ATTPS | Achieving The Trust Paradigm Shift

D1.2: Impact Assessment

Monitoring Early Indicators of the Trust Paradigm Shift and identifying Opportunities & Threats for Trustworthy ICT in Europe

Final ATTPS Deliverable (Public)

Authors:
Roger Berkley - Bicore
Andres Caballero – Bicore
Maarten Kluitman - Bicore

Editors:
Lydia Kraus – Technical University of Berlin
Alexander Chaloupka – Cryptas

30 October 2015

Contents

Figures

Tables

1 Introduction

Objectives of the work Trust Innovation Funnel (D1.1) & Impact Assessment (D1.2) in the ATTPS project is to orchestrate the trustworthy innovation funnel by driving and coordinating the implementation of the identified roadmaps of TDL Strategic Research and Innovation Agenda (SRA) for the 2020 horizon. ATTPS makes a first step in achieving the trust paradigm shift and will create momentum for its progression. The progress of achieving the trust paradigm shift is monitored, and the social and economic impacts of the Trustworthy ICT Innovation Funnel are determined.

Meanwhile, possible bottlenecks in the trust paradigm shift are identified. Solutions to overcome these possible bottlenecks are also identified and include the enforcement by law as a fall-back. Recommendations for different stakeholders (e.g., industry and government) are provided to speed up the implementation of a national roll-out of proven and usable trustworthy ICT solutions.

More specifically, this document (D1.2) corresponds to task (T1.2) of the FP7-ATTPS project. The objective of T1.2 is to monitor early indicators of the trust paradigm shift. This is achieved through qualitative methods (monitoring the hype in blogs, forums, discussions …) as well as quantitative methods (by means of surveys, data mining, adoption degree in prioritized domains, web traffic measurement & analysis …).

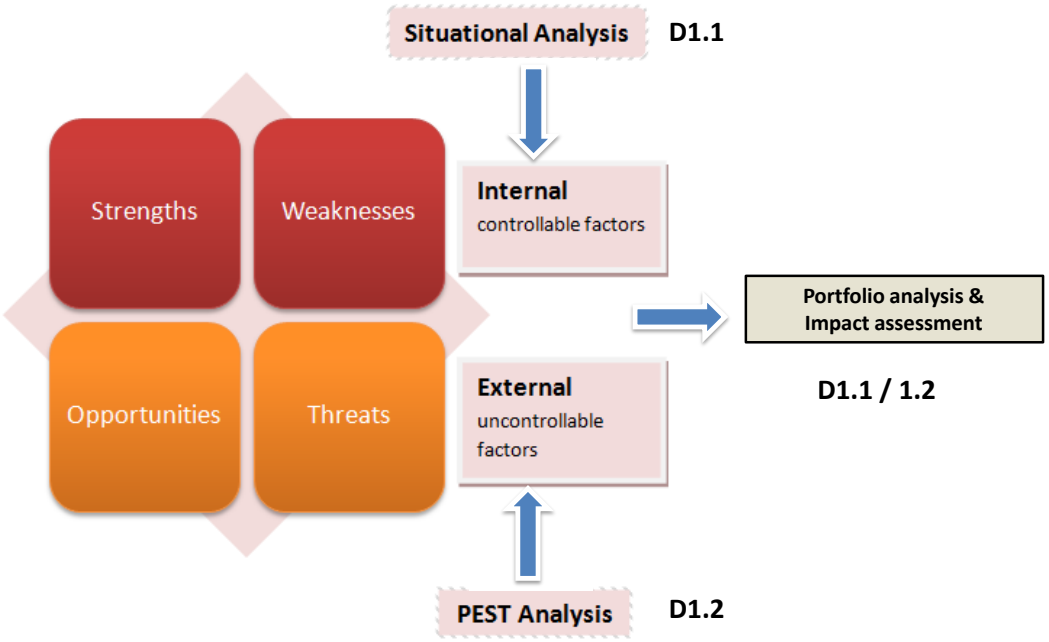


Figure 1: Scheme for Deliverables D1.1 and D1.2

Among the challenges of this study, monitoring the trust in digital life is a peculiar one. It entails observing people's perceptions to digital trust issues. For this reason a challenging aspect is taken into account. As described by researchers Hallinan & Friedewald, public opinions and perceptions are "*notoriously difficult substance to judge given the nuance and constant shift of individual's opinions*" (Hallinan & Friedewald, 2012). This is particularly more problematic in complex and

abstract concepts such as the Trust Paradigm Shift. Some sources of evidence are contradictory when compared to others, so a special precaution must be held at the moment of drawing conclusions.

The analyses of achieving the trust paradigm shift (Figure 1) are performed to:

(1) Identify the essentials and white spots in the roadmap to achieve the paradigm shift.

The roadmap will be developed and described in (D1.1). The fit between the roadmap and the drivers of the paradigm shift will be investigated in (D1.2). Opportunities and Threats for trustworthy ICT in Europe are identified as part of (D1.2).

(2) Identify the gaps for standardization and interoperability.

Standardization and interoperability are two possible drivers of the trust paradigm shift (ATTPS DoW). However, other possible drivers might have more (or less) a catalyst impact for achieving the trust paradigm shift (See project ACTOR). For this reason other drivers need to be investigated and identified first, before identifying the gaps in the roadmap.

(3) Determine social and economic impact.

The social and economic impact of the trustworthy ICT innovation funnel will be determined means of portfolio analysis and research gap analysis in (D1.1).

It is important to note that both deliverables (D1.2 and D1.1) are complementary in nature but differ in approach. D1.1 is focused on internal analysis of European projects in the domain of cybersecurity and trustworthy ICT, and adopts a business research approach portrayed in the portfolio and gap analyses over 100 European projects. While D1.2 is focused on external analysis of European ICT markets and societal needs and perceptions.

Both deliverables, ultimately serve to provide the overall situation of internal and external factors of the Trustworthy ICT initiatives in Europe (See Figure 1).

2 Research Essentials

2.1 Trust Paradigm Shift

A paradigm is a distinct thought pattern. A shift in paradigm is a fundamental change in approach or underlying assumptions that leads to change from one way of thinking to another. It's a transformation that does not *just* happen, but rather it is driven by agents of change. Our paradigm in the ATTPS project is ***perceived user untrustworthiness towards ICT services***. But, establishing trust is essential for releasing the full potential of an information-based economy. Moreover, it is imperative for the European citizen to be assured enhanced security and privacy in the digital world. Therefore, our paradigm shift is ***the move towards increased user trust in ICT services***.

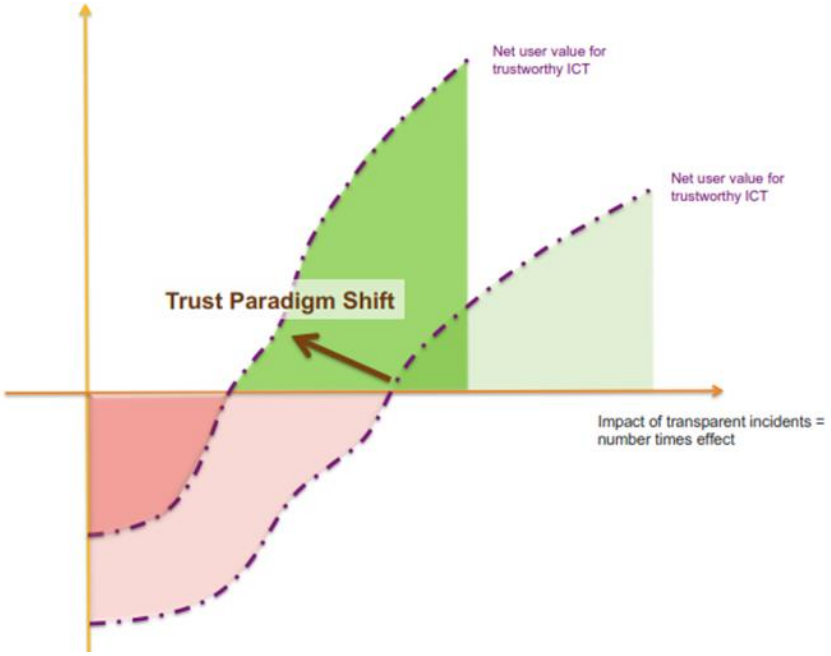


Figure 2: The Paradigm Shift visualized.

Figure 2 illustrates *trust perceived as a burden* and needs to be stimulated (red), and illustrates the climb towards *trust perceived as a benefit* and is self-propelling (green). The paradigm shift directly affects the speed at which this adoption occurs. It includes the move to the Cloud and the "things" attached to the Cloud, which have introduced new trust and privacy challenges to be addressed.

Among the many costs that are incurred in a business to be properly run, organizations need to invest in compliance to standards and to fulfil a number of legal requirements related to trust and data protection. As a matter of financial survival, these expenses need to be recovered either directly or indirectly. An indirect cost in some cases is opting for a punishable-by-law alternative where business interest is in benefit (e.g. when fine costs are more affordable than compliance).

While some expenses can be recovered in general payment schemes; often trust as well as security and privacy are distant from the thoughts of both consumers and service providers as potentially recoverable costs. ICT providers want to keep their prices at competitive levels and also don't see

much purpose to invest in trust since the negative effects associated with the lack of trust (or privacy) are either not realized – when no trust or privacy issues occur – or realized at a later stage but not recorded – when a successful avoidance of a potentially costly incident occurs.

Trust is a firm belief in the reliability, truth, or ability of someone or something. Trustworthiness is a moral value, regarded as a virtue, where the trustworthy subject is regarded as worthy of confidence. Trust plays a decisive role in the acceptance of internet-based services (Benamati, Fuller, Serva, & Baroudi, 2010). But trustworthy services and security don't come for free; therefore someone has to pay the "price" for security. Surcharges are hidden somehow in taxes or service fees. In the case of free internet services, the "price" is paid with the acceptance of some side effects, for example, accepting that user data will be accessed by an online service provider and possibly shared among affiliated service providers. These concessions are ultimately beneficial for third-parties and service provides.

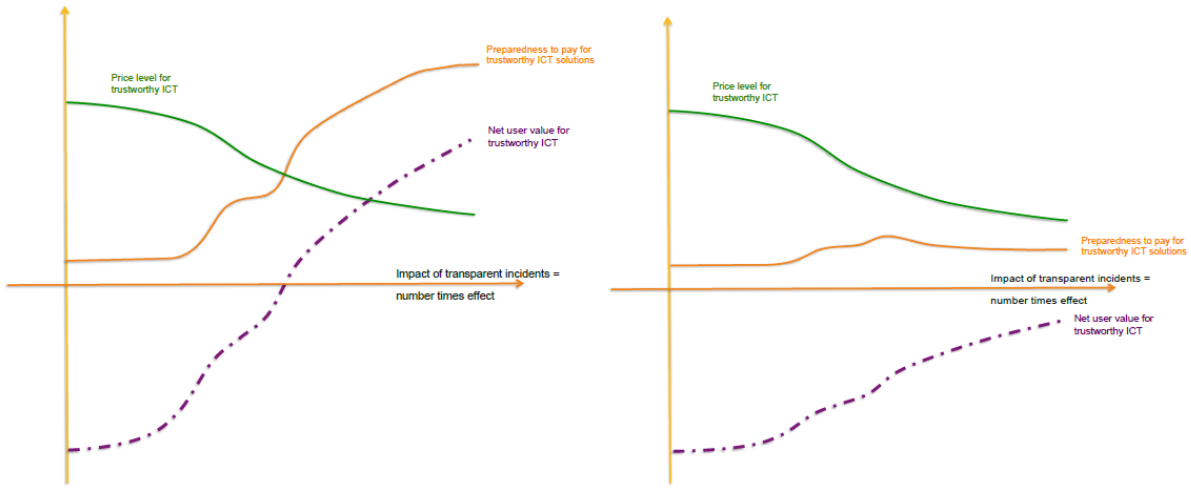


Figure 3: Positive scenario (left) and negative scenario (right) of the Net user value for trustworthy ICT.

In this sense, a lack of transparency over how user data is user and shared among service providers is prevalent. Users are directly paying for trust and security provided with a secure ICT service when a service is provided for a monetary fee; users are also paying for trust and security using their data in "free" online services. For this reason, an increase in transparency on the use of user data is required from ICT providers, and extending the choice for users on "how" to pay for these services is desirable. This explicitly outlines a need to develop business models and environmental (e.g. regulatory) conditions that permit a cost-neutral business case for the development and provision of trustworthy ICT services.

In addition, trust features often stand on the way of functionality (e.g. for example the need of an external random key generator to secure banking transactions). Therefore, trust is desirable for low risk services and a must for high risk services, but it comes at a price, usually affecting ease of use.

Factors that enable a change in trust thinking are (Sarma, Velthausz, & Leijtens, 2012):

1. Awareness and transparent impact of incidents and multiple (*mis*-)uses of provided/gathered (user) data;
2. Perceived user's need for trustworthy ICT solutions;
3. Realization that security and privacy are business enablers;
4. Preparedness/willingness to pay (in different ways) for trustworthy ICT solutions;
5. Regulations: enforcing privacy and security by design.

The relation between these factors determines the perceived price level for trustworthy ICT. The "net user value" for trustworthy ICT is the result of the preparedness to pay and the actual price of trustworthy ICT (see Figure 3).

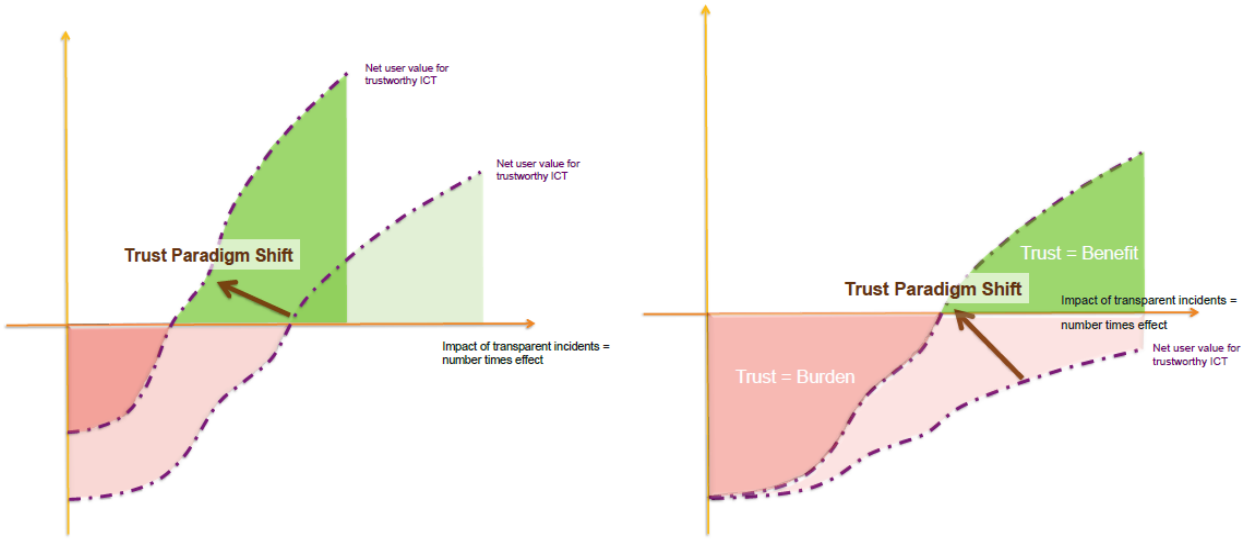


Figure 4: Positive scenario (left) and negative scenario (right) of the trust paradigm shift.

Based on the preparedness of users to pay, there are two possible scenarios (see Figure 4) **a positive one**, where net user value for trustworthy ICT solutions is perceived as a benefit to the user, **and a negative scenario** where the net user value remains to be perceived as a burden. The steepness of the net user value curve is an indicator of the adoption rates of trustworthy ICT, the steeper the curve the faster the adoption.

2.2 Research Methodology

The final version of this document (D1.2) contains an impact assessment of selected ICT innovation fields, i.e. Research Pillars, as follows:

1. Pillar 1: Cloud Computing.
2. Pillar 2: Personal Data Management.
3. Pillar 3: Digital Identity Management.

This assessment is performed on recent research publications from technical, societal, and economical perspectives. A representation of the methodology is shown in Figure **5**. The insights generated are the result product of a thorough analysis, detailed in this document, and also include an iterated validation from external experts.

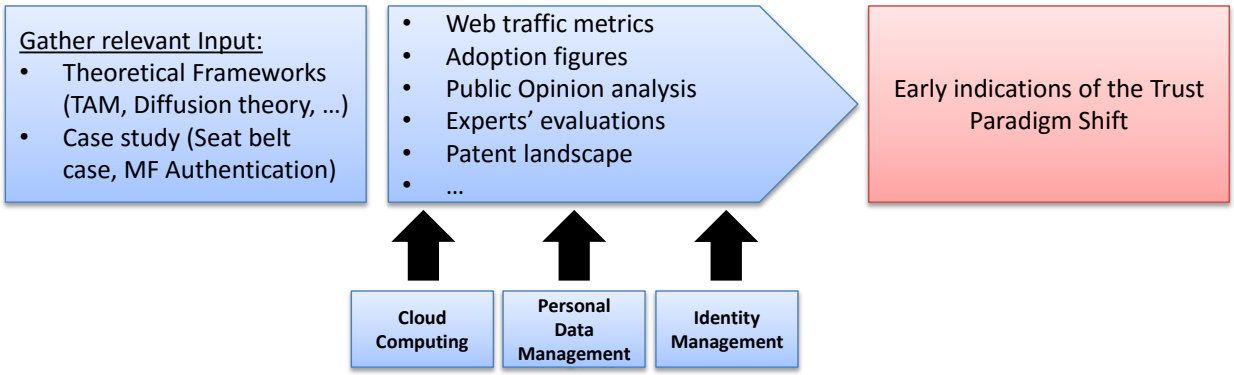


Figure 5: Deliverable 1.2 Methodology

2.3 Research Questions

Part of the ATTPS project and an objective of this document (D1.2) is to monitor early indicators of the trust paradigm shift. For this reason, based on the concepts explained earlier, the following research questions are formulated:

1. What are the characteristics of the Trust Paradigm Shift?
2. What are the indicators for the trust paradigm shift?
3. What are the drivers of adoption of trustworthy ICT, and what is the prevalent adoption model in the market?
4. What is the role of pan-European and national laws & regulations in the adoption of trustworthy ICT?
5. How do users' perceptions influence the adoption of trustworthy ICT?[1]
6. What are future opportunities and threats for trustworthy ICT in Europe?

[1] Insights from ATTPS deliverable D2.2 regarding user perceptions on usability are adopted as part of the analysis performed to address this question.

3 Theoretical Background

Drawing from the diffusion of innovation theory, the perceived attributes of an innovation extend one important explanation for the rate of adoption of that innovation. Rogers (2003) defined five intrinsic characteristics (attributes) that influence an individual's decision to adopt or reject an innovation. Table 1 contains these attributes and their descriptions in addition to a sixth factor (Ability to Communicate Product Benefits) which was added by Mohr, Sengupta and Slater (2005).

Table 1: Six Attributes Affecting Customer Purchase Decisions (Mohr, Sengupta, & Slater, 2005)

Attribute	Description
1. Relative Advantage	The degree to which an innovation is perceived as being better than the one that supersedes it and the benefits of adopting a new technology in relation to the costs.
2. Compatibility	The level of compatibility that an innovation has to be assimilated into an individual's life, based on existing ways of doing things and standard cultural norms.
3. Complexity (or simplicity)	How difficult the new innovation is to use. If the innovation is perceived as complicated or difficult to use, an individual is unlikely to adopt it.
4. Trialability	How easily an innovation may be explored. If a user is able to try an innovation, the individual will be more likely to adopt it.
5. Ability to Communicate Product Benefits	The ease and clarity with which the benefits of owning and using a new innovation can be communicated to prospective customers.
6. Observability	How observable the benefits are to the customer using the innovation, and how easily other customers can observe the benefits being received by a customer who has already adopted the product.

Relative advantage is often expressed as economic profitability, low initial cost, an increase in comfort, perceived social prestige, a saving in time and effort, and immediacy of reward (Rogers, 2003). Diffusion of innovation scholars found relative advantage to be one of the strongest predictors of an innovation's rate of adoption.

3.1 The Certainty and Acceleration of the Trust Paradigm Shift

Researchers suggest that different types of trust develop as trust relationships evolve (Lewicki & Bunker, 1996; Paul & MsDaniel, 2002). When potential users first come across a service, service provider or a technology they will first have to base their trust on factors other than their own experience with the trustee (being a service, service provider or technology). This constitutes the first form of trust, **Initial trust**: rests on trustor judgements before they experience the trustee. Researchers Lewicki and Bunker (1996) define two forms of initial trust:

1. **Calculus-based trust**: in which the trustor assesses the costs and benefits of extending trust. This trust implies the trustor makes a rational decision about the situation before extending trust.
2. **Social-psychological trust**: is based on the trustor's perceptions regarding the trustee's attributes.

Once familiar with a trustee, the second type of trust emerges as **knowledge-based trust** (*or experiential trust*): where the trustor knows the trustee well enough to predict trustee behaviour in a future situation (Lewicki & Bunker, 1996).This type of trust assumes a history of trustor-trustee interactions.

Initial trust and knowledge-based trust are different in that initial trust may erode (decay) quickly, while knowledge-based trust is more persistent. For example, in calculus-based trust, when costs surpass benefits trust fades away based on a rational decision, another example is when a potential user's perceptions are altered because of reading another user's review of a certain service, service provider or technology, where initial trust may crumble if perceptions are negatively affected.

Key to the certainty of the trust paradigm shift is the trust relationship that is formed once knowledge-based trust is established. Lweicki and Bunker (1996) explain that knowledge-based trust increases the likelihood to continue the trust relationship once the trustor is familiar with the peculiarities of the trustee, even when circumstances change or performance lapses.

The persistence characteristic of each type of trust also reflects on the rate of change (i.e., rate of adoption) within the trust paradigm shift. Where, at the early stages of the shift the change occurs rather slowly due to the erosion of initial trust, while this rate increases due to the formation of knowledge-based trust. Moreover, knowledge-based trust of post-adoptive users fuels the social-psychological initial trust of other potential users through publicity and reputation (e.g., word of mouth, user reviews) making the rate of change lean towards exponential growth rather than linearity. The Trust Indicator is based on the exponential growth formula $\mathrm{X_t} = \mathrm{X_0}\ (1 + \mathrm{r})^{\mathrm{t}}$, where $\mathrm{X_0}$ is the value of X at time 0. And r is growth or decay rate (often a percent). The Trust Indicator formula is as follows:

$$T_t = (IT + KT)^t$$

Where;

T: Trust indicator.
t: time $(1,2,3 \ldots)$.
T_t: Trust at time (t).
IT: Initial Trust = 1
KT: Knowledge based trust variable (+/-).

Example 1: initial trust was established from a trustor towards a trustee, knowledge-based trust emerged and was influenced positively by the trustor three sequential experiences by 5%. Calculate Trust indicator following these experiences.

$$T3 = (1 + 5\%)^3 = 1.157625$$

Example 2: Initial trust was established from a trustor towards a trustee, knowledge-based trust emerged and was influenced positively by the trustor first experience $(t = 1)$ by 5%, and by 10% for the second experience$(t = 2)$, and by 8% for the third experience $(t = 3)$ Calculate Trust indicator following the third experience.

After the first experience: $T1 = (1 + 5\%)^1 = 1.05$

After the second experience: $T1 = (1.5 + 10\%)^1 = 1.155$

After the third experience: $T1 = (1.155 + 8\%)^1 = 1.2474$

Finally, researchers of trust have investigated knowledge-based trust in technology and provided evidence that it is technology knowledge that informs post-adoptive use behaviours, not cost vs. benefit assessments (Pavlou P. , 2003) (Lippert, 2007) (Thatcher, McKnight, Baker, & Arsal, 2011). In contrast, constructs based on cost/benefit assessments (e.g., perceived usefulness and perceived ease of use)[2] have less predictive power in a post-adoptive context, but are a good indicator of trust in a pre-adoptive context where initial trust is prominent (Kim & Malhotra, 2005).

In summary, different types of trust play different roles in building a trust relationship. This reflects on the *certainty* and *accelerated rate of adoption* of trustworthy ICT services. The certainty of achieving the trust paradigm shift lies in developing knowledge-based trust, which in turn increases the likelihood of a continued and resilient trust relationship. Knowledge-based trust is also insightful in predicting post-adoption use behaviours. Meanwhile, the accelerated rate of adoption lies in the persistence characteristics of each type of trust, where the nimble erosion of initial trust provides for a slow pick up, and the persistency of knowledge-based trust provides for an accelerated continuation. Publicity and reputation (e.g., raising awareness) of trustworthy ICT services fuel the rate of adoption. And finally, suitable indicators of pre-adoptive trust are cost/benefit attributes like the ones assessed by the Technology Acceptance Model.

3.2 The Case for Preventive Innovations

A preventive innovation is "a new idea that an individual adopts now in order to lower the probability of some unwanted future event" (Rogers, 2003)[3]. A prominent historical example of a preventive innovation is the car seat belt. Other examples of preventive measures are getting an early screening for breast cancer, or adopting contraceptives.

By definition the **relative advantage of preventive innovations is highly uncertain**, making it difficult to demonstrate the relative advantage to possible adopters, as the undesired future event may or may not happen. For example, the fact that an individual has not contracted a harmful virus is invisible and unobservable.

Furthermore, immediacy of reward is a common sub-dimension of relative advantage, and because **immediacy in preventive innovations is rather low**, it explains in part why preventive innovations generally have a slow rate of adoption. For this reason, anything that can be done to increase the perceived relative advantage of preventive innovations can increase their rate of adoption (Rogers, 2002).

[2] Perceived usefulness (PU) and perceived ease of use (PEOU) are the main social-psychological trust attributes assessed by the Technology Acceptance Model (TAM) found within section 3.7 of this report.
[3] p. 233.

Gartner's analyst Dionisio Zumerle discussed mobile security in a conference held in June 2014 and shared an interesting analogy. He compared the evolution of authentication methods to the adoption of seat belts[4]. Zumerle's reflection on car seat belts is that it took more than 40 years for Americans to secure themselves appropriately, even with seatbelts being readily available at that time. A probably explanation for this is that non-adopters felt that the cost and effort required to use the seatbelts is greater than the possible benefit (assuming accident probability) (Rogers, 2003).

Further analysed, the seatbelts case shows important milestones throughout their adoption journey. Most prominently, before seatbelts laws were put in place carmakers saw no benefit arising from installing seatbelts in their vehicles. The overall sentiment was that: *such an addition to their products would increase production expenses and a seatbelt would hardly be used*. Nevertheless, in 1984 (see Figure 6) the first seatbelt laws were enforced in one American state, by 1987 thirty seven states had already adopted similar laws. An adoption rate of 60% was recorded in 1995.

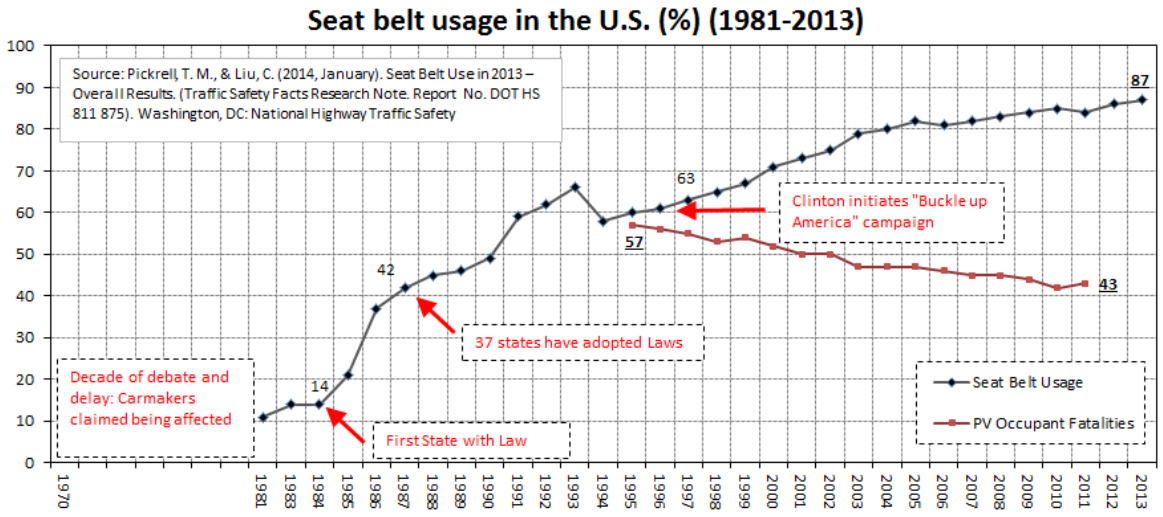


Figure 6: Seatbelts adoption in the United States (1981-2013)

By 1997 Bill Clinton's "Buckle up America" campaign for increasing public awareness was followed by a steady increase in adoption, reaching 87% by 2013. Figure 6 also shows the steady decrease in private vehicle occupant fatalities recorded over the years, while this is not solely associated with seatbelt adoption, since other safety features developed over the time might also have a role, but the correlation among seatbelt adoption and the decrease in fatalities is clearly visible.

[4] Buckle Up: How Seat Belts are Like Mobile Security, Posted by Milja Gillespie in SAP for Mobile on Jun 24, 2014.

Studies suggest that law enforcement has a causal link to seat belt use (Harper, Strumpf, Burris, Smith, & Lynch, 2014). The four elements of the plan in the "Buckle up America" campaign were:

1. Building public-private partnerships;
2. Enacting strong legislation;
3. Conducting well-coordinated education; and
4. Maintaining active, high-visibility enforcement.

Today in 2014, no carmaker builds a car without rigorous security capabilities and seatbelts are perceived as a necessary commodity. Moreover, the extent of change resulted in having safety in a car as an attribute to increase sales.

3.3 Multi-factor Authentication as a Preventive Innovation

In the realm of ICT security: *can trustworthy ICT be considered a preventive innovation?* The answer is a simple yes, since trustworthy ICT is by definition a preventive innovation. Users adopt secure ICT in order to avoid a possible future event (e.g. a cyber-attack, data leakage, privacy intrusion) that may or may not occur and are unobservable. Zumerle's reflection also lies on the fact that current security technologies are readily available, in most cases leaving it up to the user to use these technologies and further secure their digital life.

