
- How can we increase user privacy by ensuring that users are by default un-traceable when they present credentials to applications? How can users make informed decisions on which information is needed to be shared with applications?
- How to ethically collect data about mobile users being fully proportionate and compliant to the consent they have given to the service provider?
- How to package SLAs so users can choose to support different levels of privacy and trust at different cost?
- What is the impact of actions across the chain of services?
- How to organise trust between services, and what is the role of the user in this?
- How do we achieve trusted (i.e. certified in EU) software isolation, i.e. for OS (on servers, smartphones and embedded systems) as well as for applications.
- How to obtain a “Trusted platform as a Service” for cloud, i.e. trusted (security and privacy oriented) platform / application framework with security-oriented APIs?
- How to obtain model-driven security for formal integration of security in system engineering; consistency of security policies and compliance maintenance; and security engineering tooling?
- How to optimise the accreditation process for critical components like source code assessment automation / help, security-oriented API

- How to obtain Information system security for ID federation for heterogeneous domains; embed security as part of the design of system, software and services; adaptive security models at runtime; and security mechanisms designed and assessed with formal methods?
- Regarding software/application stores for mobile devices, what are the minimum requirements for security/privacy checks and auditing before an application can be sold to consumers?

Research questions related to trusted stack

Main questions:

- How to make the trustworthiness of an end-user device transparent to the user?
- How to model the "health" of devices and components?
- How can we increase the level of assurance on the health state of endpoints and how can unhealthy and hacked devices be readily detected? What is a "stethoscope" that we can apply to these devices?

Additional questions:

- How to compose end-to-end trust based on a set of functions that build on each other taking into account the different levels of granularity (ranging from sensor to high level services)?
- How can we increase user privacy while still guaranteeing accountability when required by services or law enforcement?
- How to protect end-user devices, networks and servers from malware?

Research questions related to social and economic impact

Main questions:

- How can we measure and forecast the dynamics of acceptance of trustworthy ICT services vs. common services?
- What are the driving factors behind the security and privacy perception of a consumer and a business?
- How to strengthen the acceptance of trustworthy technology and the Internet?
- What is the business value of trust? What is the value of the attributes that users give away and the risk and costs of losing personal data.
- How does a trustworthy Internet impact the employment and ICT services market in the EU?
- What are the incentives and barriers for the deployment of trust models?