An analogous case to the seatbelt example related to trustworthy ICT is currently presented: **multi-factor authentication.** An approach to authentication which requires the presentation of two or more (of three) independent authentication factors:

1. **A knowledge factor**: something only the user *knows* (e.g., password, PIN, pattern).
2. **A possession factor**: something only the user *has* (e.g., token, mobile phone).
3. **An inherence factor**: something only the user *is* (e.g., biometrics: fingerprint, retinal scan, iris recognition, DNA sequence).

After presentation, each factor must be validated by the other party for authentication to occur. Several popular web services employ multi-factor authentication using different names, usually it is provided as an optional feature that is deactivated by default. Some web services using multi-factor authentication and their service specific names are shown in Table 2.

Table 2: Web services using multi-factor authentication (indicative non-exhaustive)

Web Service	Multi-factor Authentication
Amazon Web Services	AWS Multi-factor Authentication
Dropbox	Two-Factor Verification
Facebook	Login Approvals
Google Accounts	2-Step Verification/Google Authenticator
Microsoft Accounts	Microsoft Account Security Code
eBay/Paypal	Security Key
Twitter	Two-Factor Verification

Seatbelts and multi-factor authentication share similarities, the authentication technology existed for many years, and it is available for user adoption in well-known cloud services. Yet, users perceive it as an inconvenience and therefore low adoption rates are the current norm. Even if the actual adoption numbers of multi-factor authentication are hard to obtain, deliberate enabling rates of the two-step verification feature in Google range around 2-5%, which means that around 95% of users are either unaware or choose not to use it, according to IT security consultant Paul Moore[5]. The case differs dramatically in corporations. A 2014 survey from SafeNet reveals that 37% of IT leaders enforce the use of multifactor authentication, a number in the rise as the 2013 rate was 30%[6] and a Skyhigh Networks survey suggest that only 14% of Cloud Services Providers (CSPs) offer multi-factor authentication in their cloud services[7].

3.3.1 Multi-factor Authentication Adoption Barriers

Nok Nok Labs examined the reasons behind the low adoption rates of multi-factor authentication provided by internet service providers. After the study, Nok Nok Labs indicated that the three major barriers to this adoption are (1) cost, (2) ease of use, and (3) privacy.

Cost is a major barrier to providing multifactor authentication solutions for consumer applications. The total cost of ownership depends on many variables, including development, acquisition, integration, deployment, support, and maintenance. Adding the cost of providing additional security measures arguably increases the total cost of ownership of internet services. Nevertheless, costs associated with security breaches usually strike high and affect users as well as service providers in different ways. While the user may incur the damage resulting from the loss of high-risk data (e.g., credit card data), internet service providers face the risk of a wide data leakage that affects multiple users or a system breach that gives a level of access and control to attackers.

A study conducted by B2B International in conjunction with Kaspersky Labs[8] (2013) assessed the damages stemming from "*an average security incident can cost a large company about $649,000 in damage, and $50,000 in damage for small and medium sized companies*". While "*a successful targeted attack on a large company can cost $2.4 million in direct financial losses and additional costs, and about $92,000 of the same cost for a small or medium company*". The same study defined the nature of these costs within two main components:

1. Damage resulting from the incident itself (e.g., losses stemming from critical data leakage).
2. Unplanned 'response' costs required to prevent future similar attacks (e.g., software, hardware and hiring/training staff).

[5] https://ramblingrant.co.uk/does-two-factor-authentication-actually-weaken-security/ accessed on 26th September 2014
[6] http://www.safenet-inc.com/news/2014/authentication-survey-2014-reveals-more-enterprises-adopting-multi-factor-authentication/ accessed on 26th September 2014
[7] http://www.skyhighnetworks.com/cloud-report/ accessed on 15th August 2014
8http://media.kaspersky.com/en/business_security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf accessed 30/9/2014

The **ease of use** barrier is why most consumer applications employ a username and password combination for authentication instead of multifactor authentication, which affects the ease of use from an end user perspective. The business logic for this choice is prioritizing ease of use over security, conveying that if the authentication process is more complex consumers will perceive that as an extra burden and will avoid the service.

The **privacy** barrier relates to the ability of an authentication solution to secure factors stored in a user's authentication profile. The user's profile may include personally identifiable data. This data is stored somewhere in digital format and are at risk of a breach just like any other data.

Drawing from the previous selected cases (usage of seat belts and two-factor authentication), we can derive the following question: *How can preventive innovations, such as the trustworthy ICT, accelerate in their rate of adoption?* Aiming at providing an answer and based on extant research, different frameworks and drivers of adoption of secure technology are presented in the following section (3.4).

3.4 Drivers of Adoption of Preventive Innovations

Rogers listed three obstacles to preventive innovation diffusion, where potential adopters:

1. Are **rarely motivated by profit**.
2. Are **often discouraged by professional training, rewards, and values**.
3. Feel that they **cannot make a difference**.

Based on the theory of planned behaviour Overstreet et al. empirically found that attitude (e.g., personal motivation), social norms (e.g., being discouraged by members of their profession), and perceived behavioural control (e.g., feeling of one's ability to make a difference) play a crucial role in the adoption of a preventive innovation (Overstreet, Cegielski, & Hall, 2013).

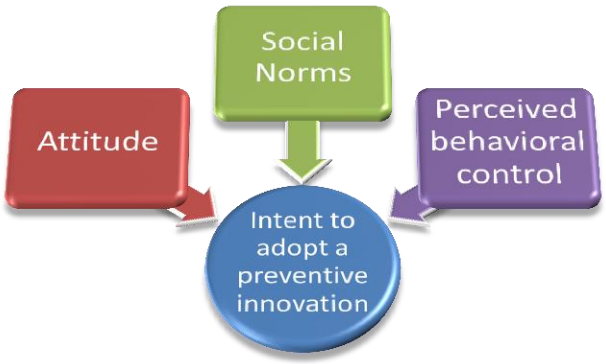


Figure 7: Drivers of adoption of Preventive Innovations.

This research framework suggest that in order to accelerate the adoption of preventive innovations, trustworthy ICT providers need to address individual perceptions by fostering a positive evaluation of the ICT by the potential adopter, as well by those individuals from whom the potential adopter

seeks approval. Perceived behavioural control may be increased by training that explains how the newly adopted behaviour will prevent negative consequences in the future (Overstreet, Cegielski, & Hall, 2013). In summary, ICT providers and policymakers should manipulate the subjective norm and explain how this shift will end up preventing undesired events.

The Global Technology Adoption Index9 findings consider security the biggest barrier for expanding mobility technologies, using cloud computing, and leveraging big data. Security concerns are holding organizations back from further investing in major technologies. For this reason an increase in the adoption of trustworthy ICT is an enabler for the adoption of other technologies.

3.5 Crossing the Chasm to Succeed in the Mainstream Market

Geoffrey Moore has adapted Rogers' theory of diffusion and adoption of innovations for the purchase of high-tech computing products in business markets. His adaptation is shown in Figure 8. Rogers' identified five major consumer categories and Moore's contribution aims at explaining how these categories are reflected within the high-tech business market; Moore also explains how to take high-tech innovations across "The Chasm" and into the mainstream market.

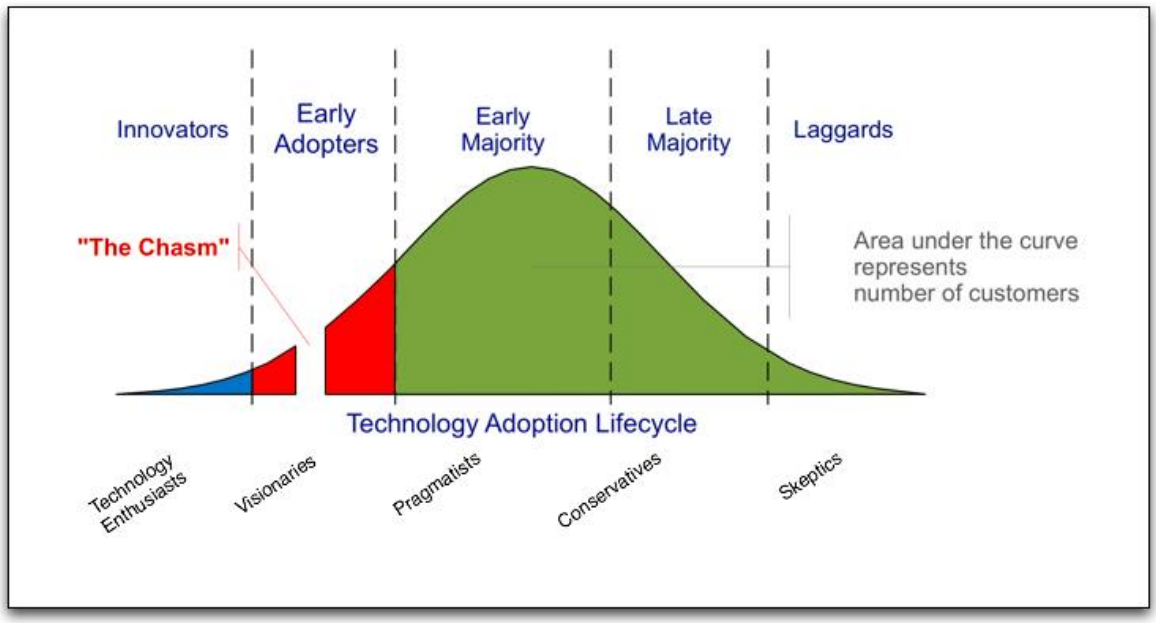


Figure 8: G. Moore's adaptation of Rogers' bell curve on the Diffusion of Innovations **(Moore, 1999)**.

Consumer categories in the high-tech market are the same as those laid down by Rogers starting with innovators and ending with laggards. These categories and Moore's contribution are detailed in the following (Table 3).

[9] Dell Global Technology Adoption Index: http://techpageone.dell.com/betterway/tech-hype-meets-tech-reality/

Table 3: The Categories of Adopters of High-Tech innovations (Mohr, Sengupta, & Slater, 2005).

Rogers' Categorization	Moore's Adaptation	Description
Innovators	Technology Enthusiasts	People who are fundamentally committed to new technology on the grounds that, sooner or later, it is bound to improve our lives. Moreover, they take pleasure in mastering its intricacies, just fiddling with it, and they love to get their hands on the latest and greatest innovations. They are typically the first customers for anything that is truly brand-new.
Early Adopters	Visionaries	The first constituency who can and will bring real money to the table. They help to publicize the new innovations, which helps give them a necessary boost to succeed in the early market.
Early Majority	Pragmatists	These people make the bulk of technology infrastructure purchases. They do not love technology for its own sake, but rather, are looking for productivity enhancements. They believe in evolutionary not revolutionary, products and services.
Late Majority	Conservatives	These customers are pessimistic about their ability to gain any value from technology investments and undertake them only under duress, typically because the remaining alternative is to let the rest of the world pass them by. They are price sensitive, highly sceptical, and very demanding.
Laggards	Sceptics	Not so much potential customers as ever-present critics. As such, the goal of high-tech marketing is not to sell them but, rather, to sell around them.

The Chasm is the gulf between the visionaries (early adopters) and the pragmatists (early majority, mainstream market); it derives from critical differences between the two (e.g., visionaries will think and spend big, whereas pragmatists are prudent and want to stay within the confines of reasonable expectations and budgets). The Chasm arises **because the early market is saturated but the mainstream market is not yet ready to adopt**. In order to reach a mainstream market, an innovation has to ***cross the chasm***.

Multifactor authentication as a technological preventive innovation, although does not burden individual users with financial costs to adopt, has not yet crossed The Chasm in the business-to-consumer market and remains at *Innovators* and *Early Adopters* levels. This is concluded by comparing preliminary adoption figures provided by Paul Moore (i.e., Google two-step verification adoption range 2-5%) against Rogers' estimation for the size of each consumer category (Table 4).

Table 4: Consumer Categories Approximate Size (Rogers, 2003).

Category	Innovators	Early Adopters	Early Majority	Late Majority	Laggards
Size (100%)	2.5%	13.5%	34%	34%	16%

Remarkably, this is not the case in the business-to-business market where motives and drivers of adoption may vary than those of individual users. While individual users may perceive additional steps imposed by multifactor authentication (and negatively affecting ease of use) as a burden that overweighs overall benefits of adoption, whereas, in the business environment corporate policies govern and increase adoption. The accelerating adoption figures in this market indicate that multifactor authentication is at the *Early Majority* adoption level for major IT market leaders in 2014 (37%). While preliminary adoption figures for cloud services providers (CSPs) suggest that multi-factor authentication is at the *Early Adopters* level (14%) (For preliminary adoption figures see part 3.3).

Intriguingly, the marketing strategies aimed at selling to visionaries (early adopters) on one hand, and to pragmatists (early majority) on the other, are fundamentally different. Mohr et al. (2005) state that "*in contrast to marketing to visionaries, who are willing to tolerate some incompleteness in the product and will fill in the missing pieces, marketing to the mainstream market entails the high-tech vendor to assume total responsibility for the solution provided*". **Pragmatists** of the mainstream market like to adopt complete, end-to-end solutions that meet their needs, **they often require the provider to take care of the overall adoption of the new technology**, including assuming responsibility for system integration where required.

The main takeaway from this concept is that the mainstream market is not buying a product to satisfy a technology enthusiasm (as the visionaries do) but to solve a specific need and marketers should address this need by delivering a complete and integrated product. Moreover, a pilot study presented in Deliverable 2.2 of the ATTPS project concludes that "*psychological needs influence users' views and feelings on security and privacy*".

Finally, in terms of multifactor-authentication adoption in the B2C market, where adoption figures are rather low, raising individual users' awareness about the need for adopting higher security authentication practices (on top of the traditional username/password combination) is arguably a more effective approach to reach the pragmatists in this market, other than merely to make the authentication technology available for use, which has more chances of succeeding with the visionaries category.

3.6 Role of Law in the Diffusion of Preventive Innovations

Laws and regulations directly affect social norms and social behaviour. Bernstein (2007) indicates that the law has an expressive function that is distinguished from its coercive function. Firstly, the law's ***expressive function*** operates by sending a message, it publicizes a societal consensus that certain behaviour is required in order to comply with an abstract internalized norm. The violation of the concrete obligation publicized by the expressive function induces behavioural change by producing guilt. This function expresses normative principles and symbolizes societal values. Secondly, the law's ***coercive function*** affects behaviour through enforcement; since failing to comply to law often results in disciplinary action (e.g. fine).

A direct consequence of these moralizing features is behaviour change, in order to comply. Bernstein also indicates that "*technologies that are preventive and non-triable exacerbate privacy threats*"

(Bernstein, 2007). These technologies are prone to be entrapped in a situation where individuals perceive a risk and are consequently reluctant to use the technology. Since the diffusion attributes of preventive innovations (see part 3) make it likely that the perception of privacy threat will affect its diffusion, the expressive function of the law is of particular importance.

Laws and regulations that govern new technologies can be divided into three categories according to their effects on users' perception of risk, as follows (Moses, 2005):

1. First category: where the law undertakes a clear-cut express restriction on uses of the technology that threatens privacy.
2. Second category: where the law undertakes a hesitant stance that includes inconsistent restrictions on privacy-threatening uses of the technology.
3. Third category: where the law may endorse a blanket clear-cut express legal pronouncement not to restrict certain privacy-threatening uses of the technology.

The first category includes laws that are well-defined and sufficiently-defined in keeping up with emerging technologies. In the second category prohibitions are often combined with inaction, this ambiguous stance places the legality of a technology or the use of it in a grey area, producing uncertainty that may inhibit the use of the technology. Finally, laws within the third category which clearly defined the legality of adopting privacy-threatening uses of a technology is counter-productive in terms of alleviating potential users' privacy fears with regards to emerging technologies.

Bernstein indicates that laws in the first category- those providing clear-cut and express restrictions- Are more likely to influence individual's risk perceptions regarding the use of technologies that are preventive and non-triable positively (Bernstein, 2007).

In fact, the erosion of users' trust due to perceived security and privacy threats is usually the trigger for regulatory intervention:

> *The import of trust is only noticed when trust becomes scarce. Usually, we trust man-made technical marvels, such as spacecraft, planes, autos, bridges, and buildings. As long as they work, we seldom think of trust. When they don't (e.g., the Apollo spacecraft or the (recent) Columbia space shuttle), the trust question arises*.
>
> - *Diane M. McKnight* (2005)

To summarize the role of law in the diffusion of preventive innovations, imposing a legal rule that sends a clear message and clarifies an emerging norm consensus is important in engaging with potential users' risk assessment towards adopting preventive innovative technologies. The expressive function of law plays a significant role in regulating technology, since the mere exercise of centralized control can allay public fears regarding potential threatening uses of a new technology.

Individuals are often afraid of the unknown and, therefore, are put at ease when legal principles are exercised to govern new technologies. People are reassured by the existence of limits that the technology is under control. The coercive function of law reinforces compliance by force through applying a corresponding penalty to noncompliance.

3.7 Technology Acceptance Model (TAM) and Trust

Two dominant theories – *trust* and *technology acceptance* – have been employed to understand user behaviour towards technological solutions and innovations.

The *theory of reasoned action* (TRA) is a widely applied theory that is the basis for (TAM); TRA describes how beliefs, attitudes, and behavioural intentions influence a person's behaviour. The *technology acceptance model* (TAM) explains the effects of users' *technology beliefs* on its use, in other words, the TAM theory models how users come to accept and use a technology. But, positive technology perceptions are insufficient to encourage users to adopt that technology.

Models of *trust* focus less on the technology and more on the user's perception of the technology providers. Users' trust concerns towards the provider are critical because of the separation of time and space that occurs in digital life over the internet (Benamati, Fuller, Serva, & Baroudi, 2010), this separation catalyses users' trust concerns towards a service or technology provider.

TAM was developed to explain user acceptance of technology within a business context. It's based on the concepts that beliefs drive attitudes, and attitudes drive intentions, and intentions drive behaviour. TAM suggests two main factors that influence users' decision about how and when they will use a new technology (Davis, 1989):

i. **Perceived usefulness (PU):** the degree to which a person believes that using the technology will enhance his or her job performance.
ii. **Perceived ease-of-use (PEOU):** the degree to which a person believes that using the technology will be free of effort.

Benamati et al. (2010) indicate that the two theories of *trust* and *TAM* complement each other. They propose that users' intentions to adopt a technology are affected by both technology and trust concerns. They also indicate that a technology's *usefulness* and *ease-of-use* facilitate adoption, simultaneously; users' trust in the service or technology provider enables them to overcome the risk associated with being vulnerable to an untrustworthy provider. For these reasons, Benamati et al (2010) state that combining these theories may explain users' intentions and behaviours towards technology in a more comprehensive manner.

Because of the multidimensionality of its meaning and dynamic role, there is no general agreement on the definition of trust (Dimitriadis & Kyrezis, 2010). However, trust has been normally defined in research as: "*the willingness of a party to be vulnerable to or depend on the actions of another party in situations of risk*" (Benamati, Fuller, Serva, & Baroudi, 2010).

Trusting beliefs include the trustor's perception of the trustee's ability, benevolence, and integrity (Benamati, Fuller, Serva, & Baroudi, 2010):

1. **Perceived ability**: the perceived skills, competencies, and characteristics that enable a party to have influence within a specific domain.
2. **Perceived benevolence**: the trustor's belief that the trustee wants to do good towards the trustor.
3. **Perceived integrity**: the belief that the trustee adheres to a set of principles that the trustor finds acceptable.

Shin (2010) studied the effects of perceived security and perceived privacy on the trusting attitude of a potential user. Shin distinguished security and privacy to avoid common confusion, in his study he defined the tangled concepts as follows (Shin, 2010):

A. **Perceived security**: the ability to protect data against unauthorized access.
B. **Perceived privacy**: the ability of an individual to manage information about themselves and thereby reveal themselves selectively.

So far in this section we went through the particulars of TAM and the various trust perception hypothesis tested by different authors. Other than Benemati et al. recommendation to include both TAM and trust perceptions to gain a more comprehensive view on potential users' behaviour towards technology, Yousafzai et al. (2009) states: "*trust has a significant role in predicting technology adoption*" and: "*in order to be successfully accepted, a new technology (or service) has to be perceived not only as useful and easy to use but also it has to include trust-building mechanisms*". For these reasons we will combine TAM particulars *(i,ii)* and trust perceptions (*1,2,3 + A,B)* in one model (Figure 9).

While authors Benemati et al. (2010) and Shin (2010) empirically tested the effects of user perceptions on adoption and provided measured values for these effects, both did so from partial perspectives (Benamati et al. focused on perceived ability, benevolence and integrity, while Shin focused on perceived security and privacy). A study that empirically tests adoption and includes the complete set of factors is not available for our knowledge at this time.

Finally, while TAM *perceived usefulness* and *perceived ease-of-use (i, ii)* both have varying effects on the technological attitude of users, which in turn affect potential users' intention to use or adopt a technology. At the same time, each tested perception hypothesis of the two groups of trust factors laid down by Benamati et al. *(1,2,3)* and Shin *(A,B)* also resulted in varying effects on the potential users'. Nevertheless, all these factors had a **positive effect**. That is, an increase in the perceptions of potential users in any of the seven factors positively affects their technological attitude and trusting attitude, therefore, positively affecting the intention to use or adopt that technology.

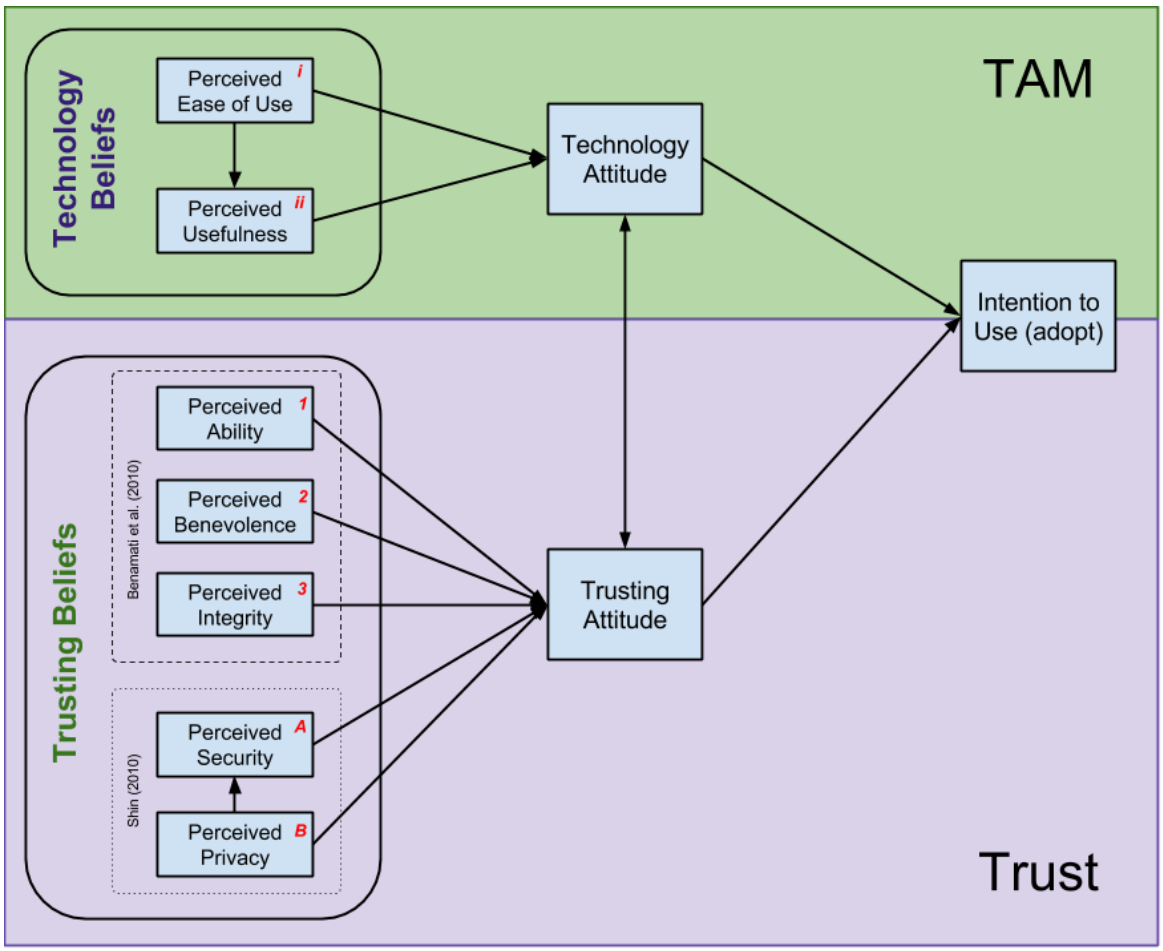


Figure 9: Technology Acceptance Model (TAM) and User Trust Perceptions Combined

3.8 Conclusion

- Trustworthy ICT might have slower initial adoption rates due to the preventive nature of measures required to achieve higher trust in internet services.
- Regulations and compliance, law and enforcement, as well as campaigns for raising awareness can help accelerate this rate. These elements prove effective as they change behavioural patterns and moral conduct.
- Imposing well-defined and sufficient (keeping up with latest) law and regulations to govern the use of innovative technology is crucial for alleviating users' concerns towards adopting new technologies. The expressive function of law plays a significant role in regulating preventive innovative technologies like multifactor authentication.
- In order to succeed in the mainstream market, trustworthy ICT solutions must embody an end-to-end solution that delivers the job that is meant to be delivered with no workarounds. Otherwise, the trustworthy ICT solution will be more inclined towards remaining as a niche product only attractive for early adopters (visionaries), not crossing the chasm and subsequently not reaching the big market portion (pragmatists, the ones who look for a solution to an unresolved need).

- Drawing from the technology acceptance model and scientific literature on trust, it can be inferred that trustworthy ICT is more likely to be accepted if it is perceived as useful, easy to use and trustful.
- Key to increase the net user value of trustworthy ICT is to increase the adoption rate. Actions like (1) law enforcements and regulations, (2) decrease of cost associated with the development of trustworthy ICT, (3) increase of the perceived need for trustworthy solutions, and (4) increase of the preparedness to "pay" for it, will have positive effects in increasing the rate of adoption, thus increasing the net user value of trustworthy ICT services. Leading directly to achieving the trust paradigm shift.

4 Monitoring Early Indicators of the Trust Paradigm Shift

4.1 Introduction

Certainly, monitoring a fundamental change in approach or underlying assumptions that leads to change from one way of thinking to another – or a paradigm shift – is a subjective process. By definition, a measurement in change of a thought pattern on a macro social scale is:

- **Subjective**: ideas, perceptions and beliefs are subjective by nature as they are based on or influenced by personal feelings, tastes, or opinions. Subjectivity is applicable for individual ideas, perceptions and beliefs, as well as communal or societal ones.
- **Loosely-bounded**: monitoring a change of societal way of thinking is a long running process with loosely-defined boundaries. For example, sociologists widely use the theory of generations as a basis for bounding milestones and breakthroughs of long-running societal change. According to the theory of generations "*people are significantly influenced by the socio-historical environment that predominates their youth, forming –on the basis of that experience- social generations that in turn become agents of change and give rise to events that shape future generations*." (Mannheim, 1952 - first published 1923).

Moreover, a paradigm shift in user trust towards technology is also subject to technological advancement and possible disruptive change (user awareness of such advancement is key), an example of this is increased user trust in conducting online payment transactions as a result of using a trusted third-party payment service (e.g., Paypal) which acts as a trusted intermediary between the user and an online e-commerce service.

Three fundamental areas were identified as major actors in the current ICT arena, with a focus on trustworthy ICT:

1. Cloud Computing.
2. Personal Data Management.
3. Identity Management.

While capturing views on the dynamics of these industry sectors and their characteristics and drivers towards trustworthy ICT in specific, we found in those fields sufficient evidence to build an opportunities and threats assessment for trustworthy ICT. The pervasiveness and impact of these sectors in the overall industry is the main reason they are considered as key areas.

For the half-century that computers have been part of the workplace, companies have bought their own machines for corporate data centers, Cloud Computing may just change that. In fact, cloud computing powers thousands of workplace software programs, mobile games and advanced research programs already. Cloud services harness global networks of millions of computers, renting and using huge amounts of computing powers, opening up possibilities that were unthinkable a few years back. One of the top ranking perceived risk of adopting cloud computing is security & privacy, for this reason cloud computing is a good indicator for trustworthy ICT adoption.

Secondly, Personal Data Management is where public opinion has the most to say. If Cloud Computing can show strong evidence signs in the Business to Business sector, Personal Data Management will cover for the Business to Consumer segment. People's opinions will be formed mostly from regular-user applications and solutions. Third, the Identity Management has been chosen as it's an emergent ICT offering that can provide signals of yet-to-come tendencies in the sector. Choosing this third field aims at not only sensing early indicators in well-established services but also in the new alternatives that are becoming available as well as people's reactions towards them. For these three fields we aim to understand how recent events and facts can serve to gauge an apparent shift in trust. Next, a set of conclusions will be drawn. Table **5** highlights the type of evidence that will be presented during the rest of this section:

Table 5: Example of Early Indicators of the Trust Paradigm Shift

ICT field	Example of Early Indicator of a paradigm shift
Cloud computing	• Adoption of security standards and compliance with certification bodies • Patents filing facts • Expert's surveys results (e.g. EY, KPMG, and others) • Reports on Cloud Services adoption • Surveys gauging impact of security incidents (e.g. spying programs) • Data storage location proportions • Tendencies in search engines and social media • Experts' opinions
Personal data management	• Web traffic metrics (rankings and bouncing rates) of online security services • Results of surveys gauging public opinions towards trust, privacy and security concerns • Monitoring of evolution of monetization of personal data (adoption, tendencies) as a new way of handling the issue of private data sharing • Expert's opinions
Identity Management	• Adoption of new identity management services • Hot research topics in identity management • Expert's opinions • Limited disclosure technology emergence • Multifactor authentication adoption

4.2 Pillar I: Cloud Computing

4.2.1 Introduction

Perhaps, the most circulated definition of Cloud Computing has been provided by the National Institute of Standards and Technology (NIST):

> *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*

Cloud computing promotes high-availability and is characterized by providing on-demand self-service computing, broad network access, resource pooling, rapid elasticity to change in demand and resource requirements as well as the ability to robustly scale to handle unexpected spikes in user demand. Cloud computing services provision these capabilities to businesses in a measured fashion, following a *'pay-as-you-go'* and *'pay-as-you-use'* model simultaneously. Key enabling technologies of cloud computing include: (1) fast wide-area networks, (2) powerful inexpensive server computers, and (3) high-performance virtualization capabilities for commodity hardware.

Cloud computing services are shaped by three widely recognized service models (e.g. SaaS, PaaS, IaaS), as well as four main deployment models (e.g. public, private, community, hybrid). Both service models and deployment models dictate and govern the distribution of responsibilities (e.g. security) among CSPs and cloud service consumers or users. Figure **10** illustrates the essential characteristics of cloud computing services that are extended to users through defined service models over different deployment models.

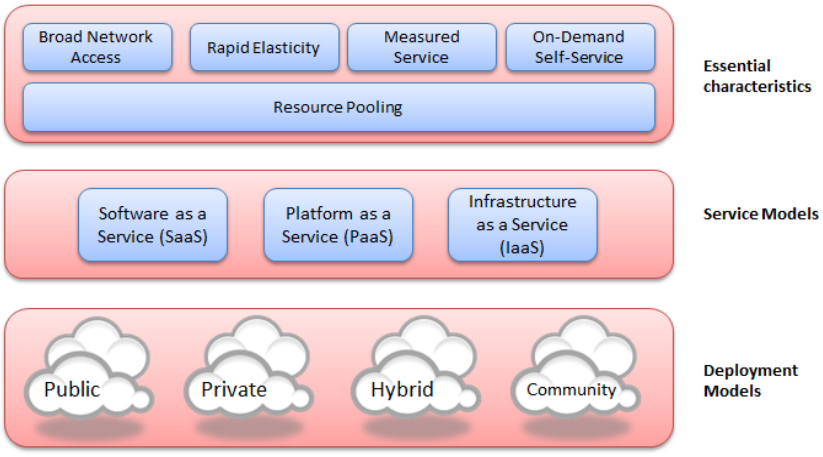


Figure 10: Essentials of Cloud Computing

4.2.2 Theoretical Background

4.2.2.1 Three Service Models

Cloud computing services can be provisioned at different levels to match a range of end user needs and requirements. Each of these service levels provides computing utility over the network and each introduces its division of responsibilities among the cloud service provider and the end user differently. Services range from 'high' levels of service provided through SaaS, where the majority of tasks (e.g. infrastructure management, software development, maintenance, deployment) are the responsibility of the CSP. To 'lower' levels of service is provided through IaaS, where bare computing resources are provisioned to service consumers.

1. **Software as a service (SaaS):** this service model provides full-fledged software applications to the end user. It portrays the highest level of service provided by cloud vendors in the form of ready-to-use applications deployed in the provider's cloud environment. These applications are accessed through a client interface (e.g. web browser) and are accessed over the network. In this model the end user does not control the underlying cloud infrastructure not the provided software applications, leaving the operations and maintenance responsibilities to the cloud provider. Examples of this model are Google Docs or CRM cloud based applications (e.g., SalesForce) (Berkley, Jamous, & Ozokan, 2013).[10]

2. **Platform as a Service (PaaS):** this service model provides the environment for developing and provisioning cloud applications. The end user is able to deploy their own applications which are created using their preferred programming languages, libraries, web services and tools supported by the cloud provider. End user is not capable of managing the underlying cloud infrastructure, but has control over the deployed applications. In this model elasticity and scalability of the applications are the cloud provider responsibility, as well as the distribution of the applications to the infrastructure. The responsibility for security is shared among the provider (i.e. infrastructure security) and the user (i.e. native application security) (Berkley, Jamous, & Ozokan, 2013).

3. **Infrastructure as a Service (IaaS):** this service model gives more control and responsibility to the consumer to write and deploy their applications over the cloud provider's infrastructure. The cloud provider supplies the resources (e.g., virtual machines, storage, networks, firewalls, load balancers), these are readily-available for the end user to install an operating system image and maintain it themselves. While it's evident that the end user has full control of designing, developing, deploying and running their applications, yet they do not manage the underlying cloud infrastructure. An example of this model is Amazon Web Services or Microsoft Azure (Berkley, Jamous, & Ozokan, 2013).

[10] https://www.academia.edu/7678674/A_Heuristic_Mathematical_Decision_Support_Model_for_SMEs_Cloud_ERP_System_Adoptability

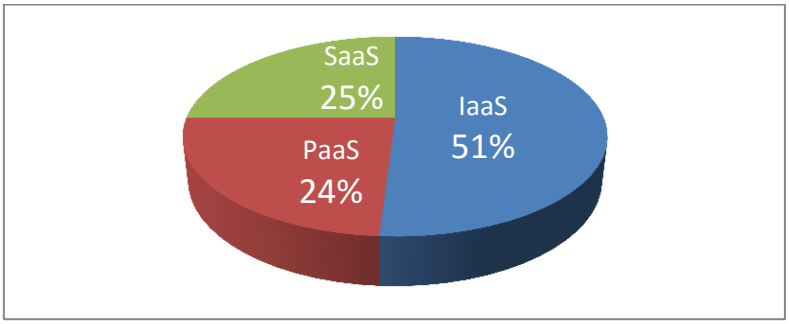


Figure 11: Market Share by Service Model for 2012 (Source: 451 Research)

4.2.2.2 Four Deployment Models

Cloud services can be deployed in different ways, depending upon many factors, such as: the organizational structure, hosting location, datacenter ownership, **security requirements**, desire to share cloud services, the ability to manage some or all of the services, customization capabilities. Four deployment models are usually distinguished, namely public, private, community and hybrid cloud service usage.

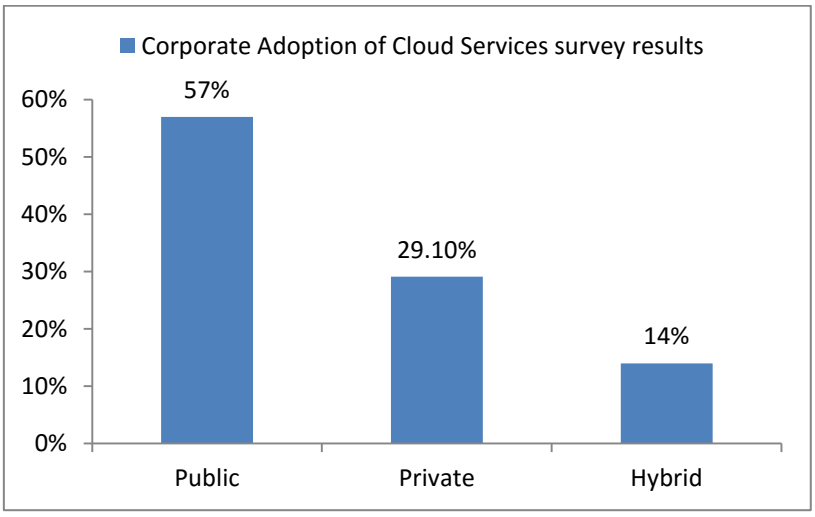


Figure 12: Organizational adoption of cloud services based on deployment models (Deloitte, CIOnet 2011)[11]

1. **Public:** a public cloud is available to the general public (businesses and individuals alike) and is owned by a CSP. In a public cloud the CSP dynamically provisions computing resources over the internet to various end users who share resources (resource pooling and virtualization). Similar in fashion to that of a utility billing system where consumers pay for their share of resource consumption. Public clouds can be the most effective deployment model for organizations or companies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability.

11 http://webserver2.deloitte.com.co/Consultoria/Cloud%20Adoption%20Survey.pdf accessed on 29/9/2014

Nevertheless, to benefit from a public cloud an organization (or individual end user) must accept the **reduced control and monitoring over the CSPs governance and security**.

2. **Private:** a private cloud is operated solely for a single organization. The cloud owner has full control over the specifics, architecture and services deployed on their cloud to be delivered for their private consumption. A common reason for organizations and companies to procure or build private clouds is their ability to **enforce their own data security standards and controls**.

3. **Community:** a community cloud is procured jointly by several organizations or companies that share specific needs such as security, compliance, or jurisdiction considerations (e.g. community of medium-sized Dutch insurance companies). Community clouds enable organizations who have a common set of requirements to capitalize on combining and sharing their computing resources, storage, data and capabilities, **while maintaining control over their cloud policies (e.g. security levels) to match their similar requirements**.

4. **Hybrid:** a hybrid cloud comprises two or more clouds (private, public, community) with a mix of both internally and externally hosted services.

4.2.3 Analysis

4.2.3.1 Cloud Computing Adoption and Trust Concerns

Over the last few years global cloud computing revenue steadily grew. The year 2012 recorded a $5.7BN revenue for global cloud services. Market Monitor (Peraza & Zwakman, 2013) report on cloud computing estimates that this figure will grow by 36% CAGR[12] by 2016, Figure **13**: Global Cloud Computing Revenue (Source: 451 Research)Figure **13** illustrates this projected growth.

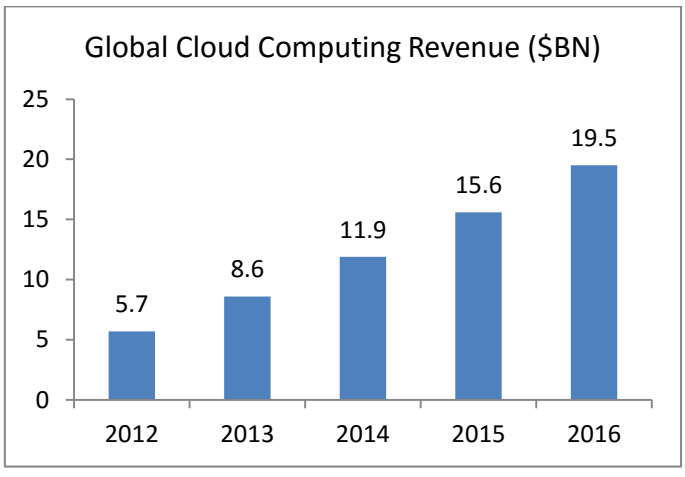


Figure 13: Global Cloud Computing Revenue (Source: 451 Research)

[12] Compound Annual Growth Rate.

In addition to global cloud computing revenue indicating an increase in adoption, a cloud usage survey on the actual use of cloud computing services by enterprises returned an 11-point increase in public cloud usage over a year between April 2012 and April 2013. The results brought by ChangeWave Research (Crumrine & Deb, 2014) are illustrated in figure 14.

North America accounts for the vast majority of cloud computing revenue for 2012 at 62%, Europe (as part of segment EMEA[13]) ranks second with 23%[14], and this adoption gap is rather unusual. Europe, being a developed market for technology innovation where adoption of new technologies is considered a competitive advantage is moving to the cloud rather slowly. This can be explained with a few different reasons. First, cloud ease-of-adoption is an advantage for startups looking to save initial investment by not buying hardware, especially considering that startups intend to grow fast in the early years. Traditionally, there have been more startups based in North America than in Europe. This can be explained by the amount of available venture capital, where Europe tends to be more conservative and may take less risk in investments.

A second reason is the diversity of the nation states of Europe. Every European country has its own set of data privacy legislation. When using cloud computing, it is very likely that national boundaries are crossed which adds to the perceived complexity and risk of having data stored or processed in a place other than a CTOs preferred on premise datacenter.

In light of this rate of adoption, Research Monitor estimates that by 2016 EMEA is expected to represent 29% of total global cloud computing revenue[15].

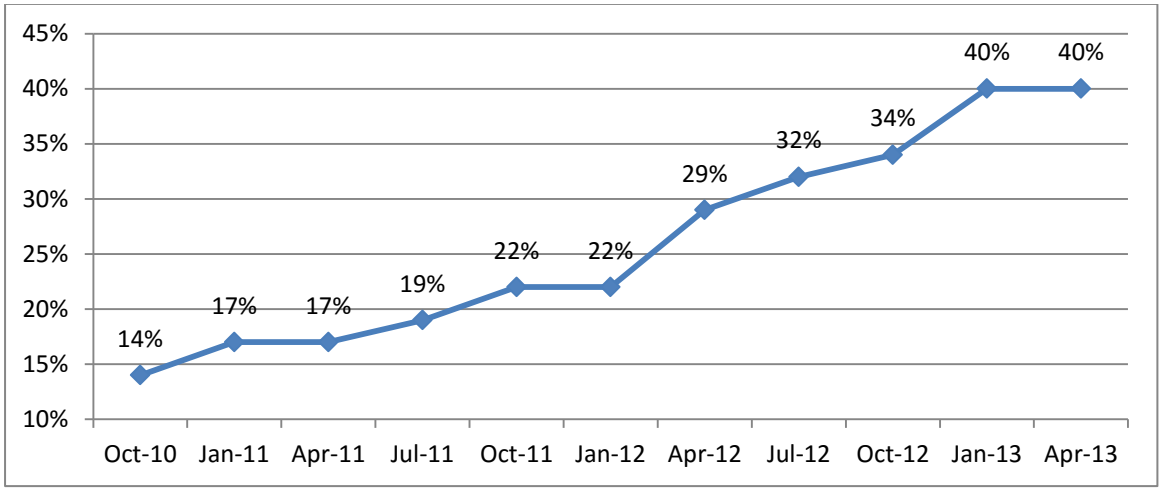


Figure 14: Cloud Computing Usage survey results (source: ChangeWave Research)

However, results from an IDC survey of corporate usage of cloud-based storage solutions (Chute, 2014) show closer rates of adoption among the United States on one hand, and the United Kingdom and Germany on the other (figure 14). We can see that U.S. large and medium businesses are

[13] Europe, Middle East and Africa.
[14] Followed by: APAC 13% and LATAM 2%.
[15] 2016 Estimate: APAC 18%, LATAM 3%.

leading in adoption compared to U.K. and Germany based counterparts, but small businesses from these two European countries are relying more on cloud-based storage solution than their U.S. counterparts.

Chute (2014) survey also measured the adoption rates for different cloud-storage functions (i.e., use cases) and included the following:

1. Data protection: cloud backup.
2. Business continuity: replication, disaster recovery.
3. Archiving.
4. File services and office enablement: sharing, synchronization, collaboration.

The results showed that European SMEs are adopting cloud-based archiving solutions at a faster rate than their U.S. counterparts. And overall, European businesses show higher rates of cloud file services and office enablement adoption. However, data protection and business continuity solutions are taking longer to gain traction in the European markets.

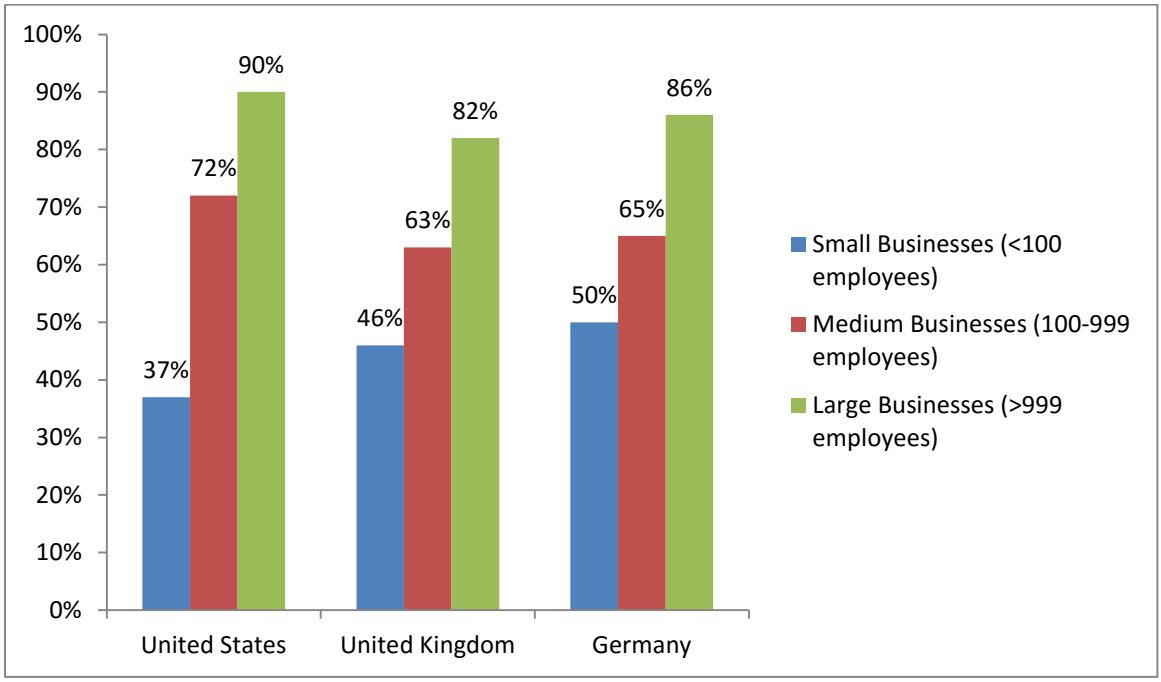


Figure 15: Cloud Storage Adoption Rates survey results (Chute, 2014)

Curmrine & Deb (2013) indicate that the increase in cloud services adoption is primarily for lower-level workloads (e.g., testing and development), and not for mission-critical applications. This is due to workload readiness for public clouds, for which 73% of surveyed enterprises had 25% or less of their workloads ready for public cloud migration. Beyond the issue of workload readiness, Curmrine & Deb (2013) name security concerns and trust issues as primary impediments to cloud adoption. Furthermore, the authors argue that as more organizations actively more (or plan to move) their

workloads to the cloud trust concerns surpass those of security. Since technological improvements in security are laying the groundwork for cloud computing to become more prevalent, there is an opportunity for CSPs to present prospective customers with demonstrable transparency and well-defined security metrics which help appease trust concerns.

Even though security concerns are widely regarded as the main barrier to increased cloud adoption only 2% of Market Monitor (2013) survey respondents believed they had actually experienced a security breach related to the use of cloud services. This result supports the view that as of 2014, and with technological improvements to cloud security, threats associated with cloud security are more exaggerated than the reality of incidents compared to on premise datacenters.

Given these points, cloud computing adoption is evidently on the rise. While North America leads this adoption, the opportunities for an increased rate of adoption in Europe are eminent. From another perspective, managing cloud security and alleviating user trust concerns towards the cloud can benefit from conceived partnerships with cloud providers where responsibilities and metrics are laid down transparently.

4.2.3.2 Security as a Barrier to Increased Cloud Computing Adoption

Adoption rates of cloud computing have been growing in the last years due to the wide-array of benefits it brings to organizations. On the other hand, cloud computing security and privacy concerns have topped the lists of threats and barriers towards increased cloud computing adoption. Cloud Security Alliance's (CSA) "Notorious Nine[16]" list includes the top security threats associated with cloud computing as of 2013. CSA risk analysis of the nine top security threats to cloud computing includes a risk matrix which shows the levels of actual risk and perceived risk for each threat. The majority of these threats rank higher with perceived risk rather than actual risk, as follows in Table 6.

Table 6: Cloud Computing Top Threats in 2013. (Source: Cloud Security Alliance).

Rank	Threat	Description	Risk Matrix (Actual vs. Perceived)
1	Data Breaches	Data leaked to or accessed by unauthorized users.	Balanced
2	Data Loss	Permanent loss of data due to error or catastrophe.	More Perceived
3	Account or Service Traffic Hijacking	Phishing, eavesdropping, data manipulation, redirection.	Balanced
4	Insecure Interfaces and APIs	The security and availability of cloud services is dependent on the security of APIs, these interfaces must be designed to protect against accidental and malicious attempts to circumvent	More Perceived

[16] Cloud Security Alliance: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf

		policy.	
5	Denial of Service	Meant to prevent users of a cloud service from being able to access their data or applications.	Highly Perceived
6	Malicious Insider	Breaches of information confidentiality, integrity or availability by a formerly authorized person.	Highly Perceived
7	Abuse of Cloud Services	The use of cloud services for illegal activities or orchestrating attacks out of the cloud.	N/A
8	Insufficient Due Diligence	Rushing into the cloud without fully understanding the full scope of the undertaking, most notably operational responsibilities such as: incident response, encryption, monitoring.	Highly Actual
9	Shared Technology Vulnerabilities	A compromise of an integral piece of shared technology (e.g., Hypervisor) that exposes the shared environment to a potential compromise and breach.	More Perceived

Cloud security is rarely regarded as a benefit of adopting cloud computing, but it's arguable that certain security concerns are alleviated with cloud computing. For example, data loss is a major concern for enterprises and could have serious implications, storing and backing up data in a cloud protects this data from loss in case a machine (e.g., employee laptop or smartphone) is lost or irrecoverably damaged[17]. Others[18] argue that the cloud brings in security benefits centralized data management and monitoring, where handling and securing large amount of data is simpler than securing data residing in different places and on a variety of devices.

4.2.3.3 Government Spying Programs

A major recent event brought public attention to an additional threat to user privacy. On June 6th 2013 Edward Snowden shared classified information with the Washington Post and the Guardian. The information slides he shared revealed PRISM: a highly secretive government program that allows the National Security Agency (NSA) and Federal Bureau of Investigation (FBI) to retrieve data directly from Microsoft, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.

After becoming public the scandal of NSA espionage on companies and people by Eduard Snowden, some experts have coined the term Snowden effect as the consequence on privacy awareness that might result influencing the cloud computing adoption. After some surveys, some figures are very revealing. The market research firm Vanson Bourne carried out an extensive independent survey of 1,000 ICT decision-makers (60% from Europe) in which the main findings are:

[17] http://www.salesforce.com/uk/socialsuccess/cloud-computing/why-move-to-cloud-10-benefits-cloud-computing.jsp
[18] http://cloudsecurity.org/

- 87% respondents agree that after the Snowden affair, their approach to Cloud Computing has changed to some extent.
- 62% of those still not using Cloud Services feel now prevented to move their ICT to the cloud.
- 72% ICT leaders will revisit their cloud and hosting arrangements to ensure data protection.
- 97% of European ICT leaders will prefer to contract with European Cloud Providers.

Some expert declares that Businesses have become more aware of privacy concerns […] since the NSA Prism program became public knowledge and the fact that the "Largest Swiss cloud provider reported a 45% increase in revenue the month following Snowden's NSA revelations" (Source: The Information Technology & Innovation Foundation) tells of a clear effect on cloud adoption that this affair might have. Some others in this privacy debate that it has mostly a negative impact on US providers: Google, Yahoo, Microsoft, particularly among consumers outside the US.

In the EU, companies have increasingly asked cloud service providers for data location options at a local or regional level (to feel safer…) and after Angela Merkel's declaration to reduce dependency on international providers, it would indicate a potential benefit for local and regional European cloud firms. According to Ed Ferrara from Forrester Research, Europe is especially sensitive to privacy concerns as this region has some of the tightest restrictions on the collection and use of personal information anywhere in the world (Market Overview: Managed Security Services, Europe, Q2 2014). As consumers become more concerned about privacy and security, more companies reconsider the way data privacy and security affect customer's interests. That same study states that companies in Europe are paying especial close attention to this after the revelations regarding the depth and breadth of government spying programs.

A recent study conducted by Skyhigh Networks (Cloud Adoption & Risk Report, 2014 Q2), shows that the average number of cloud services in use by companies has shown a slight decrease in the second quarter of 2014. The reports states that this flattening is not due to decreased supply or demand of cloud services, but due to the result of IT's efforts to educate employees on the dangers of high-risk cloud services, and greater awareness among employees on the care required when dealing with corporate data. These findings are based on anonymized data collected from over 10.5 million enterprise employees across all major verticals - Education, Financial Services, Food & Beverage, Healthcare, High-Tech, Media, Oil & Gas, Manufacturing, Retail, and Utilities.

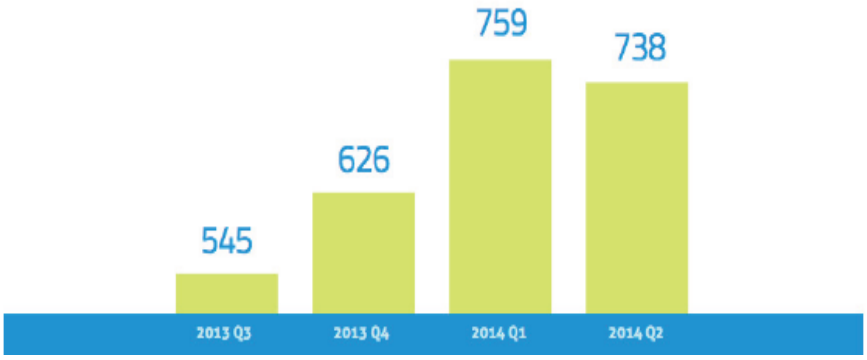


Figure 16: Average Number of Cloud Services in use By Company (Source: Skyhigh Networks)

Skyhigh Networks results also suggest that still firms are using cloud services that lack basic security features. For instance, only 11% encrypt data-at-rest, only 16% provide multi-factor authentication, and only 4% are ISO 27001 certified. In addition, based on their results, Skyhigh Networks claims that despite the buzz around data privacy and data residency, 72% of cloud services used in Europe store data in the U.S (Skyhigh Networks). In the report "The Snowden Effect: Data Location matters", by Carsten Casper from Gartner in 2014, one major assumption is that the physical location of data will become increasingly irrelevant and will be replaced by a combination of legal location, political location and logical location in 80% of all organizations by 2020.

Survey answers to the question, "After the PRISM revelations, how concerned are you about the privacy of your organization's data in the Cloud?", about 84% of respondents are somewhat or less concerned about it (Detail in Table 7).

	Total	Public	Private
Not at all concerned	12%	3%	14%
Marginally concerned	29%	24%	30%
Somewhat concerned	43%	62%	39%
Significantly concerned	11%	9%	11%
Extremely concerned	5%	3%	5%
Base	195	34	161

Table 7 How concerned are respondents after PRISM revelations? (Source: Cloud Industry Forum, 2014)

To the question, "Has the PRISM revelations and related concerns about the privacy of your organisation's data caused you to do any of the following things differently?", 56% of respondents have not done anything differently, and a minor portion (9%) have changed Cloud Service Providers.

	Total	Public	Private
Change the way I secure my information	32%	65%	25%
Change where I choose to put our organization's data	17%	21%	17%
Change my Cloud Service Provider	9%	12%	8%
It has not caused me to do anything differently	56%	26%	62%
Base	195	34	161

Table 8 What have respondents done differently after PRISM revelations? (Source: Cloud Industry Forum, 2014)

It can be concluded that private information leakage has had an effect on how European firms will ultimately decide on selecting certain Cloud Service Providers. As the majority of accepted and reputed providers are American-based (see Gartner's Magic Quadrant 2014), and the European region has one of the tightest data privacy regulations, clients are more likely to enforce Cloud Service Providers to comply with security standards. This might explain why after client firms announce a deep concern after the PRISM program revelations, still the US-based Cloud Service Providers remain as the leaders in the European region.

4.2.3.4 Security Standards Compliance

Third-party accredited institutions can certify that Cloud Service Providers comply with the standards given a specific Cloud Certification schemes. The following is the list of cloud relevant

security certification schemes published on ENISA's (European Union Agency for Network and Information Security) website.

Security	Security Rating Guide		EuroCloud Star Audit	AICPA SOC	Service Organization Control (SOC) 2
Certified Cloud Service TÜVRheinland CERTIFIED	Certified Cloud Service - TÜV Rheinland	OCF Open Certification Framework	Open Certification Framework - OCF	AICPA SOC	Service Organization Control (SOC) 3
		ISO 27001	ISO/IEC 27001 Certification		

Figure 17 Cloud Certification schemes (Source: European Union Agency for Network and Information Security)

Buyers of public cloud services require a standard scheme that can help ensure a provider's ability to maintain information confidentiality, integrity and reliability, and to restore data and service after a disaster. These formal cloud security standards are establishing the best practices for security and continuity.

In order to find a more conclusive evidence of the awareness of implementing secure cloud solutions as a demonstration of the trust paradigm shift, the ISO 27001 norm implementation evolution has been analyzed in a global context. The ISO 27001 is the security standard published by the International Organization for Standardization (ISO). This norm is a specification for an information security management system with the main goal to help organizations keep information assets secure. Some organizations choose to implement the standard in order to benefit from the best practice it contains while others decide they also want to get certified to reassure customers and clients that its recommendations have been followed.

Implementations show a sustained growth since 2006, with a special behavior for Asia and Europe as the regions with more implemented organizations. Interestingly, Europe is the region gaining a higher share in the last five years whereas the US barely has a few companies using the standard. Asian companies account for the largest share of implemented organizations, however, this proportion is consistently being eroded started to be shared with the Europe region[19] (See purple area in Figure 18).

[19] http://www.iso.org/iso/iso-survey

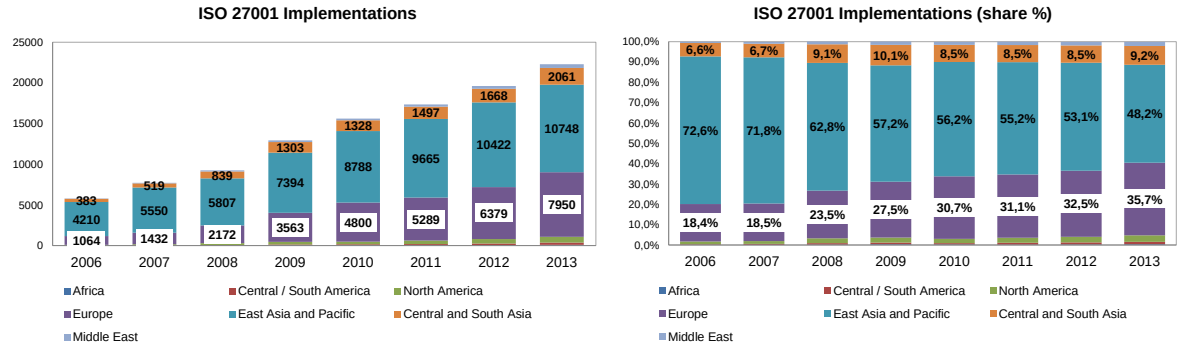


Figure 18 ISO 27001 implementation evolution per region. (Source: ISO Survey 2013)

A second standard that has become widely accepted to label secure cloud solutions is the Cloud Security Alliance, Security Trust & Assurance Registry (CSA-STAR). "Technology-related compliance and operating integrity audits are becoming increasingly important as the adoption of cloud-based services become the norm for businesses," said Jim Reavis, executive director of the CSA. The STAR serves as the standard for demonstrating transparent alignment with CSA security best practices. "The cloud can create great efficiencies for businesses, but it also introduces challenges and complexities for those businesses and their stakeholders who rely on the information's integrity, security and privacy," said Susan Coffey, CPA, CGMA, senior vice president for public practice and global alliances. To this day, 82 firms are certified with this standard and US and European-based count with the largest contribution[20] (See Figure 19).

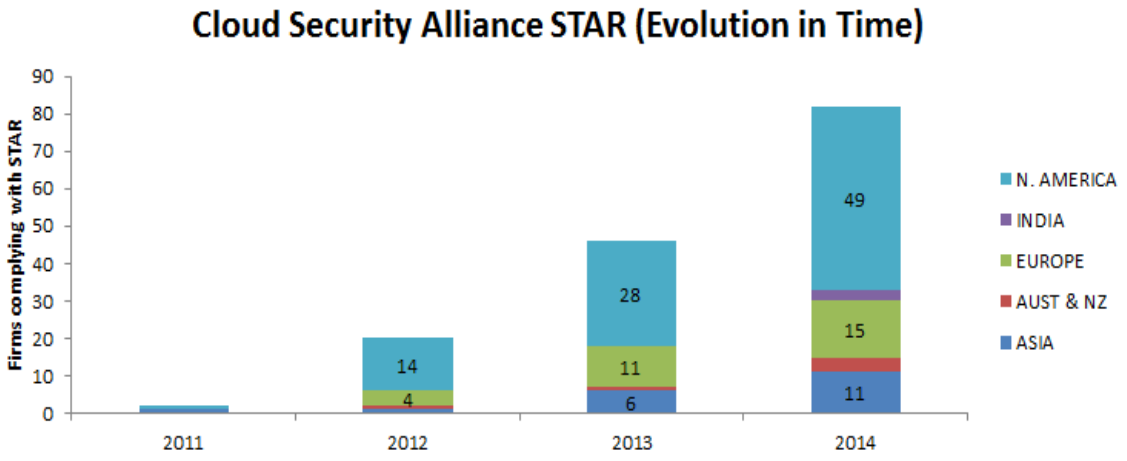


Figure 19: STAR certification evolution. (Source: Cloud Security Alliance website)

[20] https://cloudsecurityalliance.org/star/#_registry

Other standards like the SAS 70 (known today as SOC2 and SOC3) and the Service Organization Controls Reporting, by the AICPA, do not have public information available to check the adoption and implementation evolution, however, a survey from Ernst & Young in the EMEIA region (2013) reveals that organizations are attempting to differentiate themselves and increase their trust with clients by obtaining multiple assurance reports and/or certifications. Not surprisingly, firms declare that having this type of certifications will maintain the level of competitiveness, comply with regulatory obligations (in the European Region), and assure data integrity, availability and data privacy to their customers. In a survey study in the UK by the Cloud Industry Forum, it was found that 62% of organizations seeking to use Cloud Services would prefer to work with certified Cloud Service Providers. Last, Gartner research expects that certifications in 2015 will continue the uptake tendency[21].

It can be argued that this tendency constitutes a proof of the increasing awareness of both customers (demanding more secure cloud services) and cloud service providers (wanting to differentiate by offering more secure service proposals). This reduction on the "cloud complacency" can be taken as an evidence of the trust paradigm shift in Cloud Computing.

4.2.3.5 The European Cloud Computing Strategy: "Unleashing the potential of Cloud Computing in Europe"

The European Commission intends to gain new 2.5 million European jobs, and an annual boost of EUR 160 billion to the European Union GDP (around 1%), by 2020. The strategy is designed to speed up and increase the use of cloud computing across all economic sectors. This strategy is the result of an analysis of the overall policy, regulatory and technology landscapes and of a wide consultation with stakeholders, to identify ways to maximize the potential offered by the cloud. This strategy was adopted on September 2012 and aims to have publicly available cloud offerings ("public cloud") that meet European standards not only in regulatory terms but in terms of being competitive, open and secure[22].

4.2.3.6 Initiatives for a Secure Cloud in Europe

In the frame of the European Cloud Computing Strategy[23], one definite factor for cloud computing to attain its potential in Europe is to increase trust in the cloud. The European Cloud Partnership Steering Board recognizes that Europe is lagging behind other regions in the take-up of cloud computing. They identify events like the recent revelations about intelligence services surveillance of data that have the potential to harm trust in cloud-based solutions. The European Cloud Partnership Steering Board also identifies barriers for cloud adoption being Data protection and Information security concerns two of them. Among the different actions defined to establish a Trusted Cloud Europe, this section will remark two that are related to finding evidence of the trust paradigm shift.

[21] Service Organization Controls Reporting. Ernst & Young 2013
[22] http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy
[23] Document "Unleashing the Potential of Cloud Computing in Europe", Brussels, 27.09.2012

1. Through the definition of best practices and the facilitation of compliance assessments (against a recognized scheme as ISO 27001 or SOC2) are two key pillars of the Trusted Cloud Europe framework.
2. Make consultations and workshops targeting cloud users (citizens, SMEs and larger businesses) in order to educate and raise awareness so users can know where their data is hosted, how it is secured, what their rights are and how they can exercise them. The aim of this action is to increase understanding of the cloud computing paradigm.

The ultimate objective of the Trusted Cloud Europe initiative is to have a single digital market, free of needless barriers or restrictions in which all cloud users have access to high quality, secure and trustworthy cloud services[24].

Furthermore, different European research projects funded by the European Commission under the FP7 framework tackle the challenges of realizing trustworthy cloud services in Europe. Around six European projects explicitly undertake this effort and aim at increase the trust of users in the cloud services and thus increase their widespread adoption with consequent benefits for the digital users community and in general for digital economy. The budget destined to cloud security initiatives use 6% of the budget for ICT in security. This partially reflects the idea that both, cloud users and cloud service providers are reaching the state of awareness and therefore the trust paradigm shift becomes more evident.

4.2.3.7 Patenting activities related to Cloud Security and Trust

A patent landscape can also shed light in the evolution of the R&D efforts in the field of enhancing security in software applications as well as in hardware. In the following plot, it can be seen that filing patents in the field of security in cloud computing has gained momentum as of 2008. The interesting fact in this set of patent families is the low leadership of the European corporations. The US and Chinese corporations appear as the clear dominants when it comes to file patents related to privacy and security in the cloud, however, a larger tendency to file patents in the United States does not mean that the European region is not achieving the trust paradigm shift. The shown patent landscape is just an indication that top firms in the cloud security field are US-based, and therefore a more intense R&D effort is observed there (Figure 20).

[24] Establishing a Trusted Cloud Europe. A policy vision document by the Steering Board of the European Cloud Partnership: final report

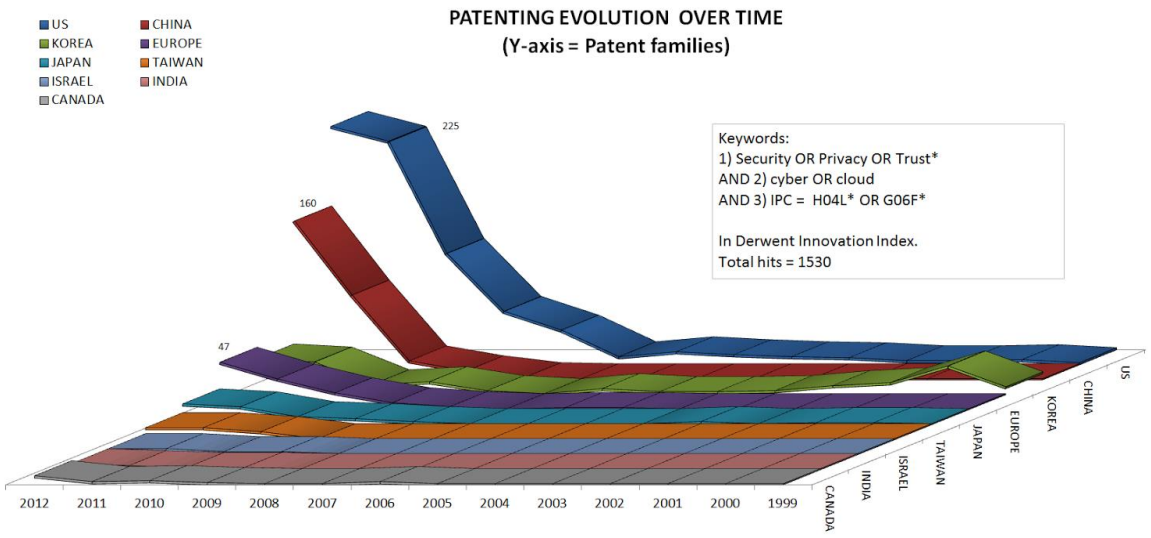


Figure 20 Cloud security and privacy patent filing (Source: Derwent Innovation Index)

4.2.3.8 European Cloud Security Market

Gartner forecasted in mid-2014 that growth in cloud-based security will remain strong, at about 20% through 2017, which means that the cloud security market is a “viable market that offers providers many opportunities for expansion”. Gartner also noted that cloud security providers would be best served from this market growth by focusing their marketing on small and medium-sized businesses. In addition, a specific delivery model of cloud computing -Application Security as a Service-, has been ranked by Gartner as a service with a high benefit impact with a potential of market penetration of 20% to 50% of the target audience.

4.2.3.9 Cloud Trends

In order to check a search pattern and trends in the online google search engine, four terms have been analyzed, namely “Cloud Security”, “ISO 27001”, “SAS 70” and "SOC 2". The scope of the search is worldwide, from 2004 until present. A general uptake in the cloud security topic is present since its inception. This indicates a rising interest in the topic. A more timid interest is observed in the topic ISO 27001, and the tendency indicates a constant interest which is rising in the last months of 2014. The SAS 70 standard, which traditionally has been used to assess security compliance, is now replaced by the Services Organization Control Reports, the SAS 70 interest is in decrease and the SOC 2 is now in the uptake. This indicates that firms alternate their interest in a security standard, and a rising interest (still timid) in the compliance of the SOC 2 standard is linked to the interest to provide more secure offers when it comes to cloud services.

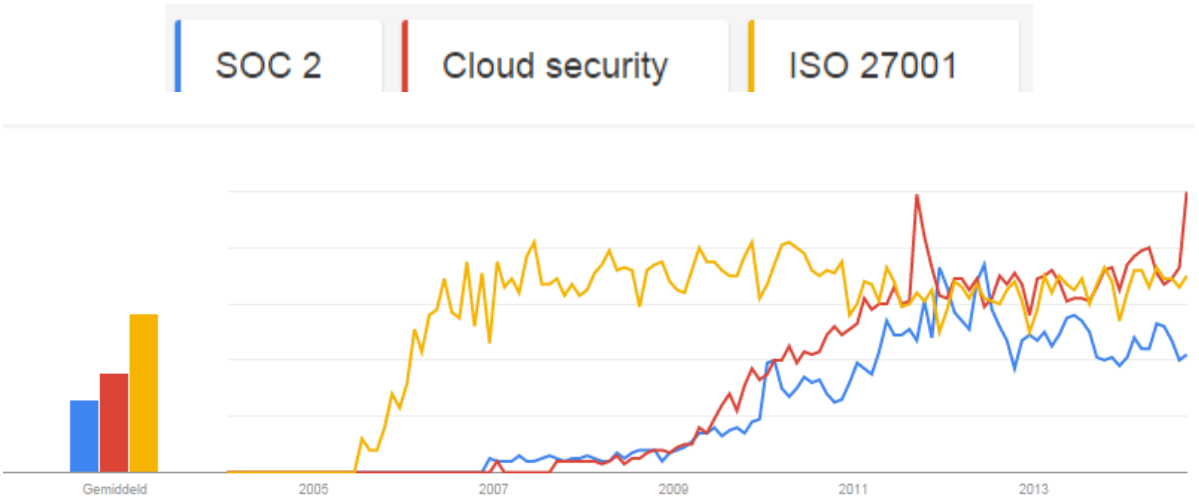


Figure 21 Google trends (Cloud security, ISO 27001, SOC 2)

4.2.4 Conclusions

To summarize, cloud computing has been observed as a potential technology that no longer is considered an emerging technology but rather it is seen now as a mainstream service. The European Commission has high expectations from cloud computing. They intend to gain 2.5 million new European jobs, and an annual boost of EUR 160 billion to the European Union GDP (around 1%), by 2020. The strategy is designed to speed up and increase the use of cloud computing across all economic sectors.

Cloud computing will continue with its sustained positive adoption rate, but still managers see cloud security along with its related privacy implications as a major concern in the decision to adopt. Some recent events regarding espionage and privacy incidents suggest that users' sensitivity towards cloud security concerns is increased. Public opinion (among managers) suggests that security is a top barrier for adoption, yet some evidence[25] suggest that this is a matter of managing perceptions rather than an evidenced risk.

It can be concluded that private information leakage has had an effect on how European firms will ultimately decide on selecting certain Cloud Service Providers. As the majority of accepted and reputed providers are American-based (see Gartner's Magic Quadrant 2014), and the European region has one of the tightest data privacy regulations, clients are more likely to enforce Cloud Service Providers that comply with security standards. This might explain why after client firms announce a deep concern after the PRISM program revelations, still the US-based Cloud Service Providers remain as the leaders in the European region.

Cloud certification implementations, e.g. ISO 27001, show a sustained growth since 2006 and Gartner research expects that certifications in 2015 will continue the uptake tendency. It can be argued that this tendency constitutes a proof of the increasing awareness of both customers

[25] Source: Paper 14: The Normalization of Cloud in a Hybrid IT Market (Cloud Industry Forum, 2014)

(demanding more secure cloud services) and cloud service providers (wanting to differentiate by offering more secure service proposals). This reduction on the "cloud complacency" can be taken as an evidence of the trust paradigm shift in Cloud Computing.

A patent landscape also shed light in the evolution of the R&D efforts in the field of enhancing security in software applications as well as in hardware. Patent filing activities related to security and privacy in the cloud does not show a conclusive evidence of the paradigm shift, at least when a comparison is made across regions (e.g. Europe, vs, Asia). It does show however that this sector (security in the cloud) is rising with a lot of traction especially as of 2009, with an increasing R&D intensity and that it will continue with such pattern in the coming years, which is in line with Gartner's predictions.

4.3 Pillar II: Personal Data Management

4.3.1 Introduction

Personal data can be understood as the digital data created by and about people. After all, personal data is the digital record of "everything a person makes and does online and in the world." The huge amount of personal data that is becoming available these days in the digital world has converted personal data in such a valuable asset. For Meglena Kuneva, European Consumer Commissioner, personal data is the new oil of the internet and the new currency of the digital world. This has opened a wide opportunity for new data-driven services and applications in the public and private sector. Still, 78% of consumers think it is hard to trust companies when it comes to use of their personal data (Orange, The Future of Digital Trust, 2014). Because of these concerns, several initiatives now offer user a full spectrum of services regarding the protection of this valuable asset and the exploitation of its value. For instance, many offers provide the user with a functionality to surf the net without being tracked. Other offers provide the user with the power to monetize all the traces of information that are produced when transactions are made. So, a new market is enabled to tackle the security concerns, but the question remains: do these new initiatives entail a powerful evidence of the achievement of the trust paradigm shift? The signals given by the market are not entirely clear. First, we hear about the merge of Whatsapp being bought by Facebook and all the media coverage about the risks involving Facebook selling information from Whatsapp chatters. Some could have predicted a dis-acceleration of active users of Whatsapp moving towards more secure chat services. By the end of August 2014 we learn about the 600 million users in Whatsapp, which is a undeniable sign of good traction in this service's adoption. In order to form a solid body of evidence of the trust paradigm shift, different angles of the market should be analyzed.

In the rest of this subsection, sources like surveys from public opinion, experts' analysis and website traffic metrics will be observed with the main purpose to build evidence in favor or disfavor of the trust paradigm shift. Therefore, we state the research question as follows:

Can we find early indicators of shifting adoption towards applications focused on privacy and security in the B2C domain?

In order to tackle this question, we will aim at answering the following sub questions:

1. Is there a shift to trustworthy versions of same sort of application in the B2C domain (Messaging, Storage, Social media)?
2. Are there indicators of new business models, new organizations, or new solutions that try to catch the new wave of trustworthy applications in the B2C domain?

The last section of the personal data management to introduce the new business model of monetization of personal data.

4.3.2 Theoretical Background

According to the Gartner Hype Cycle for privacy report on 2014, the privacy discussion has seen a boost over the past 12 months. When compared to the same report from 2013, organizations worldwide are now rethinking their privacy investment priorities, now putting a higher priority. In

their privacy survey 2014 (not published yet), Gartner found that in 31% of organizations privacy receives the attention of top-level management. They also recognize that attention to privacy goes in waves: "*Massive privacy intrusions or data losses result in public outrage, which is followed by legislative or regulatory activity. However, this response may take months or even years. The market for privacy-related technologies also typically has a delayed reaction, offering tools that prevent intrusions or personal data leakages months or years after the first events occurred*" (Gartner Hype Cycle for Privacy, 2014). Regardless of the impact that media coverage has on public attention when it comes to privacy and security online, the B2B sector is highly aware of the risk implications. The same cannot be told for the B2C sector: people are somehow aware of the privacy risks, but different to organizations, people are more passive and don't react in the same way. Especially in Europe, Gartner report states the following: "*High privacy awareness in Europe coincides with the final phase of the legislative process for this European regulation, creating high expectations — and concerns — among citizens, enterprises and policymakers. Public attention will increase once more when the proposal becomes law, which is expected at the end of 2014 (after the EU parliament voted for the proposal in March 2014, it's now in the hands of the EU Council of Ministers).*"

In addition, Gartner categorizes many of the privacy enhancement initiatives (technologies and legislations) in the Peak of Inflated Expectations reaching productivity in no less than 2-5 years. This means that online privacy is still an emergent discipline. In addition, some technologies and legislations provide more benefits than the others. For instance, by displaying this in a Priority Matrix, new technologies are classified in a scale of low-moderate-high-transformational in terms of delivered or potential benefits (see y-axis in Figure 22). In the same tool, the x-axis displays the years to mainstream adoption of the new technologies. As can be seen in the Priority Matrix for Privacy, the high benefit to be obtained from the U.S. and EU privacy regulations contrast to the benefits to be obtained from initiatives like Privacy-controlled social networks (See Figure 22).

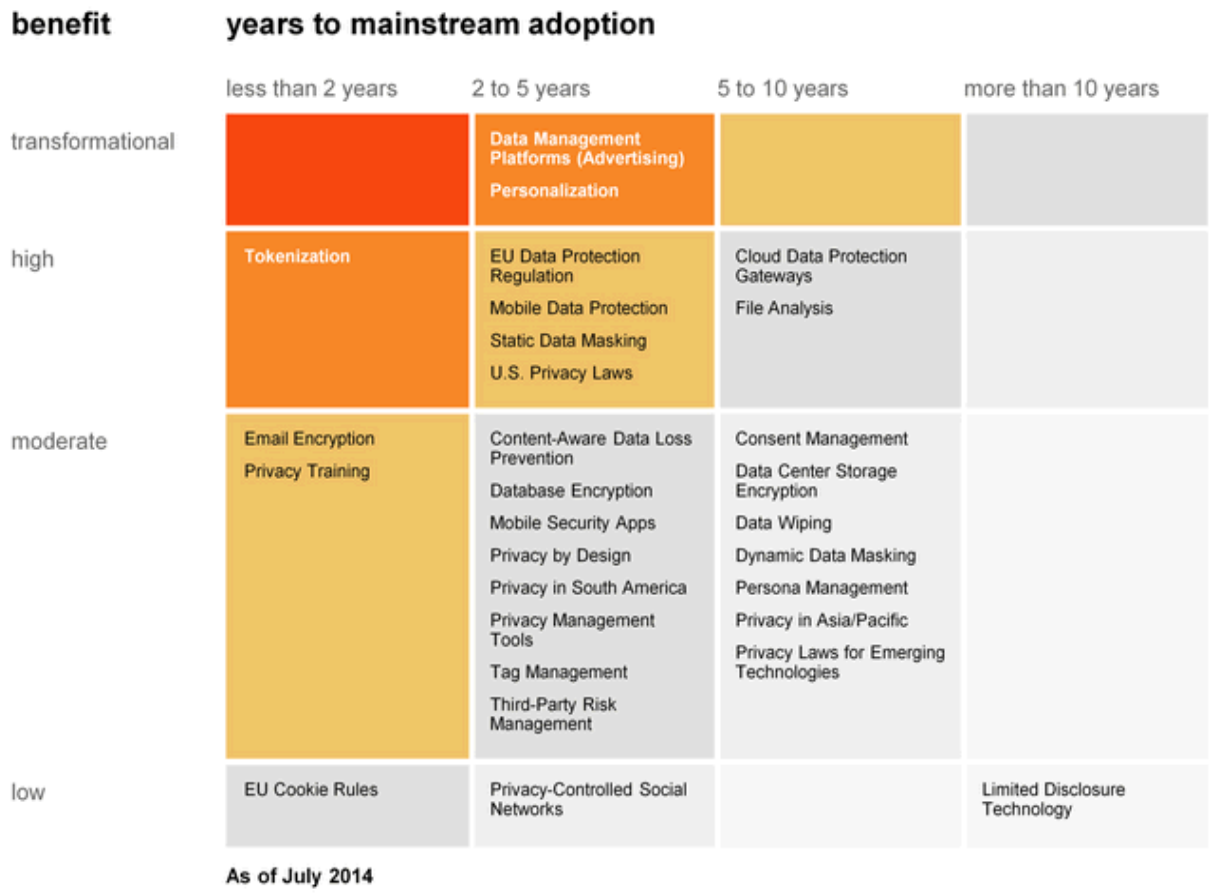


Figure 22 Priority matrix for Privacy (Source: Gartner July 2014)

4.3.3 Analysis

4.3.3.1 What Web Traffic Metrics Reveal

A whole set of new applications that have the purpose to enhance security and privacy for businesses and particulars have emerged in the last years. Due to the recent events of data leakages and espionage programs, some of these tools have got some relevant attention, which implies that their acceptance and adoptions might see benefits in these days. In order to understand how the adoption patterns of such solutions can constitute an evidence of the trust paradigm shift, the web traffic of these services is analysed. Even though we don't have the metrics of active users of these services in smartphones, website traffic metrics shed some light about the perceptions and trends in public usage of such services.

The case of secure chat services: after it was revealed that the popular Whatsapp chat service was going to be acquired by Facebook, some users saw this event as a threat for their intimacy, as Facebook is recognized for having a posterior use of the personal information of users. Some secure services sought some acceptance. Threema, based on Switzerland, uses end-to-end encryption. It saw huge acceptance during the days when the Whatsapp acquisition came on public. Web traffic metrics imply that the buzz lost its power some months later. It is possible that Threema adoption

figures show an increase due to the positive tendency of Europeans becoming aware of the privacy threats, but it can be said that it remains as a niche service. A similar story can be told about Telegram. Telegram is the Russian counterpart of a secure and free messaging service. It also got much of the attention during the first quarter of 2014. It has gained rapid popularity. It saw 8M downloads after Whatsapp was acquired[26] and it reached 35 million users by March 2014. The web traffic plot lets us assume that the steep growth (1M downloads per day after Whatsapp acquisition) is due to a human reaction to the privacy threats. How this will sustain over the time and how this will entail a threat to Whatsapp as a solution, it is there yet to be seen. What the metrics can show is a more sustained measure of traffic for Whatsapp, who by the end of August 2014 announced the record of 600 Million active users.

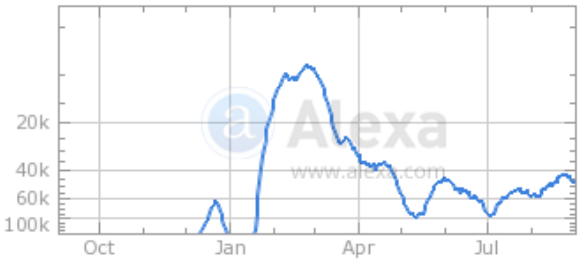
www.threema.ch "Seriously secure mobile messaging"	www.telegram.org "Taking back our right to privacy"
	
www.wickr.com "Top secret messenger"	www.whatsapp.com "Simple, personal, real-time messaging"
	

Table 9 Chat services web traffic comparison (as of Oct 2013 – Today. Source: Alexa.com)

The case of security and privacy enhancement tools show an interesting pattern: Online tools like Disconnect.me that aims to reduce people's exposure to many threats, including malware, identity

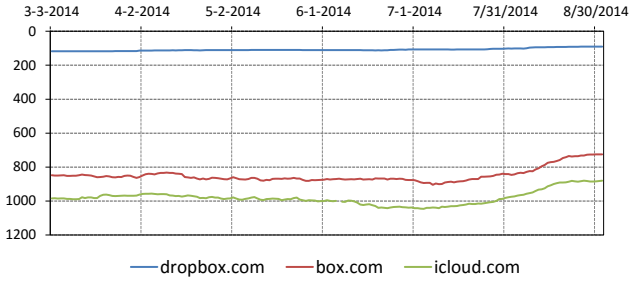
[26] http://techcrunch.com/2014/02/24/telegram-saw-8m-downloads-after-whatsapp-got-acquired/

theft, and tracking of search and browsing history. The web traffic pattern exhibit a more sustained evolution over the time, and has today 2 million users per week[27] (see Table 10).

www.disconnect.me "The Internet on your terms: Fast, Private, Secure"	www.abine.com "Protect your privacy. Stop companies from tracking you"
	

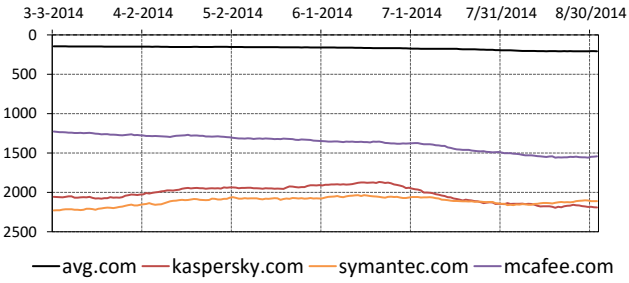
Table 10 Privacy and security online services web traffic comparison (Source: Alexa.com)

But private and trustworthy applications are not yet in the mainstream. This type of application resembles a niche market of customers who are aware of the privacy concerns and really want to utilize trustworthy applications. In some cases, some services tend to look like hypes or buzz words that are influenced by the media coverage, but it is clear from the information shown that a set of users are willing to be more proactive against privacy threats. Table 11 explains per type of service the web traffic comparison and some observations.

Type of Service / Remarks	Historical Traffic trends
Data Storage services Along with the addition of security features, services like Box and ICloud have increased the web traffic, which directly means that they are broadening their customer base. Leader services like Dropbox, which lead on the B2C segment, are now tackling the challenges to satisfy the B2B segment.	

[27] https://disconnect.me/

Antivirus
Surprisingly, website visits to the most well-known antivirus packages are in a slight decline. Conclusions should not be drawn from this fact, but it is still a clear signal that customers are looking for more integral solutions.



Different privacy tools
Tools that seek to enhance online privacy and security are not part of the mainstream applications and remain in the lower levels of popularity.

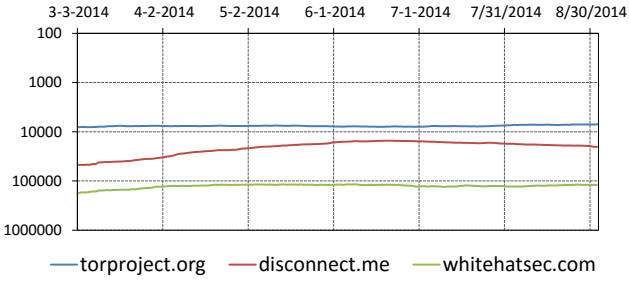


Table 11 Historical traffic trends for different privacy and security tools.

Source: Alexa.com accessed on 29th September 2014

4.3.3.2 Surveys gauging the public opinion

Plenty of studies using public surveys are found available. For the purpose of this document, only studies that are published not before than 2013 are taken into account. This stream of evidence is important as it explicitly demands people a reaction about the topic of privacy and security in online and cloud services. we still have to note that this type of study might be problematic as public opinions is normally influenced by the media coverage to a certain topics like data leakages and cyber-crime, which has been in the spotlight for the last 18 months. Still, it is considered valuable that this stream of research makes part of the body of evidence that is being used to observe the trust paradigm shift.

According to a survey held in late 2013 by Edelman Berland and Microsoft 39% of Americans have changed their browser settings to request that websites do not track them, while this statictic shows a considerable amount of privacy concerned users, but the majority of users have yet to reflect similar privacy concerns . Such fact must be interpreted with caution, as it refers to the American public, which is already known to differentiate with the Europeans regarding awareness of privacy issues. Yet, that study reveals the following:

- Tech elites want technology companies to deliver innovations that automatically protect individuals' privacy.
- Europeans expect a more pervasive role from governments that establish privacy protection policies, than Americans.
- Americans are more willing to make privacy trade-offs for routine online activities, e.g. shopping and banking, while Europeans place lower value on ease-of-use.

A second survey study, called Perceptions of Data Privacy and published by Ipsos MORI (July 2014) presents the following findings:

- Consumers consider that data loss is one of the worst things a company can do, and selling anonymous data is not far behind – but people only think of it if prompted.
- There is a sense that data sharing is inevitable.
- The public shows high support for transparency, as most agreed that they "would really like to know what information government knows about me" (only 5% disagreed). However, the public is unlikely to drive action on transparency by themselves. Only about one in 20 people (5%) said that they have asked a government department, public service or private company what information they hold about them.
- On balance, the research suggests there is more support for the government preventing misuse of personal data than there is an appetite to have personal control over this.
- People don't like sharing personal information, but under a safeguard policy, their attitude changes (see Figure 23) and turns more positive towards data sharing.

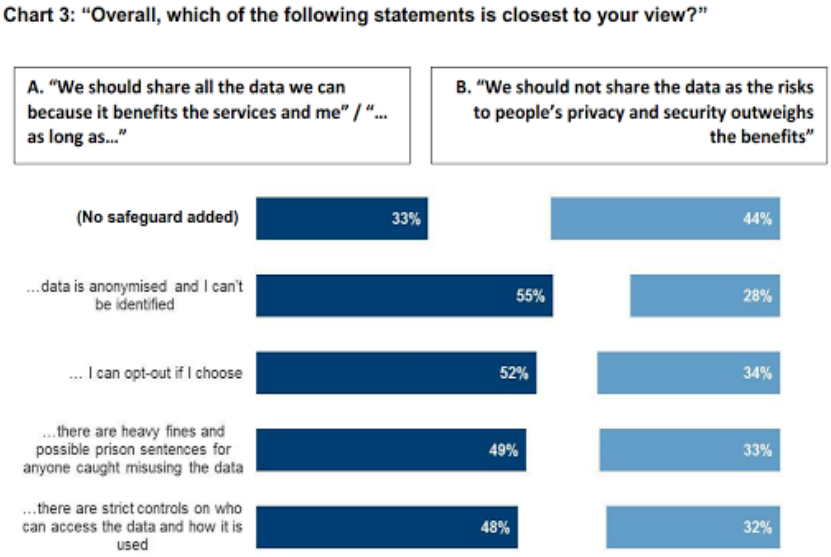


Figure 23 Safeguards impact on willingness to share data (Source: Ipsos MORI July 2014)

- Regarding this last point, Eric Bloom from Abine brings up a study from Forrester in which is evident the tension between the concern over being tracked and the desired of being tracked to obtain a reward[28]. Again, users don't like being tracked but are willing to accept it for some reward.

An additional relevant study is the Special Eurobarometer 404 Cyber Security survey, which is endorsed by the European Commission. Its fieldwork is from May-June 2013 and it was published in November 2013. The main remarks regarding our topic are:

[28] http://www.abine.com/blog/2014/forrester-privacy-study/

- EU citizens express they are slightly less likely to have concerns (regarding privacy and security) than in 2012. Specifically, smaller proportions are concerned about someone taking or misusing personal data (down from 40% to 37%), security of online payments (from 38% to 35%), and not receiving goods or services that they buy online (from 19% to 15%). Correspondingly, the proportion that has no concerns has increased (from 21% to 23%).

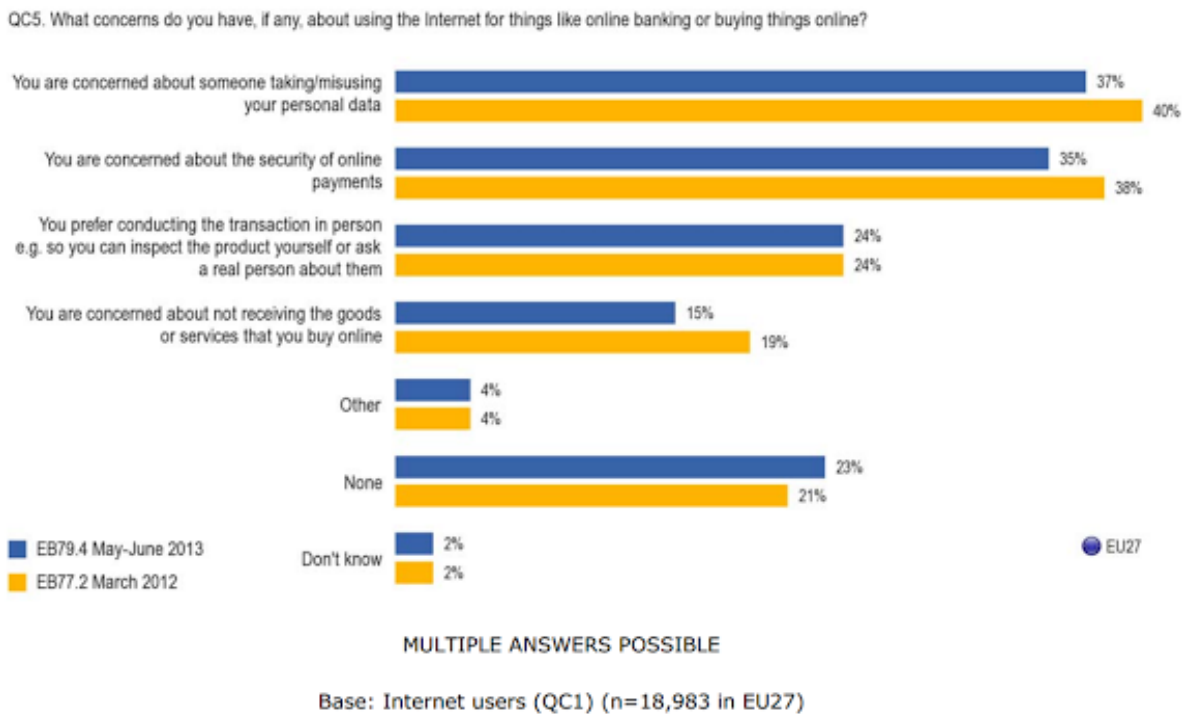


Figure 24 What concerns people about using the internet?

- A clear majority also agree that they are concerned that their online personal information is not kept secure by websites (70%), while 27% disagree. Most respondents are also concerned that this information is not kept secure by public authorities (64%). When compared to data from 2012, respondents state they are slightly less concerned, but at the same time they acknowledge that the risk of becoming victim of cybercrime is increasing.

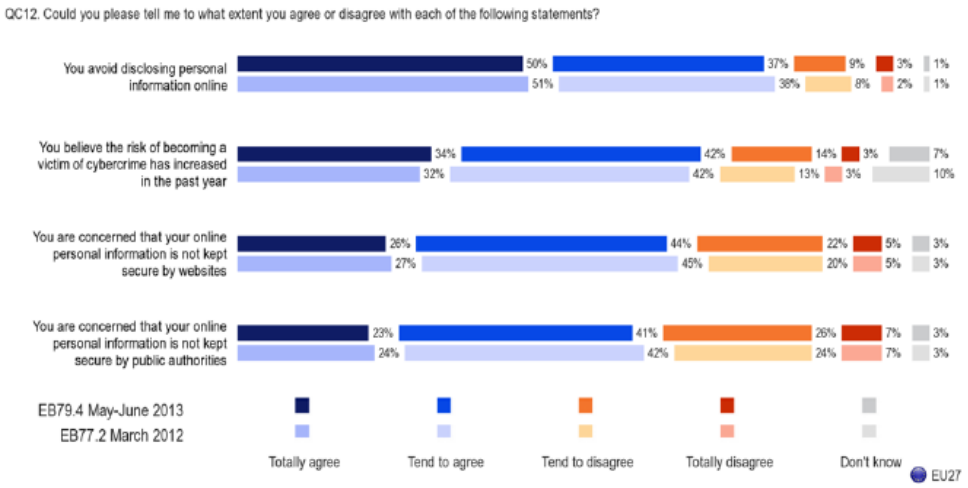


Figure 25 Are Europeans concerned about privacy and security online?

- Respondents mitigate their concerns by using different alternatives. The most used one is the installation of anti-virus software (46%) and 16% change the security settings in the browser, online social media, search engine, etc. The rest of actions reflect the avoidance to use not trusted online services instead of using more powerful tools. Only 1% of respondents use other methods.

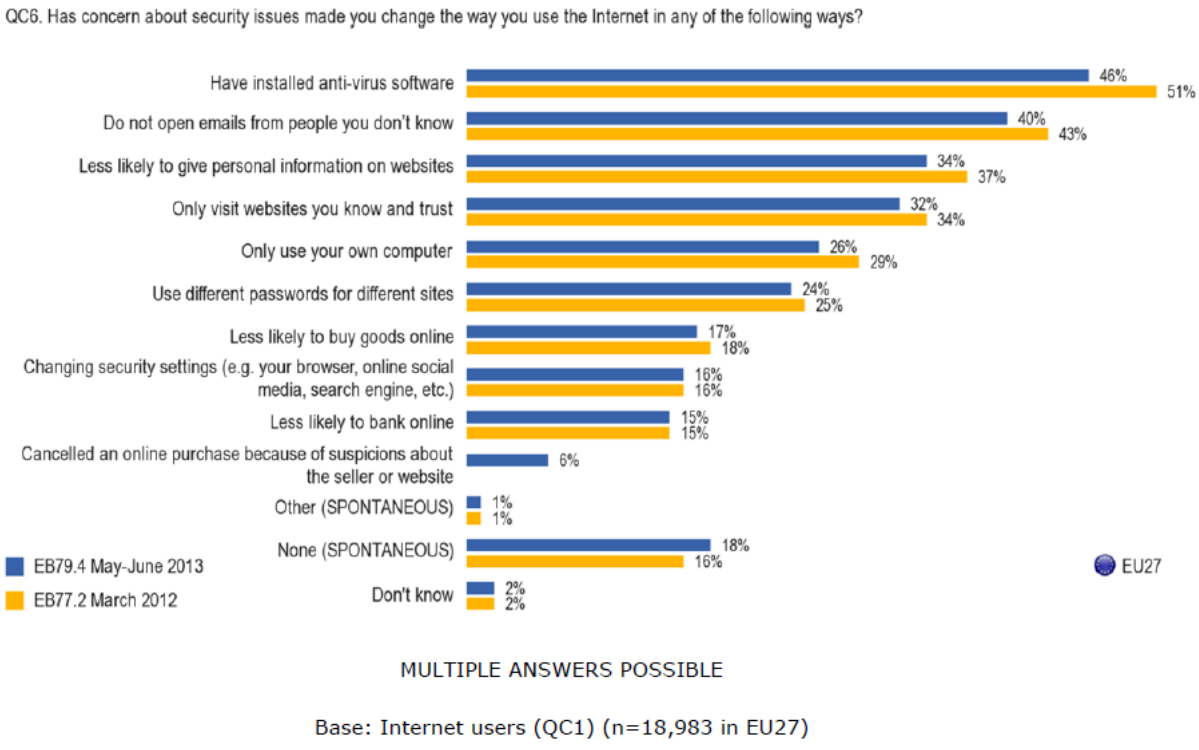


Figure 26 How Europeans react to privacy issues on Internet?

A fourth study, which uses the findings as well from large scale surveys, is also considered for the present document. The study, published in April 2014, is endorsed by Sciecewise, a British programme to improve Government policy making involving science and technology. The main findings regarding our topic can be summarized as follows:

- Awareness of data collection and use by government and companies is quite high, but the level of understanding of what this means in practice is much lower.
- When asked, the public are ostensibly opposed to any form of data use and collection by government and companies, but in practice the public consider there to be no alternative to sharing personal information with government and companies in the modern world and expect it to increase in future.
- Offering a specific personal or public benefit can significantly increase the general public's acceptance of the collection, sharing and use of their data by government and companies, but even when a specific benefit is offered, the public remain concerned about the collection, sharing and use of particular types of personal data (e.g. bank account, savings and pension details).
- People are keen to have more control over the use of their personal data and want stronger safeguards towards its use, and there is strong support from the public for more information on how government and companies collect, share and use data.
- Despite the media attention in the past couple of years it appears that public awareness of personal data collection and use is not necessarily increasing. In fact, Deloitte (2013) found that the percentage of people who say they are "fully aware" that organizations collect data about them and their activities fell by 10 per cent (from 45% to 35%) between 2012 and 2013.
- There is a significant discrepancy between the public's stated preferences and their actual behaviour. The discrepancy in views and actions is in part due to not having the information required to rationally make the necessary trade-offs on a day-to-day basis.
- The general public's real world approach to sharing their personal data with government and companies suggests that they are much less concerned about the risks and much more sold on the benefits than they make out.

4.3.3.3 Monetization of Personal Data

Personal data is considered nowadays as a valuable asset. Yet, the question of "who has access to what data?" remains a nearly impossible question to answer. During the conversations in Davos about this topic, three main challenges are stated to strengthen trust in the personal data industry: obtain meaningful transparency, strengthening accountability and empower individuals (See Figure 27). Related to this last point, i.e. empowerment, experts acknowledge the current system reflects an asymmetry in power that broadly favors institutions (both public and private) over individuals and large institutions have greater resources to orient notice and consent agreements to advance their interests.

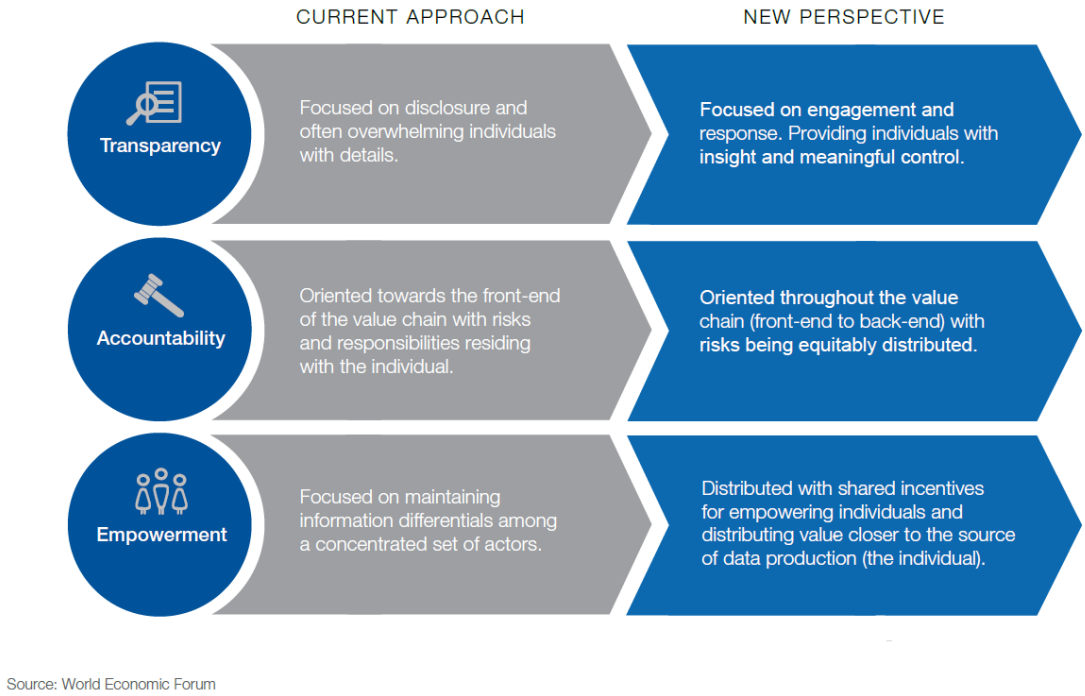


Figure 27: Strengthening trust in Personal Data Management. World Economic Forum, 2014

From a business innovation angle, a new set of applications are becoming available which can help individuals assert more control over how personal data is leveraged and value distributed. One attitude that users might take against such asymmetry is the use of protection tools (several of them explained above) to prevent a third-party to access personal data. A second attitude might be the consented sharing of personal data in exchange of some reward. One example of such services is what is known as monetization of personal data.

According to a survey, value exchange for data is regarded positively by the community29, and new initiatives as monetization of personal data make sense to some users in the community. Users are becoming aware of the existence of data brokers like Axciom, Epsilon and Experian who play as leaders in the multimillion dollar industry of collecting, analysing and selling individuals' information. This shift of awareness might incentivize the monetization of personal data by individuals. One example is Google's Screenwise Trends panel, which gives a cash voucher to anyone willing to simply share their Internet browsing behaviour with Google and its partners, with a further continuous voucher every week thereafter. Another example is Raptr, an app that tracks users' video gaming habits in exchange for regular rewards, such as in-game content or free games. The UK- based Handshake believes that if someone is making money of personal data, the individual should be the first one in the line of profit. Other new firms under the same logic are Ctrlio and Datacoup. So, it's clear that these initiatives constitute an effort to empower the user over their data, and despite the good intentions, these initiatives have to overcome one big barrier: users' apathy to take control

[29] Rethinking Personal Data: A New Lens for Strengthening Trust

over their data transactions. Because they are new, good metrics of popularity should not be expected, however the table below[30] displays how far they are from becoming a mainstream service (Table 12).

Web traffic metric	Handshake	Datacoup	Screenwisetrends	Meeco
Alexa Ranking[31]	1.5 Million	368 thousand	318 thousand	970 thousand
Bounce rate[32]	38.5%	36.1%	15%	34.6%

Table 12 Web Metrics for Monetization of Personal Data Services (Source: Alexa.com)

Regardless the long road still ahead to become top popular, these disruptive ways of monetizing personal data establish a new model of enabling individual empowerment over this valuable asset and tackles one of the three challenges unveiled in the World Economic Forum global dialogue about achieving trust. This nascent business models should be closely observed as an early indicator of the trust paradigm shift.

4.3.4 Conclusions

From the presented evidence, it looks like the people acknowledge the problem but don't do much to take a proactive attitude, or they do something when there is a moment of panic (e.g. NSA espionage program becoming public, or Whatsapp being acquired by Facebook), but people who consistently adopt and use trustworthy applications remain as a minority. Powerful and secure services like Threema or Telegram manage to build a solid customer base, but when compared to the mainstream services, the accepted and "not-the-safest" services take the lead. In the B2B segment, things turn different: service providers know that they must offer secure and trustworthy services, otherwise organizations will not use them, as organizations take privacy seriously. The evidence also suggests that people acknowledge the fact that personal data is valuable and settle to share it, at least a vast majority, and it remains as minority those who block or take the effort to charge for their own information. People's opinion regarding sharing information turns more positive when safeguards and benefits make part of the deal.

People's opinions and conclusions drawn from survey studies must be taken very carefully as media coverage of personal data breaches and government espionage programs largely affects people's attitudes towards this topic.

New forms of individual empowerment are emerging in the personal data management arena. The monetization of personal data comes as an alternative for individuals to take control over their data and start realizing its value. Though nascent, this disruptive business sheds light on the change of

[30] Taken from Alexa.com on 29th September 2014

[31] Ranking system set by alexa.com that audits and makes public the frequency of visits on Web sites. It is based on the amount of traffic recorded from users that have the Alexa toolbar installed over a period of three months and takes information from parameters such as reach and page views.

[32] Engagement metric that measures the percentage of visitors to a particular website who navigate away from the site after viewing only one page.

perception about the data management and all the controversial around its privacy, security and potential value and how a minority is aware of the circumstances.

4.4 Pillar III: Digital Identity Management

4.4.1 Introduction

Identity is the fact of being who a person is, or what a thing is. Identity management is a security discipline that enables the right entities to access the right resources at the right times for the right reasons. Effective identity management entails organizing and controlling authentication, authorization, and privileges of individuals and things. Identity management is implemented within a system (e.g. country, enterprise, online service) and relies on associating user rights and restrictions with the established identity.

Identity management is a *gatekeeper mechanism* that guards access to services, systems, applications, and information. It represents the first line of defence protecting the confidentiality, integrity, and availability of services, systems, applications, and information. In the digital space, identity is represented in the data that uniquely describes an entity. Identities correspond to entities, and identities consist of attributes or identifiers (Figure **28**).

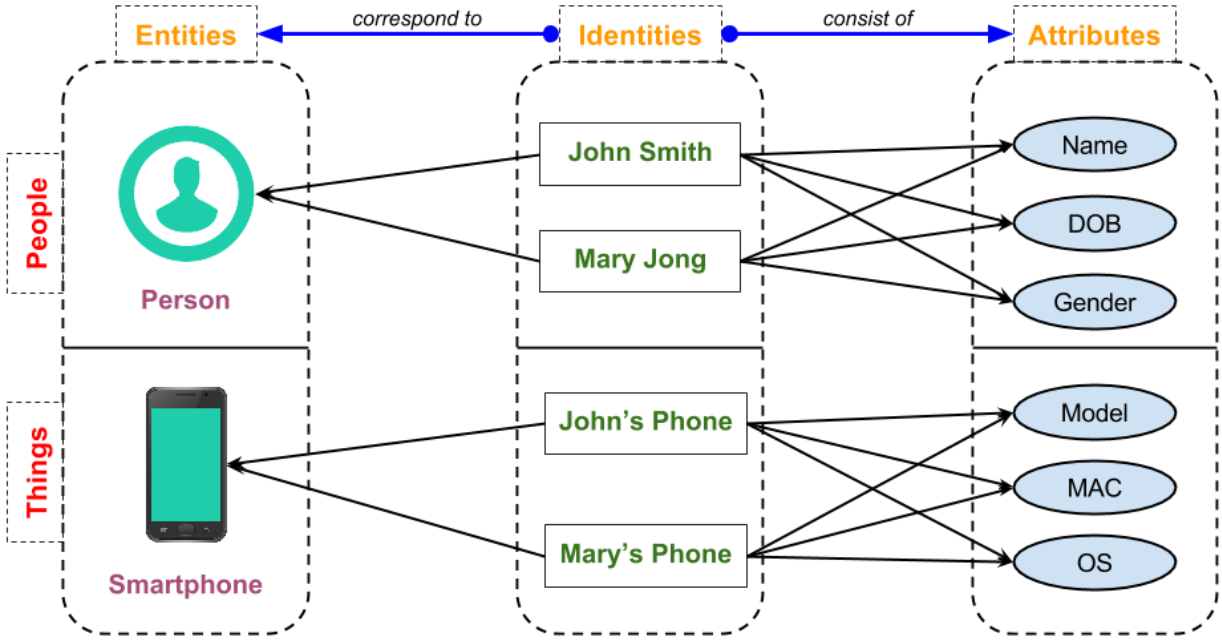


Figure 28: Digital Identities: entities and attributes.

Heterogeneous technology environments (e.g. loosely coupled applications) are becoming more able to work together through interoperability, integration, and standardization. Yet identity management systems emerge in an environment where much less efforts have been put to achieve similar goals on a large scale.

Authentication is the first step in establishing an identity; it is the act of confirming the truthfulness of the presented attributes. Authentic attributes associated with a valid entity lead to identification: attesting to the claims of an entity of being who or what it really is. Authorization is the following

step, which specifies the access rights of an identified entity. Different identities within a system have different access rights; this usually entails associating roles with privileges.

Increase in the complexity of designing and implementing useful eID systems is synonymous to the recent increase in complexity for other technologies. The continuous transformation of the internet introduces new challenges to many related technologies and eID is no exception. During the first internet era, pioneers had more trust in online identities. That trust was sufficient at the time due to the low risk associated with benefiting from the internet. Since then, tremendous changes happened and in 2015 as we are witnessing the emergence of the internet of things, the number of connected users and devices multiplied. Table **13**: Increase in internet users, connected devices, and apps. reflects on these increases.

Table 13: Increase in internet users, connected devices, and apps.

Era	Platform	Users	Devices	Apps
Web 1.0	**First** Mainframe, minicomputer, terminal.	Millions	Thousands	Thousands
Web 2.0	**Second** LAN/Internet, Client/Server.	Hundreds of millions	Millions	Tens of thousands
Web 3.0	**Third** Mobile, cloud, big data, social, things.	Billions	Trillions	Millions

Following this introduction, the following section analyses the case for eID from a European perspective, taking into consideration legal and regulatory aspects, as well as technical and implementation considerations. The same section also investigates eID related initiatives at the European level as well as the national (member state) level.

4.4.2 European Identity Management Perspectives

Warnings that European eID initiatives might not succeed due to major obstacles were raised in a paper published by the European Network and Information Security Agency (ENISA[33]) in 2009. The findings resulting from an analysis of 10 eID systems already in use within EU member states, and 13 that were under development showed a "*lack of coordination in European eID privacy features*"[34] and a "*need for a European eID strategy*"[35]. The study showed that Europe had no coordinated strategy to protect user data, leading to a lack of cross-border interoperability between the different eID systems, and to reluctance in accepting them by potential users.

Things changed since 2009. European digital strategy evolved and addressed eID strategy requirements, legislations and regulations (e.g. eIDAS) were introduced, and these specifically tackle the warnings raised by ENISA. On the practical side, European projects were funded and kicked-off to make things happen (STORK 1.0, STORK 2.0, e-SENS). Figure **29** illustrates the timelines of these initiatives, and highlights the milestones of the eIDAS regulation.

[33] https://www.enisa.europa.eu/
[34] http://www.unwatched.org/node/1287
[35] http://www.out-law.com/page-9771

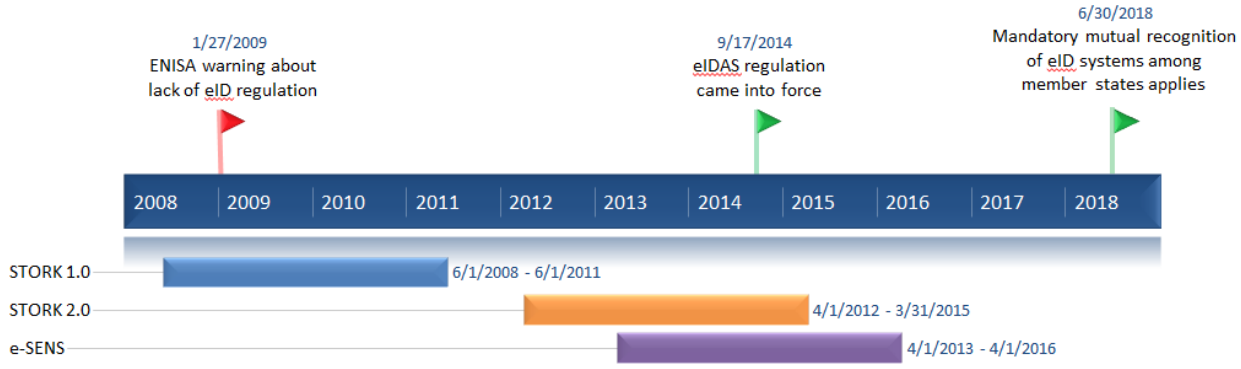


Figure 29: Timeline for eIDAS regulation and European Level eID initiatives.

The following section (1.1.2.1) addresses European eID strategy and regulations, their objectives and how they evolved. Sections (1.1.2.2 and 1.1.2.3) address practical eID initiatives at the European and national levels respectively. Section (1.1.2.3) also presents the Estonian eID experience as a leading European case study, and summarizes eID experiences from five other European countries.

4.4.2.1 European e-ID Strategy and Regulations

The Digital Agenda for Europe[36] is the European Union's IT strategy until the year 2020. It aims to reboot Europe's digital economy and help citizens and business get the most out of digital technologies. It is the first of seven flagship initiatives set up within the EU's overall growth strategy Europe 2020[37]. Under the first 2 pillars of the Digital Agenda (i.e. Digital Single Market, and Interoperability & Standards) are actions to push forward the harmonization, implementation and adoption of EU wide eID.

Europe recognizes that an electronic identification (eID) and electronic trust services (eTS) framework that works across the EU countries is vital for safe electronic commerce and for the efficient delivery of public services. Europe also recognizes that electronic identification is a key enabler for secure cross-border electronic transactions and central building blocks of the Digital Single Market.[38]

This recognition materialized in the European Union regulation N°910/2014[39] on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). This regulation was adopted by European level legislators on 23 July 2014 to provide a predictable regulatory environment which enables secure and seamless electronic interactions between businesses, citizens and public authorities. It is expected that this regulation will increase the effectiveness of public and private online services, eBusiness and electronic commerce in the EU.

In practice, the eIDAS regulation enables the use of eID and eTS technologies (i.e. electronic signatures, electronic seals, time stamping, registered electronic delivery, and website/service

[36] http://ec.europa.eu/digital-agenda/
[37] http://ec.europa.eu/europe2020/index_en.htm
[38] https://ec.europa.eu/digital-agenda/node/50813
[39] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

authentication). It enables the use of these technologies by citizens, businesses and public authorities as their digital way of interaction, in a similar fashion to offline interactions.

eIDAS regulation ensures that people and businesses can use their own national eIDs to access public services in other EU countries where eIDs are available (i.e. eID interoperability). eIDAS also ensures that eID services have the same legal status as traditional paper based processes, by providing certainty on the legal validity of these services.

To effectively achieve these objectives, the regulation provides for:

1. Transparency and accountability: well defined minimal obligations for Trust Service Providers (TSP) and liability.
2. Guarantee of trustworthiness of the services together with security requirements for TSPs.
3. Technological neutrality: avoiding requirements which could only be met by a specific technology.
4. Market rules and standardization certainty.

Realizing the full benefits of this regulation requires defining additional milestones as a push for adoption. EU regulators defined the following:

1. 17 September 2014: the eIDAS regulation came into force.
2. Mid-2015: member states may adopt relevant implementing acts to make use of the voluntary recognition of eID services of other member states.
3. 1 July 2016: the rules for trust services (eTS) apply.
4. Mid-2018: mandatory mutual recognition of eIDs applies.

eIDAS is certainly in place to regulate eID systems and their interoperability across European Union member states. But, realizing the full benefits of this technology requires additional efforts at the same EU level as well as on the national level, where member states are in charge of developing their eID systems.

Further efforts at the EU level include designing a clear and detailed framework of technical interoperability which member states can adopt to develop national eID systems, such a framework is a key enabler of a smooth and interoperable overall implementation. Furthermore, and as an additional option to consider alongside the much needed framework: developing an interoperable eID system at the EU level and providing eID-as-a-service to the member states that do not wish to develop an exclusive national eID system.

Progress is ongoing on both the European and national levels. A technical interoperability framework is in place, and some member states are making remarkable progress on national eID systems.

4.4.2.2 European Level e-ID Initiatives

Major progress in enabling the interoperability of national eID systems was made through large-scale multinational projects co-funded by the various technological development programmes of the European Commission.

The European Interoperability Framework (EIF[40]) first published in 2004 is a set of recommendations which specify how administrations, businesses and citizens communicate with each other within the European Union and across member states borders. It was published within the context of delivering interoperable eGovernment services. EIF serves as a high-level architecture of interaction, on which a technical interoperability framework can be built upon.

Seventeen out of twenty-nine member states have set up national guidelines on interoperability. A 2012 case study showed that nine out of these seventeen countries have their national interoperability plans aligned to EIF[41].

4.4.2.2.1 STORK

The technical battle for interoperability started in 2008 with the European project *Secure Identity across Borders Linked* (STORK). STORK was a competitiveness and innovation framework programme which included 35 partners from 18 European countries. Its main aim was: "*to establish a European eID Interoperability Platform that allows citizens to establish new e-relations across borders, using their national eID*" [42]. STORK recognizes the EIF and aligns with its principles.

This aim was achieved through laying down common technical rules and implementing an EU wide interoperable platform for the recognition of national eID and authentication. The STORK platform was built using open source and neutral technologies (JAVA, SAML 2.0)[43]; it is based on a distributed architecture that paves the way towards full integration of European e-services. Moreover, the platform takes into account infrastructure specifications of the currently existing eID systems in European member states. STORK platform is designed to be robust, transparent, safe to use, and scalable.

What STORK essentially delivered at the end of the project period in 2011 are common specifications. These have been defined on legal, organizational and technical grounds. Technical specifications resulted in a semantic model for interoperability that allows centralized and decentralized instances of cross-border authentication using national eID systems. Another significant result of STORK was the Quality Authentication Assurance (QAA) levels. STORK QAA levels were defined to achieve a mapping to a common model while acknowledging the different existing policies and procedures. QAA allows a common assessment of eID quality and authentication assurance, this makes it easier for member states to accept other member states eIDs regardless of their specific format.

Common code created and published by STORK facilitates the integration of identity providers and service provider. The code was released under a European Union Public License (EUPL) allowing for entities within member states to use the code for their integration process. STORK also defined and published process flows for the operational procedures to be adopted for interoperability and integration.

[40] http://ec.europa.eu/isa/documents/eif_brochure_2011.pdf
[41] https://joinup.ec.europa.eu/news/european-countries-aligning-their-interoperability-policies
[42] https://www.eid-stork.eu/
[43] For service providers PHP and .net is also supported.

4.4.2.2.2 STORK 2.0

STORK 2.0 is an ongoing European project that is building on the results of STORK; the project consortium consists of 58 partners from 18 European Union member states and Turkey. It aims to establish interoperability at EU and national levels through different approaches: eID for persons, eID for legal entities. STORK 2.0 makes use of experiences from four cross-border, cross-sector pilots to demonstrate the use and societal impact the infrastructure developed in STORK.

The project extends the common specification and building blocks for interoperable legal identities and mandates, on top of the interoperability infrastructure developed in STORK. It also aims to solve legal issues arising within the scope of the pilots for privacy, data protection, and liability across the different national entities involved. STORK 2.0 includes an update of the STORK QAA model to include attributes, legal entities, and mandate agreements.

eID packaged as a service for EU national governments and businesses is also part of the project deliverable plan, giving an opportunity to national governments to circumvent developing a national eID system and aligning it with European interoperability standards (e.g. EIF) since the STORK platform is aligned by design. The project addresses eID governance issues through the requirements for an accreditation body.

STORK 2.0 pilots are focused on strategic eLearning and Academic Qualifications, eBanking, Public Services for business and eHealth services. Pilots demonstrate interoperable services in real-life settings and validate the common specifications laid down; pilots also assure the harmonization of interoperability standards and infrastructure building blocks.

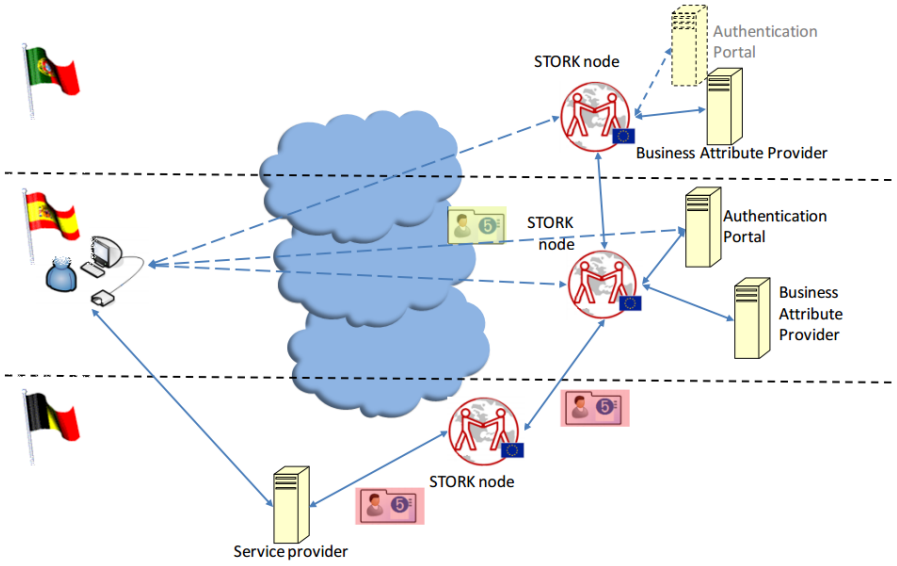


Figure 30: STORK 2.0 Architecture with Centralized Nodes (source: STORK 2.0 Deliverable D4.2, p.95, MINHAP , 2013)

Figure 31 illustrates an architectural use case of the STORK 2.0 platform, where a Spanish user accesses a Belgian service and has additional Portuguese business attributes. In this case the user indicates that she/he has business attributes in Portugal. The Belgian service provider requests

authentication-with-business-attributes for the Spanish user; this request passes through the Belgian service provider's Pan European Proxy Server (PEPS) and on to the STORK node.

The STORK node communicates with the Spanish authentication portal and sends the reply back to the Belgian PEPS. An ad hoc request is made through the STORK node to the Portuguese authentication portal for authenticating the business attributes. The Portuguese STORK node, or authentication provider, or attribute provider may request re-authentication.

4.4.2.2.3 eSENS

Electronic Simple European Networked Services is a European project that is focused on public administration service networking across member states. It runs until 2016 and is being managed by 22 partners from 18 EU countries in addition to Norway and Turkey. The project aim is to "*consolidate, improve, and extend technical soultions to foster electronic interaction with public administrations across the EU"*[44].

eSENS will facilitate operations that involve administrative procedures, in a cross-border context, by:

- Making it easier for companies to set up inter-state business electronically.
- Enabling electronic procurement procedures for businesses.
- Creating seamless access to EU legal systems.
- Making it easier for citizens to use healthcare services while in another member state.

Technical solutions developed by eSENS are within the areas of: e-Delivery, e-Documents, e-Identity and e-Signatures. Most relevant to this deliverable are the technical solutions provided for e-Identity and e-Signatures. Solutions in these domains are an extension of the STORK and STORK 2.0 deliverables. The eSENS project recognizes the importance of assuring the wide spread usage in post-development stages through adopting the earlier interoperability standards laid down by previous European regulations and predecessor projects.

The eID building block of the eSENS project aims to establish cross border recognition and eID validation that meets the requirements set for e-Government applications in different domains. Thus e-SENS permits businesses, citizens and government employees to use the presently widespread (national) identities in cross-border public and private services. The solution includes the know-how gained in STORK which is developed to provide infrastructure for cross-border use of government-endorsed electronic identities and exchange of attributes, including roles and mandates as needed by various on-line services[45].

4.4.2.3 National Level eID Initiatives

Much work has gone into developing European national systems that can recognize and verify digital identities. But providing a widely used national system, letting alone interoperable systems for the moment, is yet to be achieved for most EU member states.

[44] http://www.esens.eu/
[45] http://www.esens.eu/technical-solutions/e-sens-competence-clusters/e-identity/

The economist (2014[46]) describes achieving full societal benefits of a widely used and trusted eID system as a 'Cyberdream'. In fact, the benefits of such a 'dream' are remarkable in terms of how they support the profound change in the relationship between citizens and their state authority that happened over the past years.

The classical passive mono-directional interaction between citizens and authority has become bi-directional, where citizens are given an increasingly pro-active role to play in managing their identities and official digital interactions. This entails citizens taking active responsibility for their identity, to fulfil their obligations and easily access their rights.

4.4.2.3.1 Benefits of National eID Systems

Google, Microsoft, Facebook, Twitter and other large service providers are all trying to make their accounts a form of eID. But these are issued without verification, so pseudonyms are rife and impersonation easy. At the same time, private Identity Verification Service Providers (IVSPs) offer their own eID services (e.g. Trulioo, IDchecker, miiCards), while these entail some identity verification by the IVSP, they fall short of the reliability of a state-backed identity: that is issued by a government official, verified against other data sources, using biometric data and legitimized by law.

The benefits of national eID to **citizens** can be summed up in this sentence: 'A trusted, reliable, secure, and easy-to-use authentication system for accessing online governmental and non-governmental services'. Such a system acts as a trusted gateway to e-services of all types. And the real level of citizen benefit is reflected in the magnitude and usefulness of available e-services. These e-services range from small routine interactions like paying a parking meter fee, to larger ones like filing personal annual tax returns, or even starting a new company.

The benefits of eID to **governments** are more varied in nature and include:

1. Designing a national eID system provides an opportunity to design a uniform national e-government strategy, or more specifically, a strategy of governmental e-services, which can be established and built upon in the future. This opportunity also includes defining the government-citizen e-relationship, and the infrastructure on which such a system would operate.
2. A national eID system is a common platform serving many governmental administrative divisions (if not all), which reduces overall maintenance and operating costs.
3. New e-government services can be easily installed and plugged into the eID system, reducing citizen reach time. New services can originate from any governmental administrative division.
4. Simplification and automation of administrative tasks reduces complex bureaucracies and increases service efficiency. Automated validation procedures can be implemented, as well as automated audits.

[46] http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge

5. Change processes can be reduced to adjusting the business rules of the overall system, increasing change speed and decreasing change costs.
6. Secure identities, automated validation, and automated audits together detect, prevent and reduce fraud (e.g. identity fraud, financial fraud, mismanagement.. etc).
7. Insight extracted from the system information leads to the identification of optimization opportunities that serve continuous improvement.

The benefits from a trusted identity service to private **businesses** overlap with those gained by governments, and are also varied in nature:

1. Extending their service portfolio in a faster, easier, and more cost effective fashion.
    a. eID system already exists and new services can be plugged in.
    b. Easier integration of new services to eID systems.
    c. Economies of scale save costs.
    d. Decreased time-to-market.
2. Easier access to e-services provided by governments and other businesses alike.
3. Reducing identity fraud risk.
4. High number of potential users resulting from a widely accepted national eID system.

Estonia is a place where what the Economist described as an eID 'Cyberdream' is more of a reality than any other place. The following section provides more details on Estonian eID, as well as other examples from member states which made progress on their national eID systems.

4.4.2.3.2 Estonian eID as a leading national eID system

Estonia has by far the most highly-developed national ID card system in the world. Impressive facts and statistics highlight this digital success: There are more than 1.23 million active eID cards in Estonia. That's about 95% of Estonia's 1.3 million residents[47]. Before a newborn even arrives home, the hospital will have issued a digital birth certificate and his health insurance will have been started automatically. Taxes take less than an hour to file, and refunds are paid within 48 hours. The Estonian state offers 600 e-services to its citizens and 2400 to businesses[48].

The same mandatory national picture ID card serves as the digital access card for all of Estonia's e-services. The chip on the card carries embedded files which, using 2048-bit public key encryption, enable it to be used as definitive proof of identity in an electronic environment. Worth noting that the data stored on a card (although heftily encrypted) is kept to a bare minimum, stolen or lost cards can be easily cancelled.

Estonian eID card can be used for any public or private e-service that requires secure identification. Here are some examples of how the eID card is used in Estonia:

[47] http://id.ee/
[48] http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge

- As a national ID card for legal travel within the EU for Estonian citizens.
- As the national health insurance card.
- As proof of identification when logging into bank accounts from a home computer.
- As a pre-paid public transport ticket.
- As an authentic payment method.
- For accessing state e-services portal (tax, welfare & social services, starting a new company..etc).
- For accessing educational records and employment history.
- For viewing and paying fines.
- For digital signatures (status upgraded to legally binding).
- For i-voting (internet voting).
- For accessing electronic health records and picking up e-Prescriptions.

MOBIIL-ID is an Estonian service that allows a client to use a mobile phone as a form of secure electronic ID. Like the ID card it can be used for accessing e-services and digitally signing documents. It is an optional extension of the eID card that does not require a card reader.

Two PIN codes are also issued along the mandatory eID card, one for authentication (proving who the holder is) and one for authorization (signing documents or making payments). Upon user login to an e-service, the service queries a central database to authenticate the user identity. This authentication procedure conforms to the principles of limited disclosure technology to protect the user privacy. So an e-service querying an authentication database does not ask "*how old is this person*?", but instead asks "is this person over 18?", in this case the returned information is a true or false value that does not reveal the user's age.

To emphasize the efficiency of the Estonian state in handling user data, Estonian law indicates that the state may not ask for any piece of information more than once. People also have the right to know what data is being held on them.

As a general rule, government systems in Estonia are not allowed to store the same information in more than one place. At the same time, there is no one place where all the information about someone is held. These two simple rules applied to technically complex systems assure that any breach to system security would limit any data leaked to a bare unusable minimum, and does not provide a complete de-anonymized de-encrypted citizen profile.

Basic personal details[49] are stored in a relational population database (see Figure 31). This database provides each citizen with a unique identifier, and this identifier is stored in other databases where citizen basic information is required, eliminating the need to replicate the same data in different locations. Interestingly, visualizing the data in the Estonian population database generates a family tree of the nation that goes back until about 1950.

[49] Name, date of birth, sex, address history, citizenship and legal relationships.

The Estonian e-Services architecture (Figure 31) is based on the principles of Service Oriented Architecture (SOA) distributed application design pattern. X-Road is a secure data sharing layer that employs messaging and web service standards. X-Road enables, secures, routes, and translates communication messages across the various system components (i.e. Message Broker). The Estonian X-Road network is comparable to an Enterprise Service Bus (ESB) topology that is suitable for loosely-coupling heterogeneous and complex application landscapes. ESB is an Enterprise Application Integration (EAI) topology.

The same government issued eID is used to authenticate users and authorize procedures across the system landscape. Enabling private services to integrate to the system and use the same eID for their non-governmental services is an opportunity to leak the same secure thinking (e.g. limited disclosure technology) into the private sector.

This architecture is technically sustainable over the long term since old legacy (or legacy-to-be) systems can be plugged out of the overall architecture and new systems can be plugged in (as opposed to tight coupling). Systems do not have to share commonalities and also do not share fatal dependencies, allowing the different system components to evolve (e.g. scale, develop, test..etc) independently while still being able to function as part of the overall system. Persistency, priority and queuing mechanisms can be defined and altered for different procedures as part of the data sharing layer (X-Road).

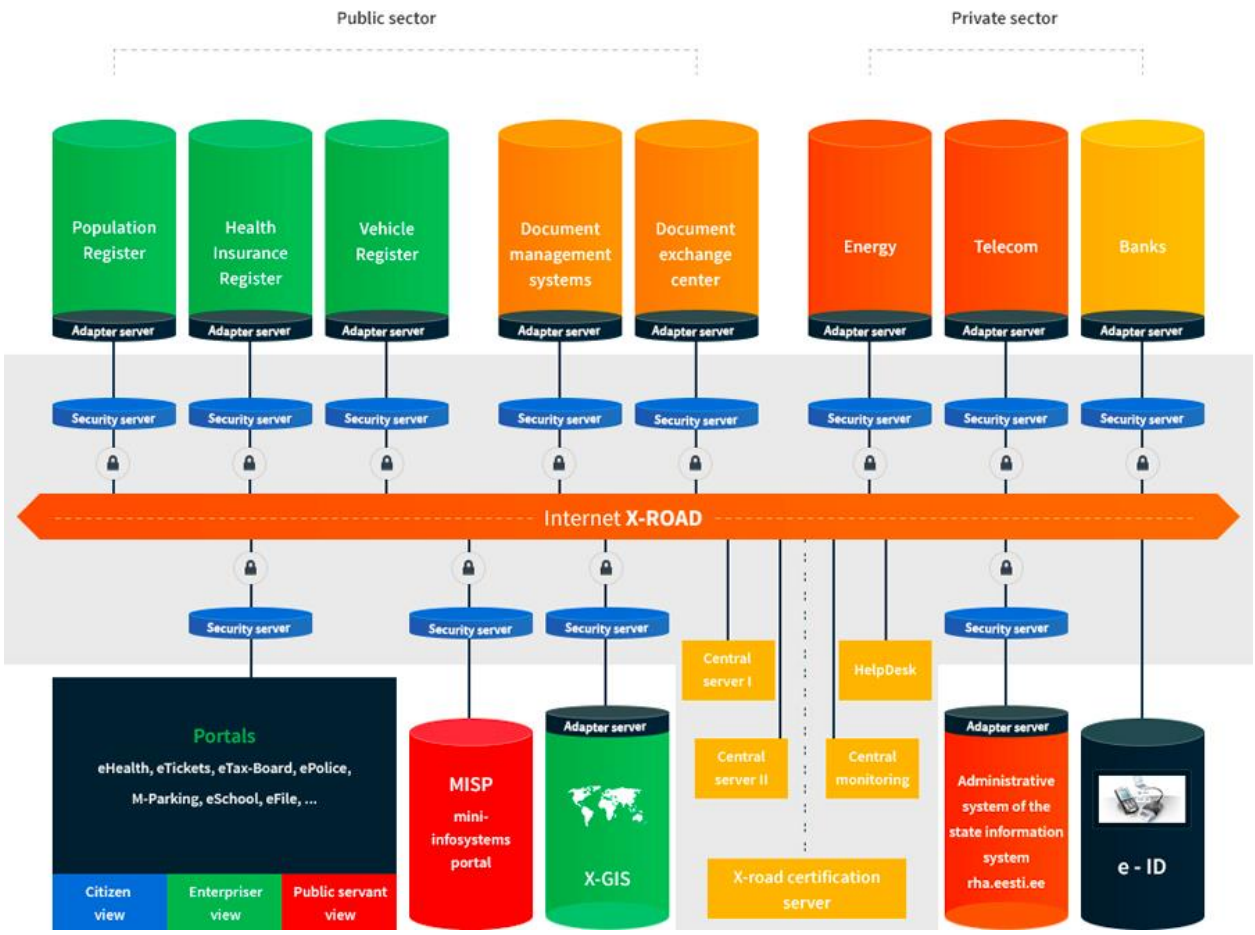


Figure 31: Estonian e-Services Architecture and X-Road.

The advanced status quo of the Estonian digital market provides a unique opportunity that Estonia hopes to fill. Citizens of other nations of the world where the digital market has not yet reached a similar level of maturity will be able to obtain Estonian e-residency[50]. This extension of the Estonian digital market allows e-residents to make use of the same e-services provided to Estonian citizens.

4.4.2.3.3 Other European Experiences

Some other European countries have already developed and adopted eID technology, but there are stark disparities among different countries experiences and implementations. In this section cases from five other European states are summarized to extract main lessons that could be of benefit to others.

Netherlands

First Launched in 2003 the Dutch DigiD[51] was made available to citizens as of the beginning of 2005. By 2013 the system was handling over 20 million monthly authentications, and the number of users

[50] https://e-estonia.com/e-residents/
[51] https://www.digid.nl/

surpassed 10 million. eHerkenning[52] is a parallel service to DigiD provided to authenticate identities of legal bodies (e.g. companies). Both DigiD and eHerkenning are provided at no cost to end users. Organizations that offer services with DigiD are governmental organizations, municipalities and provinces, pension funds, law enforcement, water boards, healthcare providers, and health insurers. DigiD is a basic form of eID as it only supports username and password authentication and does not include a physical electronic identity card, for this reason it is being replaced by Dutch eID[53]. An initial controlled implementation phase for Dutch eID is planned for the beginning of 2018[54].

Belgium

Belgium started using eID in 2004. Since 2009 its possession is mandatory for all Belgian citizens. A national database containing information on every citizen was already in place prior to the introduction of eID, so there was less debate on government collecting citizen data than in other countries. Belgian citizens can check online what information the government stores on them. In terms of the usability and availability of services, the Belgian eID is yet to be implemented as a payment method, a voting method, and other uses. For the time being Belgian citizens can use eID to pay taxes online.

Italy

First introduced in 2001 and aims to replace paper identity cards. Since then about 83 Italian cities and towns have adopted eID and started issuing electronic cards. eID remains not mandatory for Italian citizens, reflecting on the current low adoption rates. Italian eID stores biometric data directly on the card.

Finland

Introduced in 1999 and considered a failure by the Finnish government. Recommendations to cancel the card surfaced to the Finnish government in 2009 because it had only been adopted by 300000 people out of the 5 million living in Finland. Finnish eID remains not mandatory for citizens to obtain. Finnish eID does not store biometric data directly on the card.

Sweden

Swedish eID is in a similar situation as the Finnish one. It costs citizens 400SEK (42 euros) to issue the card, and it remains not mandatory. For these reasons it is currently being used by only 1% of the population (100000 people). People often choose to use their driver license or their passport (which costs 2 Euros more to issue compared to the eID). Swedish eID does not store biometric data directly on the card.

Portugal

Similar to Italy, Portuguese eID users must give their fingerprints to the government to obtain eID. In Portugal the eID card replaces 5 different cards: the identity card, the tax card, the social security card, the voting card, and the social services card. 2.5 million eID cards are currently in use. The Portuguese government created a database to store citizen data and simplified the relations

[52] https://www.eherkenning.nl/
[53] http://www.eid-stelsel.nl/
[54] http://www.eid-stelsel.nl/fileadmin/eid/documenten/Factsheet_-_Planning_eID_Stelsel.pdf

between its administration and citizens. Portuguese eID can be used for a large variety of online government services.

4.4.3 Conclusions

1. Early partnership among government, private sector service providers and IT sector eases the development of a national eID system and eases adoption.
2. Plugging in private sector services increases the adoption of eID, and provides an opportunity for the private sector to avoid developing and adopting their own authentication systems.
3. Minimizing complex relationships between governmental administrations and easing the relationship between the government and the citizen are important to achieve a usable eID system. Automating complexity does not lead to a simple final system.
4. Estonian eID architecture proved robust over the last decade. No security breaches were recorded, and the sustainable architecture ensures continuity.
5. Enabling private services to integrate to the system and use the same eID for their non-governmental services is an opportunity to leak the same secure thinking (e.g. limited disclosure technology) into the private sector.
6. Cost to issue an eID should not be higher than issuing a regular ID card. In case a basic eID system (i.e. username and password authentication) is provided to citizens and companies it should be free of charge.
7. Issuing an eID should become mandatory to all citizens after a pilot stage and proof of concept and usability.
8. eID can be extended as a service from the European level to the national level. This can be of interest to countries that do not wish to develop their own eID systems. And to countries where there is a low level of trust from citizens towards their governments in handling their data (including biometric data).
9. Other identity service providers could (e.g. telecommunication service providers) can be considered.
10. Private sector companies adopting a national eID system avoid the cost and hassle of implementing a private eID system for their e-services.
11. Private sector companies can benefit from an increased traffic to their services resulting from integrating a widely used national eID system, making it easier and more trustworthy for user to access these services.
12. Private sector companies adopting a widely used national eID system that is interoperable with European eID systems may benefit from additional traffic incoming from European eID users.
13. Providing an extension of eID to use mobile phones as an authentication method (e.g. Estonian MOBIIL-ID) leads to increased adoption and ease-of-use as it eliminates the use of using the electronic ID card accompanied with a card reader for authentication.
14. National eID increases user trust towards services that adopt it.
15. The real benefit of eID systems is reflected in the magnitude and usefulness of e-services that it leads to.

5 Identifying current Opportunities & Threats for Trustworthy ICT in Europe

5.1 Introduction

SWOT stands for strengths, weaknesses, opportunities and threats. A SWOT analysis identifies strengths and weaknesses within a company or organization, and outside opportunities and threats. The results of a SWOT analysis lead to specifying actions that correspond to the identified elements. These results can then be used to improve the overall situation of the company or organization. Using SWOT actionable results can reduce the likelihood of developments that negatively affect the organization while improving performance.

In the following sections of this chapter (5) we lay down the foundation for overall ATTPS SWOT Analysis, present the methodology followed for the identification, iteration, and validation of the Opportunities & Threats.

Chapter (5) concludes with a presentation of the full results of this O&T analysis.

5.2 The Foundation and Case for ATTPS SWOT Analysis

5.2.1 SWOT Foundation

A common competitive strategy analysis begins with the iterative assessment of the external environment and the organization's internal capabilities. This process of looking outside as well as inside is known by the acronym "SWOT": Strengths, Weaknesses, Opportunities, and Threats. (Harvard Business Review, 2015)

Within the scope of deliverable (D1.1) is the internal analysis: **Strengths & Weaknesses**.

Within the scope of this deliverable (D1.2) is the external analysis: **Opportunities & Threats**.

ATTPS D1.1 and D1.2 tackle SWOT (Figure **32**) of the Trust Paradigm Shift by relating it to the prospects of trustworthy ICT in Europe as an emerging segment within the information technology industry. This overall assessment is performed in two main parts:

1. **External Analysis**: identification, iteration, and validation of Opportunities and Threats for trustworthy ICT in Europe.
2. **Internal Analysis**: grasping the internal strengths and weaknesses of a representative sample of EU funded projects in the fields of Cybersecurity and Trustworthy ICT.

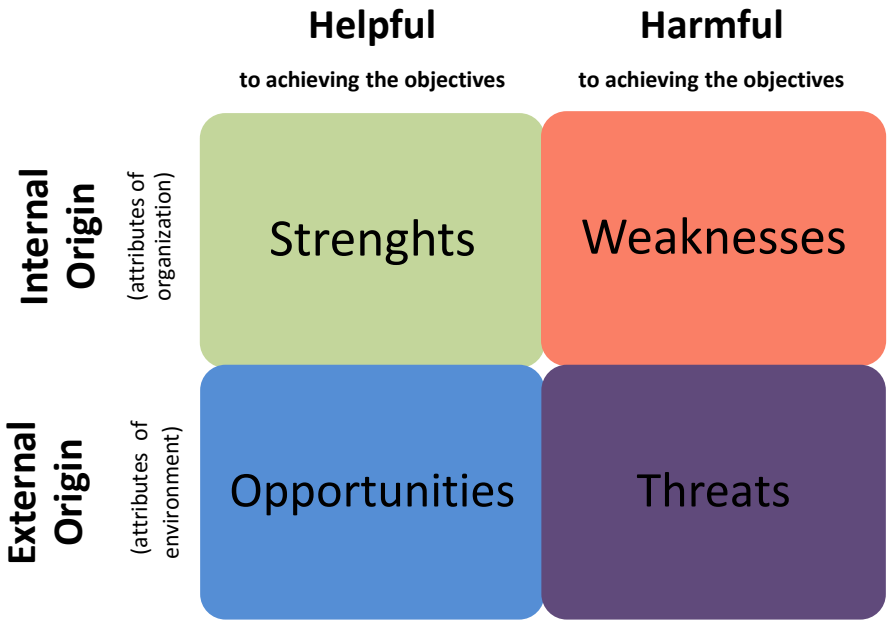


Figure 32: SWOT Analysis Matrix

A SWOT analysis aims to identify the key internal and external factors which contribute or potentially hinder achieving a strategic objective. An **Opportunities and Threats analysis** (O&T) is an **exclusively external** analysis (i.e., opportunities and threats presented by the environment external to the entity at hand).[55]

5.2.2 The Case for ATTPS SWOT Analysis

Understanding the dynamics of the future of the Trust Paradigm Shift is similar in nature to a Strategic Business Analysis also known as Competitive Strategy Analysis (*long term, based on current facts, forward-looking, and analytical*) (David, 2005). This similarity is because achieving the favourable outcome of the Trust Paradigm shift is also a:

1. **Long term objective**: as the Trust Paradigm Shift is a long-running process (*section 4.1 under the TPS boundary definition*).
2. **Based on current facts, knowledge and trends**: a useful analysis of the TPS requires gauging current facts, knowledge and trend considerations of the current paradigm (*chapter 3 and chapter 4 detail the theoretical background, literature review, trend measurement on which the Opportunities & Threats analysis is based on*).
3. **Forward-looking**: the nature of strategic processes is forward-facing; the TPS Opportunities & Threats analysis is also concerned with the future of the current paradigm.
4. **Analytical**: analyses gauged facts, knowledge and trends to formulate reasonable and data supported recommendations for the future of the TPS.

[55] http://www.businessnewsdaily.com/4245-swot-analysis.html

Moreover, current fact and knowledge are of **internal** and **external** nature. This is due to the followed approach in this research. As in Deliverable 1.1 a Project Portfolio Analysis is conducted over a set of European funded projects in the domains of cybersecurity and Trustworthy ICT. The data collected and used as input for this portfolio analysis includes internal project information and performance metrics. For this, the internal and external factors of both O&T Analysis and Portfolio Analysis are further defined, as follows:

1. **Internal factors**: facts, knowledge, and performance metrics of projects and/or organizations undertaking projects and/or initiatives within the domains of cybersecurity and trustworthy ICT.
2. **External Factors**: facts, knowledge, and trends of the external environment of projects and or/organizations undertaking projects and/or initiatives within the domains within the domains of cybersecurity and trustworthy ICT. External environment span from domain to Market, and Industry. And from National, to Continental (European), and to Global.

5.2.2.1 Benefits and Limitations of SWOT

SWOT has 5 key benefits (Coman, 2009):

1. Simple to do and practical to use;
2. Clear to understand;
3. Focuses on the key internal and external factors affecting the organization;
4. Helps to identify future goals;
5. Initiates further analysis.

Here are the main SWOT limitations identified (Pickton D.W., 1998) ,

1. Excessive lists of strengths, weaknesses, opportunities and threats;
2. No prioritization of factors;
3. Factors are described too broadly; factors are often opinions not facts;
4. No recognized method to distinguish between strengths and weaknesses, opportunities and threats.

ATTPS **recognizes** these limitations and addresses them as follows:

1. **Excessive lists**: broad lists of opportunities and threats resulting from brainstorming sessions are scrutinized. The items voted as being of lowest importance by expert groups are refined and integrated with related main items or removed from final model. Final lists provide iteratively refined opportunities and threats.
2. **No prioritization of factors**: While basic SWOT analyses do not usually include prioritization of identified items, ATTPS adopts an "*Advanced SWOT Analysis*" methodology. This methodology includes iterative three-tier probability ranking, and importance ranking. Both of these rankings are based on iterative expert groups voting.
3. **Factors are described too broadly; factors are often opinions not facts**: ATTPS noticed this limitation at the very early stages of O&T Analysis (first brainstorming session). Focus was

put throughout the model development stages of (*refinement, validation, and iteration*) to rely on factual sources that describe identified opportunities & threats to a sufficient level of detail for intended technical and business oriented audience, or the public.

4. **No recognized method to distinguish between strengths and weaknesses, opportunities and threats:** while there are no formal methods for this kind of distinction that we know of, whether ones that are applicable to a broad range of industry use cases, or cybersecurity and trustworthy ICT as domains. ATTPS research aims to exhaust each identified item from both aspects of being an opportunity or a threat. This is to make sure opportunities and threats originating from the same or a related area of focus are both addressed.

5.3 Aligning ATTPS SWOT Analysis to Strategic Business Analysis

Strategic Business Analysis includes the following exhibits (Strategic Analysis Model) (Boulton, 1996-2001):

1. **Industry analysis**: a definition of products and markets, skills and competitors contained within the industry.
2. **Business strategy analysis**: description of the strategic goals and business strategy.
3. **Strategy evaluation**: or SWOT analysis encompassing both the internal and external factors that affect the business strategy.
4. **Critical issues and recommendations**: seek to identify the critical issues that need to be done. The analysis concludes with recommendations that address the critical issues and result in changes of product-market strategy or functional implementations.

Table **14** aligns the elements of the Strategic Analysis Model above with the analysis method followed in ATTPS.

Table 14: Aligning ATTPS Analysis to Strategic Business Analysis

Strategic Analysis Model Element	ATTPS Analysis Element and Rationale
Industry analysis	Three main pillars of research identified, literature review and qualitative research conducted on these three main pillars. The market and products for cybersecurity and trustworthy ICT are taken at face value for qualitative research and further defined through ATTPS questionnaire in D1.1.
Business strategy analysis	Qualitative analysis performed on European Cybersecurity Strategy. Used for Strategic Fit Analysis in D1.1. and for Gap Analysis in D1.1.
Strategy evaluation	Strengths & Weaknesses Analysis conducted as part of sample project questionnaire analysis conducted for Portfolio Analysis in D1.1. to identify S&W of projects in scope. Opportunities & Threats developed based on research of D1.1 and validated through the Delphi method and expert opinion validation sessions (further detailed in following section 5.4).

Critical issues and recommendations	Identified as a result of qualitative research of D1.2 (three pillars and O&T Analysis, as well as a result of Project Portfolio Analysis in D1.1.

In the following section we discuss the common "textbook" SWOT Analysis methodology. We also present and explain the ATTPS Opportunities & Threats Analysis and Validation Methodology.

5.4 Opportunities & Threats Analysis Methodology

Opportunities and threats are the external uncontrollable factors that usually appear or arise due to the changes in the macro environment, industry or competitors' actions. Opportunities represent the external situations that bring a competitive advantage if seized upon. Threats may damage your company so you would better avoid or defend against them.

The initial source of identification for ATTPS O&T Analysis was the qualitative research performed in D1.2. As presented in the earlier chapters of this document, this research investigates three main pillars as focal areas of interest. Moreover, sources from leading business research organizations (e.g. Gartner), and academic research (i.e. journal publications and university research publications), are also used to identify market trends, technology maturity, and competition levels. These insights helped formulate the initial set of opportunities and threats through additional brainstorming.

Market changes provide the most visible opportunities and threats. These changes are often introduced by major regulatory changes, new technology entries to market, new innovations, and the like of relatively disruptive market changes. Market coverage, as in European originating ICT products and services as opposed to non-EU originating services is taken into consideration, in order to focus these opportunities and threats to a European cybersecurity and trustworthy ICT perspectives. Simply, when new geographical markets open up or are showing demand for a service or product, companies have an opportunity to increase exported service volumes or start operations in a new country.

From another perspective, niche markets bring in the risk of a narrow market segment, although sometimes niche markets expand unexpectedly due to technological or other changes. In such cases, spikes of increased demand are witnessed. As a result, changes in the market create new opportunities and threats that must be seized upon or dealt with if the company or concerned organization intends to gain and sustain market share and competitive advantage.

Most external changes can represent both opportunities and threats. For example, from a medium or large business perspective, new regulatory changes within a specific market may bring in opportunities arising from regulatory market needs, fulfilling these market needs attracts investment, thus increases opportunities. But at the same time disproportional over-regulation of the same market may hinder or restrict business performance. In such a case, regulatory changes can in fact bring in opportunities and threats at the same time.

In practice, any organization can *only* guess the outcome of a future change and rely on business analysis forecasts. In such analytical future-looking rationales like ATTPS SWOT; the best possible judgement is made based on current knowledge and reliable factual information.

Figure **33** illustrates the ATTPS Opportunities & Threats Analysis and Validation Methodology.

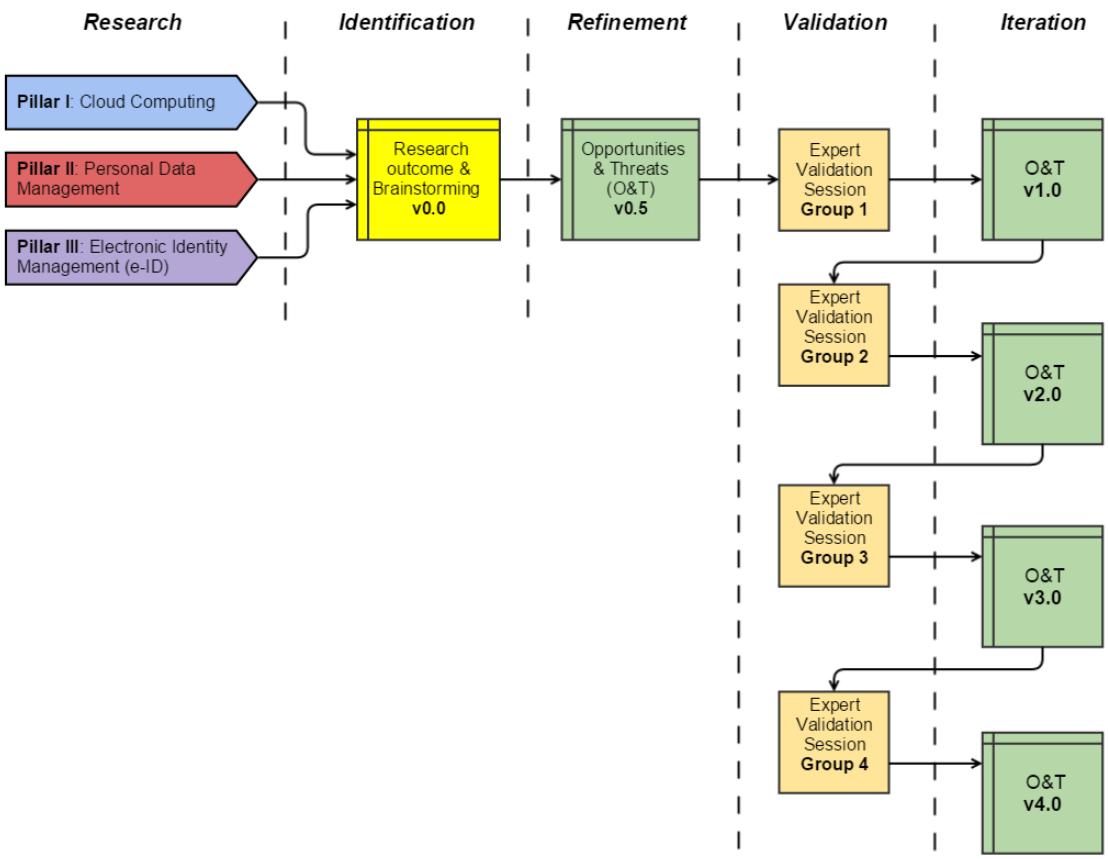


Figure 33: ATTPS Opportunities & Threats Analysis and Validation Methodology

Research for Opportunities & Threats (Figure 33) is rooted in the three main pillars of this research document (Chapter 4). From which an initial model (*v0.0*) firstly *identified* an initial set of opportunities and threats (O&T model), and secondly *expanded* on the list through brainstorming.

The initial O&T model was then *refined* to scrutinize the results of brainstorming and reduce the excessive number of items. Refinement stage was followed by an *iterative validation* and model update process.

5.4.1 Validation

Iterative validation sessions were planned and organized with a number of industry experts from cybersecurity and trustworthy ICT domains. Experts include direct subject matter experts in European electronic identity regulations, projects, and initiatives. As well as industry executives from

cybersecurity and software development sectors, and technical research experts affiliated with non-profit academic (university) research programs.

Validation sessions were conducted using teleconferencing facilities due to the wide geographical distribution of experts in Europe. The Delphi Method[56] of forecasting was adopted and adapted for the design of ATTPS validation sessions.

The Delphi Method is a structured communication technique; it was originally developed as a systematic, interactive forecasting method which relies on a panel of experts. The Delphi Method is a widely used and accepted method for gathering data from respondents within their domain of expertise. The Delphi process is iterated until consensus or minimal levels of feedback are achieved. Usually three Delphi iterations are sufficient to achieve expert consensus, and sometimes a fourth round is conducted if feedback levels after the third round are still considered of sufficient value (Chia-Chien Hsu, 2007).

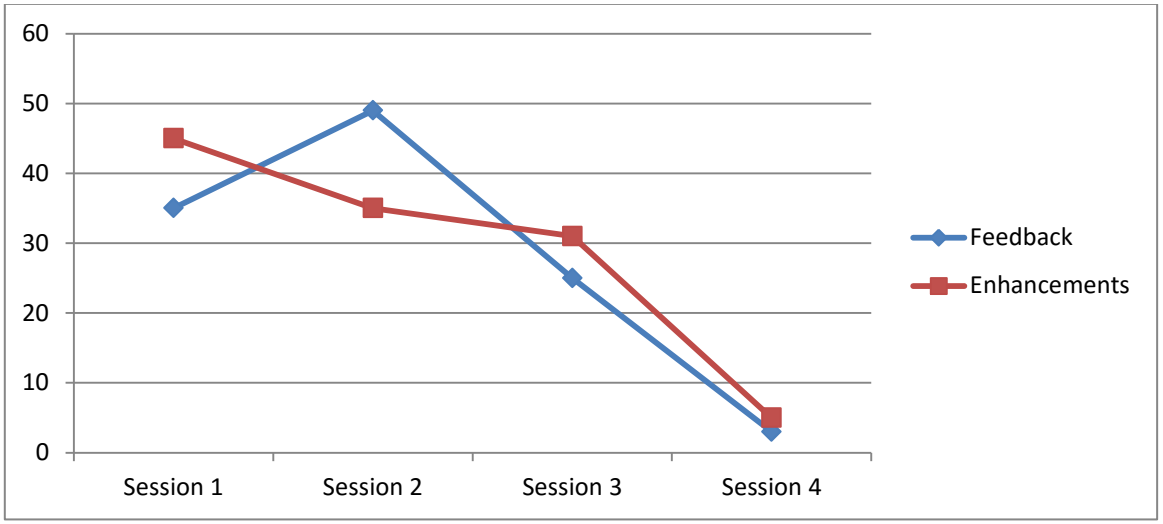


Figure 34: Validation Sessions Feedback & Enhancements

ATTPS validation sessions adopted Delphi Method as part of the sessions (50%). The remainder (50%) of session times were used for un-facilitated open discussions. This choice was made to ensure that both a structured and an unstructured communication technique are used in these sessions, in order to maximize the exhaustion of ideas and topics at hand.

The validation sessions were preceded by an initial voting on the prioritization of opportunities and threats in terms of importance, as perceived by the experts. Anonymized aggregated importance voting results were shared and discussed among experts. A second round of voting on the final (v4.0) model was conducted after the final validation session. This voting constitutes the source for the

[56] First developed by Dalkey and Helmer (1963) at the RAND Corporation in the 1950s: U.S. global policy nonprofit Think Tank.

prioritization of opportunities and threats, as part of the Advanced SWOT technique adopted in ATTPS.

5.4.2 Prioritization Technique

Opportunities and threats are prioritized through an evaluation of expert votes. Electronic voting over the initial model and the final model were conducted. Voting results were anonymized, aggregated and further analysed to produce insight. The voting and analysis technique is presented in this section, while the final prioritization results are presented in section 5.5.2 (Prioritization).

Voting was conducted the same expert panels from the validation sessions. Experts provided an initial vote before the first session, and were provided with aggregated results for discussion during the validation sessions. Experts provided a final vote after the last validation session. The analysis presented in section 5.5.2 is based on aggregate (duplicate sanitized, cross-matched) results of both voting rounds.

5.5 Opportunities & Threats Analysis Results

5.5.1 Final Model (v4.0)

The final Opportunities & Threats model provides the following information:

1. **Opportunity/Threat**: name of the opportunity or threat.
2. **Description**: details of the opportunity or threat.
3. **Category**: places the opportunity of threat in *one or two* of four defined categories (Figure 35) as follows:
    a. **Opportunity:** where direct value resides.
    b. **Opportunity Driver:** where drivers of value reside.
    c. **Threat Alleviator:** where threat minimizers reside.
    d. **Threat:** where direct threats reside.
4. **Type**: places the opportunity or threat in *one or more* of four defined types. This helps attract the reader's attention to items relevant to their interest. As follows:
    a. **Business**: ones that have potential to generate or hinder revenue for related businesses.
    b. **Technical**: ones that are intended to be explored by technical researchers, research organizations, and universities. These aim for the advancement of technology, or finding solutions to potential technical problems.
    c. **Umbrella**: ones that are intended for the attention of governmental bodies and non-governmental organizations involved in legislation and regulation activities. These aim for legislating and regulating the changing market environment. These are enablers of business opportunities.
    d. **User**: ones that have the potential to benefit or risk individual end users, their information, and their interaction with businesses and governments through systems.
5. **Purview**: defines the scope of external influence on each opportunity or threat.

Figure 35: four categories of opportunities and threats.

The tables on the following pages include all identified opportunities (Table 15) and threats (Table 16).

Table 15: Opportunities for Trustworthy ICT in Europe.

	Opportunity	Description	Category	Type	Purview
1	Trustworthy service certification	Services and service providers can benefit from trustworthiness certifications which are granted on request after adhering to trustworthiness guidelines defined by certifying organizations (e.g., ISO/IEC 27001:2013[57]). Certifying organizations can benefit from introducing industry-specific and service-specific certification programs. Publicizing the 'Trustworthiness certified' status of a service or a service provider is a stimulant for potential user social-psychological trust.	Opportunity. Opportunity Driver.	Business.	Competitive position. Regulatory.
2	SMEs may increase service traffic and avoid costs by adopting relevant widely-used national IT systems[58]	Plugging in private sector services to national IT systems that are widely adopted by citizens may increase traffic to small and medium enterprise (SME) services. SMEs may also avoid the costs of developing alternative private systems.	Opportunity.	Business.	Emerging business opportunities. Business policy change. Funding sources.
3	Adopting and improving multi-factor authentication for medium and high risk online operations	Introducing multi-factor authentication (MFA) as a mandatory authentication for online operations where a risk of breach is high, or could lead to real and quick damage (e.g. e-banking, m-banking, e-ID) and major single sign-on (SSO) services (e.g. Google accounts, Microsoft accounts). Researching and introducing inherence factors (e.g., biometrics) and behavioral factors analysis (e.g., keystroke dynamics, mouse dynamics) as additional factors for MFA. Usability is usually affected by increased security measures like MFA, it is important to assure service continuity by minimizing the effects on usability and ease-of use.	Opportunity Driver.	Technical.	Business policy change. Research-induced technological change.
4	Improving single-factor user authentication mechanisms	Enhancing username/password combination authentication (knowledge-based) by introducing shared secret authentication (e.g. additional passwords, site keys, challenge-response, randomized code selections that are based on input patterns). Usability is usually affected by increased security measures, it is important to assure service continuity by minimizing the effects on usability and ease-of use.	Opportunity Driver.	Technical.	Business policy change. Research-induced technological change.
5	Developing and adopting European-level legislations and regulations for trustworthy ICT	Keeping up with new technologies by laying down groundwork for generic electronic interaction legislation, regulation, and enforcement mechanisms (LRE), as well as technology-specific LRE (i.e. legislation that is closely tied to a certain technology) (e.g. eIDAS regulation for e-ID technology[59]). Maintaining a necessary balance between how generic or technology-specific an LRE is essential to assure LRE validity on the long term. Enacting LREs that are overly generic creates confusion in the marketplace and could lead to ineffective results. While designing LREs that are overly technology-specific risks the long term applicability of	Opportunity Driver.	Umbrella.	Legislation. Regulatory.

[57] http://www.iso.org/iso/catalogue_detail?csnumber=54534

[58] **National IT System**: is an ICT system implemented at the national coverage level of any European Union member state to provide e-services to respective state citizens, residents and businesses. This is regardless of infrastructure management and control rights (national IT systems can be run by a private sector party or consortium, while data remains in state control). For example: Dutch national tax filing and return system, or Estonian DigiDoc system for storing, sharing and digitally signing documents.

[59] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

		these LREs and/or hinders innovation within the corresponding technological field. Technical specifications for both generic LRE and technology-specific LRE should be provided for each enacted LRE to facilitate technical implementations. Technical specifications are usually decoupled from primary LRE texts to avoid legal and technological terms mix-up, and are instead provided in secondary publications (e.g. appendices to an LRE, or secondary technical specification publication).			
6	Developing and/or adopting European ICT governance and compliance mechanisms	Setting up governance and compliance mechanisms (e.g., audits by a European Commission in a similar fashion to the banking & finance industry) for the European tech industry based on international standards for IT governance (e.g., COBIT 5[60], ISO/IEC 38500:2015[61]).	Opportunity Driver.	Umbrella.	Legislation. Regulatory. Changes in the marketplace.
7	Increasing adoption of secure national systems through legislation	Making secure national systems mandatory to citizens when system maturity reaches nationally acceptable levels.	Opportunity Driver.	Umbrella.	Competitive position. Legislative.
8	Promoting & encouraging European privacy perspectives	European public awareness and sensitive sentiment towards privacy and security concerns make it a more fertile region for secure and trustworthy ICT initiatives and solutions. European trustworthy ICT solutions can be of use to other regions of the world due to their high privacy sentiment.	Opportunity Driver.	Umbrella.	Society's cultural and political ideology.
9	Increasing trust in the cloud and raising public awareness about cloud technologies	Moving forward with a framework for building trusted clouds in Europe (e.g., Trusted Cloud Europe[62]) and raising public awareness about the benefits and risks associated with use of clouds in general and use of National, European, and non-European clouds in specific. Cloud service providers may introduce user assurances to stimulate initial trust in a similar fashion to zero-liability policy provided by banks for the use of e-banking and m-banking applications.	Opportunity Driver.	Business. Technical.	Sociocultural change.
10	Promoting & encouraging secure thinking from governmental agencies to the private sector	Plugging in private sector services into national IT systems provides an opportunity to promote, encourage and activate best practices implemented in secure national systems in private business organizations.	Opportunity Driver.	Business. Technical.	Business policy change.
11	Technical Standardization	For businesses, technical standardization shifts the basis of competition from tightly-coupled integrated systems to components within the system. This shift is in line with "focus" strategy of Porter's three generic enterprise strategies. Companies offering tightly integrated systems must shift to a modular development approach. The shift to a modularized architecture increases flexibility, and rapid introduction of new products, and the ability to closely meet individual customer needs. The benefits of technical standardization on technology lie in increased interoperability and compatibility among systems. Thus, allowing information to be shared more easily in between differing system components. Users benefit from improved network effects brought in by standardization, such as making use of credentials issued by a certain national IT system in another interoperable national IT system. For business users, increased standardizations brings in the capability to mix and match components of a system to align with their specific needs.	Opportunity. Opportunity Driver.	Business. Technical.	Business policy change. Technical specifications change.
12	Enhancing user privacy protection	Researching, developing and adopting privacy-enhancing technologies (PET) (e.g. Limited disclosure technology, strong encryption). Increasing investment in PETs and offering market incentives to businesses that invest in these technologies. Usability is usually affected by increased privacy protecting, it is important to assure service continuity by minimizing	Opportunity. Opportunity Driver.	Business. Technical.	Business policy change. Research-induced technological change.

[60] http://www.isaca.org/cobit/pages/default.aspx
[61] http://www.iso.org/iso/catalogue_detail.htm?csnumber=62816
[62] http://ec.europa.eu/digital-agenda/en/news/trusted-cloud-europe

		the effects on usability and ease-of use.			
13	Monitoring emerging business models and service delivery models	Monitoring and regulating change in the business landscape stemming from new technologies, or new uses of existing technologies, or new methods of delivering services (e.g., cloud brokering, security-as-a-service, location based services, mobile service channels).	Opportunity. Opportunity Driver.	Business. Umbrella.	Regulatory. Emerging business opportunities.
14	Offering an incentive to small and medium enterprises to adopt national IT systems	The resiliency and agility of SMEs allows for a smoother adoption of national IT systems, but high costs can hinder SMEs ability to enter. Offering incentives to SMEs to adopt national IT systems increases overall system adoption. An example of an incentive is: offering decreased compliance requirements to SMEs as a result of adopting national IT systems, noting that the areas of decreased compliance are naturally compensated by this adoption (i.e. security of identities is managed by government in case it is a government-run national eID systems), this incentive of decreased compliance reflects on lower compliance costs.	Opportunity Driver.	Business. Umbrella.	Business policy change. National IT strategy. Regulation. SME competitive position.
15	Streamlining intra-governmental IT relations and government-private sector interrelations	Building new governmental IT systems provides an opportunity to streamline IT relations among different governmental bodies, and leads to reduced IT autocracy and enhanced service quality. Early partnership among government, private sector service providers and IT sector eases the development of national IT systems. Streamlining interrelated processes among partners simplifies user-business-government interactions, reflecting on improved overall final services.	Opportunity. Opportunity Driver.	Business. Umbrella.	Management. Emerging streamlining opportunities.
16	Making mobile use available for national IT systems	Including mobile channels for national IT systems as optional service delivery models. Mobile channels can ease multifactor authentication hassle to end users by avoiding a separate possession-factor device (i.e. token) where mobile devices can replace physical tokens (e.g. Estonia's MOBIIL-ID[63]).	Opportunity. Opportunity Driver.	Technical. Umbrella.	Business policy change. National IT strategy.
17	Planning for a trusted cloud ecosystem	Monitoring and preparing for the evolvement of trusted clouds into a trusted, legislated, and regulated European cloud ecosystem. Regulations and legislations for a trusted cloud ecosystem include private, public and hybrid clouds, and cloud brokerage.	Opportunity Driver.	Technical. Umbrella.	Regulatory. Sociocultural change.
18	Benefit from single digital market achieved through system interoperability	Cross border citizen, business, and governmental interactions facilitated by system interoperability is a manifestation of the digital single market. Benefits in economical synergy are achieved in a similar fashion to the single physical market.	Opportunity. Opportunity Driver.	Business. User.	Economic change. User behavior.
19	Monetization of personal data	Users have an opportunity to get monetary compensation for the share of their personal data over the web. Social networks and online businesses can benefit from adopting the emerging business model(s) of monetization of personal data. Ease-of-use is a major concern for monetizing personal data due to the diversity of networks, sites and portals where user data is provided. A main portal for managing global settings of monetizing personal data from multiple sources is a possible solution for unifying user control over data residing in various web sources. Data generated by things connected to the Internet of Things (IoT) can also be monetized and requires additional user control over what is shared and who is it shared with (e.g. car providing data to certain car manufacturer, refrigerator providing data to a certain retailer..etc).	Opportunity. Opportunity Driver.	Business. Technical. User.	User's behavior. Additional revenue stream. Technological advancement.

[63] http://www.id.ee/index.php?id=36881

Table 16: Threats for Trustworthy ICT in Europe.

	Threat	Description	Category	Type	Purview
1	Exclusion of end users from early planning stages	Excluding end users feedback at the early stages of a system planning increases the potential for producing a solution that is out of context with current user requirements.	Threat.	Business.	Business policy change.
2	Insufficient demand for trustworthy ICT systems	Implementing systems without demonstrating commercial prospects beforehand runs the risk of developing a product which is not in demand. Demand based business development and increased customer/user focus assure the commercial feasibility of systems.	Threat. Threat Alleviator.	Business.	Business policy
3	Insufficient interest to invest in privacy protection	Insufficient interest to invest in trustworthy ICT and user privacy protection may hinder advances in trustworthy ICT and prevent innovation. Exploring economical market niches where beneficial prospects can be pointed out increases investment attractiveness.	Threat.	Business.	Business policy
4	Incompatibility with existing user context	Introducing innovative IT systems that are out of context with current user behavior or greatly vary from current user-system interaction boundaries run a risk end user unacceptance.	Threat.	Business.	Competitive position. Business policy change.
5	No perceived user need for the technology	User perceptions affect the formation of initial trust, and therefore reflect on adoption levels of trustworthy ICT innovations. As a user related attribute that is external to service providers, perceived user need is influenced by sociocultural and belief considerations, for this reason initial trust can be stimulated by raising awareness and advertising.	Threat.	Business.	Society's economical ideology. Sociocultural change.
6	Rapid deployment of emerging technologies	The right innovation at the wrong time (i.e., too early) reduces the possibility of smooth adoption due to high uncertainty.	Threat.	Business.	Business Policy change. Technological change.
7	Lack of usability	Increased security measures often hinder usability, finding secure solutions that also demonstrate ease-of-use to end users is a challenge to avoid a scenario similar to the current 2-factor-authentication low voluntary adoption.	Threat.	Technical.	Technological change.
8	Lack of data provenance for e-audits	Data integrity is assured through data provenance techniques. e-Audits can only be effective if data provenance is provided to auditing bodies and organizations.	Threat.	Technical.	Technological advancement.
9	Untrustworthy stakeholders	Risks to IT systems arising from untrustworthy contracted parties risk the security of the overall system (e.g.DigiNotar). Assuring national IT system security through contracting trustworthy and accountable stakeholders is an important consideration.	Threat.	Umbrella.	Political (national and European security).
10	Complexity of differing legislation between EU member states on rolling out services across EU	The number of differing national level EU legislations increases the complexity of achieving interoperable and compliant systems across member states.	Threat.	Umbrella.	Legislation. Regulatory.
11	Identity theft	Users run the risk of having their identity (or a number of identifying attributes) compromised through theft.	Threat.	User.	User protection. Legislation.
12	Digital Fraud	Attackers may abuse stolen information and identities online to benefit.	Threat.	User.	User protection. Legislation.
13	Data remanence on decommissioned governmental and non-governmental hardware	Decommissioned hardware introduces the risk of leaking data through remanence. Business practices to assure decommissioned hardware is not re-used elsewhere are necessary to circumvent this threat. Technical solutions to assure remanence is removed from decommissioned hardware increase trust.	Threat. Threat Alleviator.	Business. Technical.	Business policy change. Technical policy change.
14	Rapidly emerging threats, vulnerabilities, and risks.	The fast advancement of ICT technology and finding new uses of existing technologies rapidly introduce new threats. Finding fast-paced "good enough" solutions is becoming a necessity while the concept of state-of-	Threat.	Business. Technical.	Changes in the marketplace.

		the-art "perfect" security is becoming obsolete.			Business Policy change. Technological change.
15	The use of vendor-specific, closed – platform, and closed-standard technologies.	The European Interoperability Framework (EIF) states "*To reach interoperability in the context of Pan-European eGovernment services, guidance needs to focus on open standards*". Open technological standards in this context are opposed to closed-platforms (walled gardens) and standards published under restricted licenses for use and reuse.	Threat.	Business. Technical.	Technological change. Business policy change.
16	Dependence on foreign IT systems and clouds	Current ICT infrastructures in government and industry support foundational elements of modern society (e.g., banking, medicine, transportation, food production, manufacturing…). Increasing dependence on technology increases the risks on foundational elements that in turn maintain the stability of societies.	Threat.	Business. Umbrella.	Political (national and European security).
17	High costs to join trustworthy national IT systems	Imposing a perceived high cost-of-entry for citizens to benefit from secure national IT systems (e.g. Swedish eID) imposes a risk of unacceptance. If there is a need to impose a cost to citizens it should not be higher than the current price levels (e.g. the cost of obtaining an electronic ID card should not be higher than obtaining a normal ID card). These additional costs can be governmentally subsidized. In case a higher fee needs to apply, end users can be compensated to offset the perceived high cost (e.g. adding a transportation bonus to eID cards that are used for public transport) to support adoption.	Threat. Threat Alleviator.	Business. Umbrella.	Society's economical ideology. Macroeconomics. Regulation.
18	Lack of trust towards private service providers and/or government bodies handling citizen data	Cases where there is a lack of trust from citizens towards private sector service providers and/or government bodies handling citizen data run the risk of low adoption or unacceptance of national IT systems. Solutions to overcome this include having a publicly trusted third-party organization (private sector or non-governmental) handle data in a man-in-the-middle fashion while adhering to privacy and limited disclosure principles. Guarantees of trust can be provided in legislation and regulation using both the expressive function of the law (explicitly including trust guarantees in law texts), and the coercive function of the law (enforcing user protecting measures to control threatening behavior and practices). These guarantees in turn lead to positive social perception change, and increased user trust.	Threat. Threat Alleviator.	Business. Umbrella.	Society's cultural and political ideology. Business policy change. Legislation. Regulatory. Political.
19	Long term viability of systems	Developing and adopting national IT systems runs the risk of systems becoming obsolete more rapidly than expected. Exhausting all planning considerations before implementing national systems assures achieving the maximum system lifecycle available at the moment of introduction.	Threat.	Business. Umbrella.	Business policy.
20	Overly offshoring European high-tech industry	Offshoring European high-tech industry solely on cost consideration introduces multiple threats. Foreign security and privacy breaches could be induced on European governmental, business, and user data (confidentiality, trade secrets, identity theft…). Differing process and quality standards could lead to home user dissatisfaction with a service. Internet infrastructure breakdown could affect home users. Loss of jobs hinders European economic growth. Political unrest at destination could affect service-as-usual at home. Currently, the majority of hardware and software used in Europe are produced abroad; this introduces threats of intentional hardware and software bugging for spying programs.	Threat.	Business. Umbrella.	Macroeconomics. Changes in the marketplace. Trends. Regulation.
21	Insufficient and inefficient (ambiguous) regulation and legislation increases risk	Insufficient and inefficient (ambiguous) regulation/legislation introduces the risk of inefficient IT security controls across member states and increases the risk of lack of system interoperability.	Threat.	Technical. Umbrella.	Legislative. Regulatory.
22	Lack of system interoperability across	The lack of national system interoperability with other member states systems introduces the risk of creating	Threat.	Technical.	National and European IT

	member states	system silos in some member states. Where citizens can be excluded from participating in the Digital Single Market in an effective manner.		Umbrella.	strategy. Business policy.
23	Assuring technical security of national IT systems	Expecting breaches and attacks as a certainty of the modern digital space, and planning accordingly. Backdoors should not be left open because they are assumed to be out of reach of attackers (security-by-obscurity). Limited disclosure policies should be implemented in the digital space.	Threat.	Business. Technical. Umbrella.	Political (national and European security). Advancement of capabilities of attackers. Technological change.
24	Failure to comply with national and European IT security regulations	Member state governments run the risk of non-compliance with national and European IT security regulations, bringing in threats that could affect other components of connected European systems.	Threat.	Business. Technical. Umbrella.	Business policy. Regulatory.
25	Loss, corruption, theft or leak of user (citizen, resident, and business) data	Citizen-data handling private organizations and governmental bodies run the risk of loss, corruption, theft, or leak of data. These threats apply to all information systems globally and Europe is no exception. These threats arise from different sources, including foreign governmental hacks, foreign and local hacktivists, insiders from service providers and governmental bodies. Users run the risk of increased local and foreign mass-surveillance often carried out by governmental organizations, or carried out by businesses on behalf of governments or at their own initiative. Mass-surveillance operations could breach the European Data Protection Directive[64] and the European General Data Protection Regulation[65] (proposed).	Threat. Threat Alleviator.	Business. Umbrella. Technical. User.	Business Policy change. Technological change.
26	Outdated and insufficient encryption policies and weak encryption methods	Relying on outdated and insufficient encryption policies and using weak encryption methods for sensitive data (business data, customer data and citizen data) threatens the security of targeted systems. Practices to minimize the risk for leak of clear text or weakly encrypted sensitive data are: adopting upgraded encryption policies for data-at-rest, data-in-use, and data-in-motion (e.g., email encryption, archive encryption). As well as researching and enhancing encryption methods (e.g., homomorphic encryption). And developing robust encryption methods that maintain a sufficiently protected position against increasing computing power (e.g. use of public cloud for brute force decryption, or future quantum computer). Usability is usually affected by increased security measures like Encryption user interfaces. It is important to assure service continuity by minimizing the effects of increased encryption on usability and ease-of use.	Threat. Threat Alleviator.	Technical.	Business policy change. Technical policy change.

[64] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en
[65] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

27	Bottlenecks and single points of failure	Increased adoption of national IT systems by public and private sector organizations introduces the threat for system bottlenecks (e.g. slowdown of a national eID system affects all relying services) and single points of failure (e.g. short term or long term unavailability of a national eID system due to technical limitations or other reasons halts access to all relying services). Technical solutions to assure quality of service (QoS) for national IT systems have to be taken into design and implementation considerations (i.e. assuring the scalability of national IT systems to meet the needs of increased adoption and use while maintaining QoS), including all foreseen and encountered bottlenecks). Technical solutions to assure the high availability of national IT systems are available to be implemented in order to: eliminate single points of failure (i.e. failure of components not leading to failure of system), and utilize reliable crossover (i.e. assuring reliable crossover in multi-threaded systems and robust architectures), and to detect failures as they occur (i.e. backend maintenance of system while front-end is still available). It is recommended for national IT systems to achieve high-end levels of availability (i.e. 99.99%[66] - 99.999%[67]).	Threat. Threat Alleviator.	Technical. User.	Technical policy change.

[66] High availability 99.99%: 52.56 minutes downtime per year, 4.38 minutes downtime per month, 1.01 minutes downtime per week, 8.64 seconds downtime per day.
[67] High availability 99.999%: 5.26 minutes downtime per year, 25.9 seconds downtime per month, 6.05 seconds downtime per week, 0.86 seconds downtime per day.

5.5.2 Importance Ranking

Ranking of opportunities and threats is based on the two voting sessions conducted with the expert panels. Experts were asked to vote on two different occasions, votes were cast for each opportunity and threat. The voting options provided were (High Importance, Medium Importance, Low Importance).

The two following lists include all opportunities and threats ordered according to the highest amount of "High Importance" vote received at the top of each list, followed by the highest "Medium Importance" and finally "low Importance" at the bottom of each list.

5.5.2.1 List of opportunities (ranked):

1. Promoting & encouraging European privacy perspectives
2. Developing and adopting European-level legislations and regulations for trustworthy ICT
3. Increasing trust in the cloud and raising public awareness about cloud technologies
4. Enhancing user privacy protection
5. Making mobile use available for national IT systems
6. Adopting and improving multi-factor authentication for medium and high risk online operations
7. Benefit from single digital market achieved through system interoperability
8. Trustworthy service certification
9. Planning for a trusted cloud ecosystem
10. Technical Standardization
11. Streamlining intra-governmental IT relations and government-private sector interrelations
12. Monetization of personal data
13. Increasing adoption of secure national systems through legislation
14. Offering an incentive to small and medium enterprises to adopt national IT systems
15. Developing and/or adopting European ICT governance and compliance mechanisms
16. Monitoring emerging business models and service delivery models
17. Improving single-factor user authentication mechanisms
18. Promoting & encouraging secure thinking from governmental agencies to the private sector
19. SMEs may increase service traffic and avoid costs by adopting relevant widely-used national IT systems

5.5.2.2 List of threats (ranked):

1. Bottlenecks and single points of failure
2. Exclusion of end users from early planning stages
3. Outdated and insufficient encryption policies and weak encryption methods
4. Overly offshoring European high-tech industry
5. Incompatibility with existing user context
6. Insufficient interest to invest in privacy protection
7. Lack of usability

8. High costs to join trustworthy national IT systems
9. Lack of trust towards private service providers and/or government bodies handling citizen data
10. Long term viability of systems
11. Complexity of differing legislation between EU member states on rolling out services across EU
12. Insufficient interest to invest in privacy protection
13. Identity theft
14. Untrustworthy stakeholders
15. Digital Fraud
16. Insufficient demand for trustworthy ICT systems
17. The use of vendor-specific, closed –platform, and closed-standard technologies.
18. Dependence on foreign IT systems and clouds
19. Insufficient and inefficient (ambiguous) regulation and legislation increases risk
20. Lack of system interoperability across member states
21. Assuring technical security of national IT systems
22. Loss, corruption, theft or leak of user (citizen, resident, and business) data
23. Rapidly emerging threats, vulnerabilities, and risks.
24. Data remanence on decommissioned governmental and non-governmental hardware
25. Rapid deployment of emerging technologies
26. Failure to comply with national and European IT security regulations
27. Lack of data provenance for e-audits

5.5.3 Usefulness Ranking

Expert panel voting results were distributed among three main categories based on affiliation and main areas of expertise, as follows:

1. Domain experts: direct experts in one of the three main pillars of ATTPS.
2. Industry executives: experts with an executive industry career background (from both small and large scale business organizations).
3. Technical research: experts affiliated with non-profit academic research institutions and universities.

Distributing the results from the two voting sessions over these categories shows us importance levels as perceived by the individuals from these backgrounds. And aggregately indicate different views on the importance of each opportunity and threat in between these affiliations and areas of expertise. Table 17 includes the data used for the Usefulness Ranking.

Table 17: Voting results distributed among three areas of affiliation and expertise.

Opportunities & Threats

									Average
High	29	22	29	19	19	11	15	18	20.25
Medium	14	16	14	17	21	29	20	24	19.375
Low	3	8	3	10	6	6	11	4	6.375
Total	**46**	**46**	**46**	**46**	**46**	**46**	**46**	**46**	
Perspective	D. Expert	Tech Research	D. Expert	Industry (Ex)	D. Expert	Industry (Ex)	Tech Research	Industry (Ex)	

Opportunities

									Average
High	9	8	11	8	8	4	8	7	7.875
Medium	7	5	7	7	8	11	7	9	7.625
Low	3	6	1	4	3	4	4	3	3.5
Total	**19**	**19**	**19**	**19**	**19**	**19**	**19**	**19**	
Perspective	D. Expert	Tech Research	D. Expert	Industry (Ex)	D. Expert	Industry (Ex)	Tech Research	Industry (Ex)	

Threats

									Average
High	20	14	18	11	11	7	7	11	13.5
Medium	7	11	7	10	13	18	13	15	11
Low	0	2	2	6	3	2	7	1	3
Total	**27**	**27**	**27**	**27**	**27**	**27**	**27**	**27**	
Perspective	D. Expert	Tech Research	D. Expert	Industry (Ex)	D. Expert	Industry (Ex)	Tech Research	Industry (Ex)	

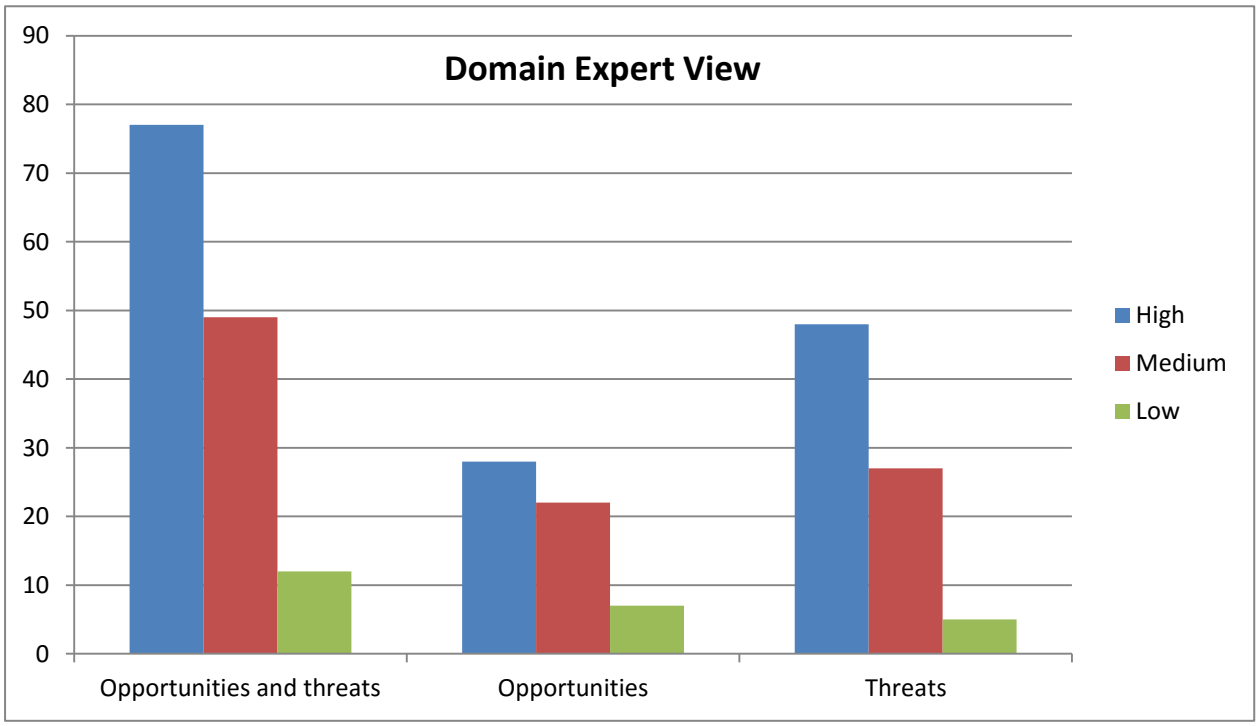


Figure 36: Technical domain subject matter experts' view on Opportunities and Threats

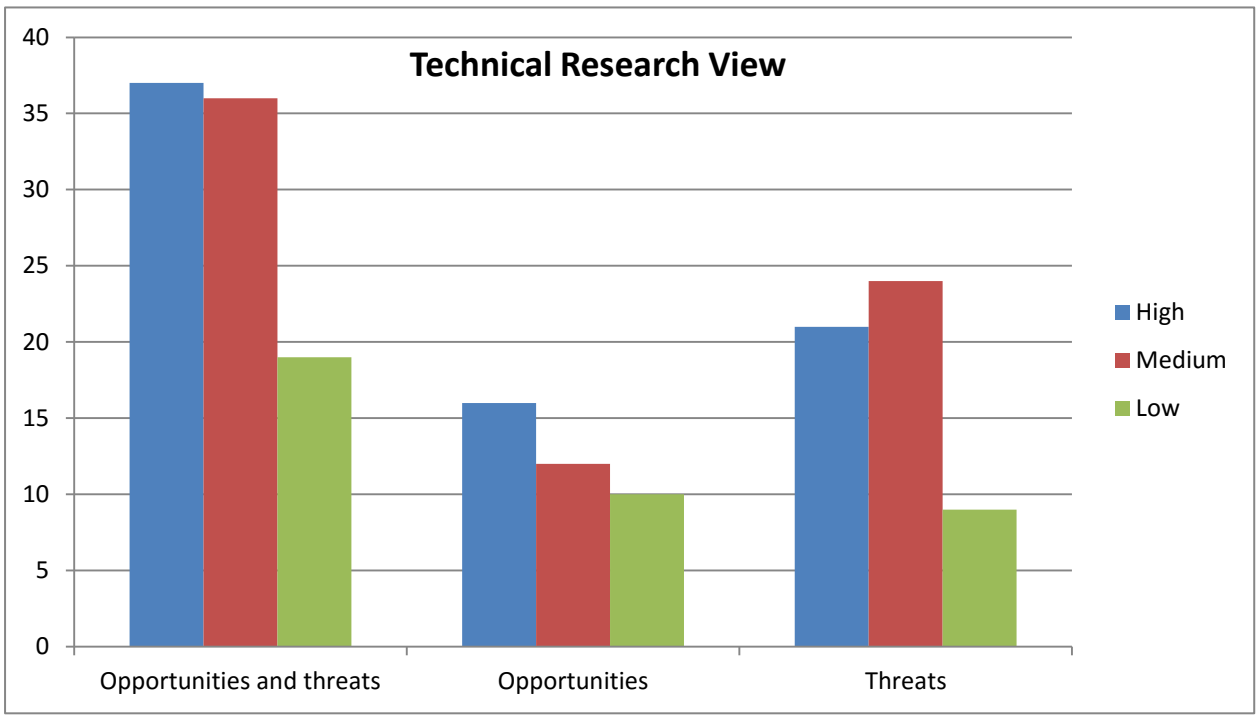


Figure 37: Technical research experts view on Opportunities and Threats

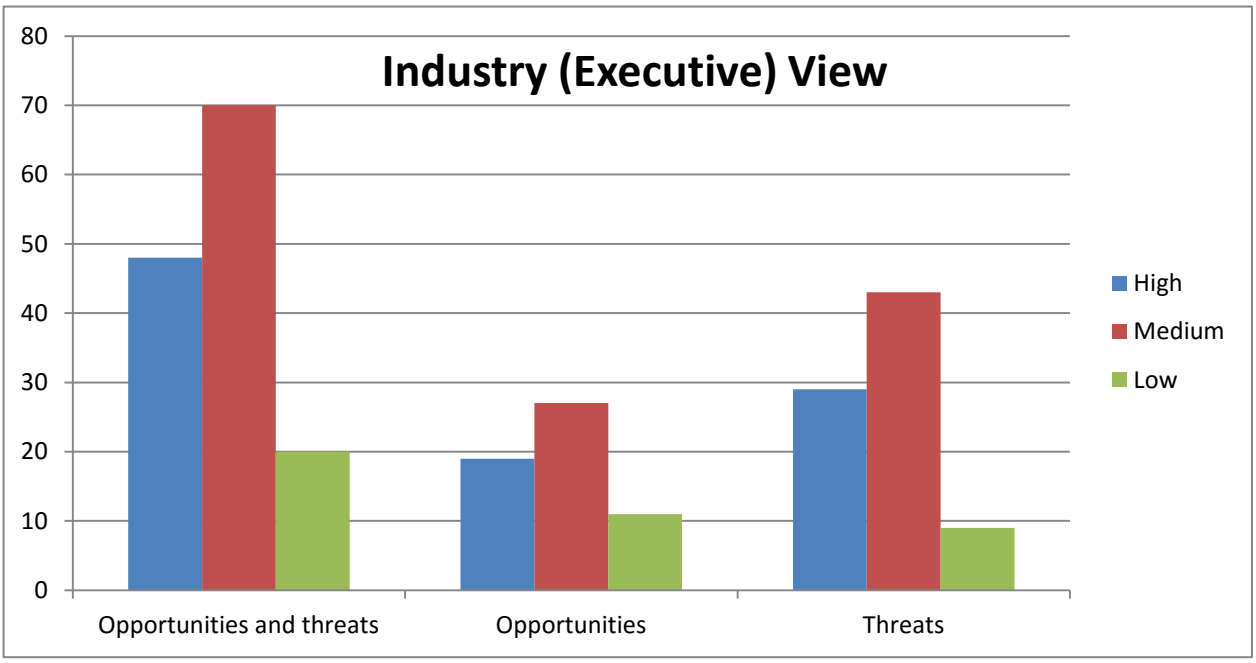


Figure 38: Industry executives' experts view on Opportunities and Threats

6 Conclusion

6.1 6.2 Introduction

The study was set out to monitor early indicators of the trust paradigm shift (T1.2 FP7-ATTPS), as a mean to capture a view of the change of user perceptions towards trustworthy ICT, and their willingness to adopt trustworthy ICT in the future. This has been achieved through qualitative methods (monitoring the web hype in blogs, forums, and discussions, in addition to experts' analysis) as well as quantitative methods (by means of surveys, data mining, adoption degree in prioritized domains, and web traffic measurement & analysis).

Having a rather comprehensive perspective is indispensable for this research matter, as conclusions are aggregative of qualitative and quantitative insights on emerging and maturing industry segments, and hold indicators on a macro-scale. To achieve this view, our work started out by recalling the paradigm shift concept (D1.1 FP7-ATTPS). After which, we researched adoption of innovations and discussed the adoption of preventive innovations, which as argued, is the prevalent adoption model for Trustworthy ICT. Two contextual special cases were reviewed: the U.S. seatbelt adoption case and the web multi-factor authentication adoption case.

Formulating an initial set of research questions the study sought to answer:

1. What are the characteristics of the Trust Paradigm Shift?
2. What are the indicators of the trust paradigm shift?
3. What are the drivers for the adoption of trustworthy ICT, and what is the prevalent adoption model?
4. What is the role of law in the adoption of trustworthy ICT?
5. How do users' perceptions influence the adoption of trustworthy ICT?
6. Are users prepared to "pay" for trustworthy ICT solutions? Does the type of user (e.g., business, individual) influence the preparedness level?
7. What are future threats and opportunities for trustworthy ICT in Europe?

Three fundamental areas were identified as major actors in the current ICT arena, with a focus on trustworthy ICT: Cloud Computing, Personal Data Management, and Identity Management. While capturing views on the dynamics of these industry areas and their characteristics and drivers towards trustworthy ICT in specific, we found in those fields sufficient evidence to build an opportunities and threats assessment. We believe that, due to their pervasiveness in the ICT industry, these fields provide a representation of the current status of the Trust Paradigm Shift in general. We also believe that the results of the opportunities and threats assessment can be fuzzily-generalized to give overall indications of the ICT market in Europe. This work serves as a complementary approach to give a complete assessment together with (D1.1 FP7-ATTPS).

6.2 6.3 Answers to Research Questions

The main empirical findings of this research are research question specific and were discussed within the respective theoretical and discussion chapters. This section will synthesize the answers to our main research questions.

1. What are the characteristics of the Trust Paradigm Shift?

- The Trust Paradigm Shift is certain: the certainty of achieving the Trust Paradigm Shift lies in developing knowledge-based trust, which increases the likelihood of a continued and resilient trust relationship. The certainty of developing knowledge-based trust
- The Trust Paradigm Shift is fuelled by an accelerated rate of adoption: the accelerated rate of adoption emerges from the persistence characteristics of each type of trust, where the nimble erosion of *initial trust* provides for a slow pick up, and the persistency of *knowledge-based trust* provides for an accelerated continuation. Another layer for further acceleration occurs when knowledge-based trust of post-adoptive users fuels the social-psychological initial trust of other potential users through publicity and reputation (e.g., word of mouth, user reviews, and raising awareness) making the rate of change lean towards exponential growth rather than linearity.
- A paradigm shift is loosely-bounded: a change in thought patterns at a macro social scale is a long-running process with loosely-defined boundaries (i.e. "beginning" and "end" of paradigm shift are defined in ranges (e.g. generations) rather than points in time).
- Monitoring the Trust Paradigm Shift is a subjective process: subjectivity arises from user ideas, perceptions and beliefs towards trustworthy ICT. This is observable in social-psychological trust and plays a major role in forming initial trust.

2. What are the indicators of the Trust Paradigm Shift?

To capture early indicators of the Trust Paradigm shift we identified three fundamental areas that play important roles in the current ICT arena:

1. Cloud Computing: a major indicator for the Business-to-Business segment of trustworthy ICT.
2. Personal Data Management: a main indicator of the Business-to-Consumer segment of trustworthy ICT.
3. Identity Management: an emerging ICT field that provides indicators of yet-to-come tendencies in trustworthy ICT.

Early indicators captured and presented for each industry field are:

ICT field	Example of Early Indicator of a paradigm shift
Cloud computing	• Adoption of security standards and compliance with certification bodies • Patents filing facts • Expert's surveys results (e.g. EY, KPMG, and others) • Reports on Cloud Services adoption • Surveys gauging impact of security incidents (e.g. spying programs) • Data storage location proportions • Tendencies in search engines and social media • Experts' opinions
Personal data management	• Web traffic metrics (rankings and bouncing rates) of online security services • Results of surveys gauging public opinions towards trust, privacy and security concerns • Monitoring of evolution of monetization of personal data (adoption, tendencies) as a new way of handling the issue of private data sharing • Expert's opinions
Identity Management	• Adoption of new identity management services • Hot research topics in identity management • Expert's opinions • Limited disclosure technology emergence • Multifactor authentication adoption

3. What is the prevalent adoption model and what are the drivers for adoption of trustworthy ICT?

Trustworthy ICT solutions are preventive innovations by definition: users adopt trustworthy ICT in order to avoid a possible future event that is currently unobservable (e.g. cyber-attack, data leakage, privacy intrusion). For this reason, a suitable adoption model for trustworthy ICT is Moore's Technology Adoption Lifecycle (an adaptation of Roger's bell curve on the diffusion of innovations) illustrated in figure 8.

Trustworthy ICT solutions also share the attributes that affect a customer adoption decision of a preventive innovation. These attributes, as perceived by a potential user, affect their willingness to adopt a solution. When a potential user perceives higher relative advantage, better compatibility, simplicity, and is able to try a solution and observe it's benefits before adopting it they will be more willing to adopt that solution and vice versa.

Following a similar perspective, the empirical evidence of Overstreet et al. (2013) includes three main drivers of adoption of preventive innovations:

1. **Attitude**: personal motivation, personal thinking patterns.
2. **Social Norms**: peer influence and status quo.
3. **Perceived Behavioural control:** of oneself, following the change in status quo.

These drivers are integral to forming initial trust towards a new technology. From another perspective, the Global Technology Adoption Index[68] findings consider security the biggest barrier for expanding mobility technologies, using cloud computing, and leveraging big data. Security concerns are holding organizations back from further investing in major technologies. For this reason an increase in the adoption of trustworthy ICT is an enabler for the adoption of other technologies. This driver for adoption indirectly results in the benefits brought in by these other technologies.

4. What is the role of law in the adoption of trustworthy ICT?

Laws play a two-fold role in increasing the adoption of trustworthy ICT. The expressive function of the law sends a message that sets a normative societal value, taking a first step towards achieving compliance through guilt arising from noncompliance to a concrete obligation. This function allays public fears regarding the security of adopting technological innovations. The coercive function pushes further for compliance through force, where noncompliants face disciplinary action.

5. How do users' perceptions influence the adoption of trustworthy ICT?

Users' perceptions play a major role in forming initial trust, when there are no previous interactions to facilitate the development of experiential trust. Theories that tackle user perceptions categorize these perceptions into Technology Beliefs (TAM): user perceptions towards the technology itself, and Trusting beliefs (Trust): user perceptions towards the provider of the technology. These two sets of beliefs result in developing a user attitude towards the technology and an attitude towards the technology provider. Together, these attitudes are the basis for forming initial trust. Individual perceptions included in the TAM and Trust theories are detailed in section (3.7). The conclusion derived from these theories is that a positive increase in the user perceptions positively affects their technological attitude and trusting attitude, therefore, positively affecting the intention to use or adopt that technology in any of the seven factors.

Deliverable 2.2 (User Experience) of project ATTPS presents qualitative studies to further explore influencing factors of user behavior in the context of usability, security, privacy and trust. The goal of these qualitative studies is to gain further understanding of users' perceptions, views and behavior in this context. In the same deliverable a pilot study performed with real potential users of trustworthy ICT products and services concluded the following results (summarized): [69]

1. The study showed that there are differences in the levels of adoption of trustworthy ICT solutions between users of low, medium, and high knowledge in privacy & security. This level of knowledge in turn affects the level of adoption of trustworthy ICT solutions.
2. The functionality and benefit of trustworthy ICT solutions should be easily understandable by users of high, medium, and low privacy & security knowledge. This is essential to enable adoption across a wide range of potential users.

[68] Dell Global Technology Adoption Index: http://techpageone.dell.com/betterway/tech-hype-meets-tech-reality/
[69] For full study documentation, andlysis and results please refer to deliverable 2.2 (User Experience) of the ATTPS project.

3. The study showed that potential users with high privacy concern were **not** more likely to have adopted security mechanisms, but those with high P&S knowledge were. This observation suggests that influencing users' privacy concerns might not help as much to support the adoption of trustworthy ICT as influencing their knowledge.
4. Privacy & security in trustworthy ICT solutions can influence potential users' adoption decision, when visible and comparable to competing offers. However, in this study no conditions were presented where the price for the trustworthy ICT solutions differed. The observed effect might change as soon as a privacy-intrusive offer is cheaper than a non-intrusive offer.
5. Against researcher expectations, the privacy protection offered by the "Egofy" system was not the main benefit which the users perceived. Factors related to efficiency and rewards were named most often as the benefit. Users still raised concerns regarding privacy, data protection and security, even though security and privacy and the fundamental pillars of this system.

6. What are future threats and opportunities for trustworthy ICT in Europe?

Answer to this research question in section 5.3.

6.3 6.4 Sustainability of ATTPS Project Elements

As a research and development supporting activity project, ATTPS resulted in a number of business models and events to be considered for future continuity. The Generic Trust Architecture Center (GTAC) is a rich download center of trustworthy ICT architecture components and related trustworthy ICT research results. GTAC is being prepared by ATTPS and will continute post ATTPS as part of the Trust in Digital Life Association (TDL). COSTAR is an initiative to protect the security of SMEs by providing cybersecurity services, monitoring and assistance, and training. COSTAR will continue as an independent entity. ATTPS Winter School on Security and Privacy (CySeP) is currently in consideration for future continuation of the event through support by TDL. The European ICT Project Survey conducted by the ATTPS Survey Coordinator is currently under consideration for future continuity of the questionnaire, analysis, and reporting to the European Commission.

Bibliography

4 safety tips for using Wi-Fi. (2014, 05. 26). Retrieved from Microsoft Safety and Security Center: http://www.microsoft.com/en-gb/security/online-privacy/public-wireless.aspx

Acquisti, A., John, L. K., & Loewenstein, G. (2009). What is privacy worth? *Proceedings of the 21st Workshop on Information Systems and Economics (WISE).*

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42(12)*, 40-46.

Bargas-Avila, J. A., & Hornbæk, K. (2011). Old wine in new bottles or novel challenges: a critical analysis of empirical studies of user experience. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2689-2698). ACM.

Benamati, J., Fuller, M., Serva, M., & Baroudi, J. (2010). Clarifying the Integration of Trust and TAM in E-Commerce Environments: Implications for Systems Design and Management. *IEEE Transactions on Engineering Management, 57*(3), 380-393.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011). On the need for different security methods on mobile phones. *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 465-473). ACM.

Beresford, A. R., Kübler, D., & Preibusch, S. (2012). Unwillingness to pay for privacy: A field experiment. *Economics Letters, 117(1)*, 25-27.

Berkley, R., Jamous, H., & Ozokan, D. (2013). A Heuristic Mathematical Decision Support Model for SMEs Cloud ERP System Adoptability. (W. A. van den Heuvel, Ed.) *Proceedings of the 2013/14 course on Advanced Resource Planning at Tilburg University*.

Bernstein, G. (2007). The Role of Diffusion Charecteristics in Formulating a General Theory of Law and Technology. *8*(2), 623-644.

Boulton, D. W. (1996-2001). *Understanding the Strategic Analysis Model.* Auburn University.

Chellapa, R. K. (2008). Consumers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, 358-368.

Chia-Chien Hsu, B. A. (2007). The Delphi Technique: Making Sense of Consensus. *Practical Assesement, Research & Evaluation, 12*(10).

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 1). ACM.

Chute, C. (2014). *Regional 2014 SMB Cloud Storage Adoption Survey: From Point Solution to Platform.* IDC.

Coman, A. a. (2009). Focused SWOT: diagnosing critical setrenghts and weaknesses. *International Journal of Production Research, 40*(20), 5677-5689.

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use.* O'Reilly Media, Inc.

Crumrine, J., & Deb, S. (2014). *Corporate Cloud Computing Trends: A Look at Public, Private and Hybrid Cloud Demand.* 451 Research. ChangeWave Research.

Data Privacy Day. (2014, 05. 26). Retrieved from http://www.staysafeonline.org/data-privacy-day/privacy-tips/mobile

David, F. R. (2005). *Strategic Management: Concepts and Cases.* Prentice Hall.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

DeWitt, A. J., & Kuljis, J. (2006). Aligning usability and security: a usability study of Polaris. *Proceedings of the second symposium on Usable privacy and security* (pp. 1-7). ACM.

Dimitriadis, S., & Kyrezis, N. (2010). Linking Trust to Use Intention for Technology-Enabled Bank Channels: The Role. *Psychology & Marketing, 27*(8), 799-820.

Dörflinger, T., Voth, A., Kramer, J., & Fromm, R. (2010). “My smartphone is a safe!” The user's point of view regarding novel authentication methods and gradual security levels on smartphones. *Proceedings of the 2010 International Conference on Security and Cryptography* (pp. 1-10). IEEE.

DoW. (2012). ATTPS Description of Work.

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074). ACM.

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There’s a price for that. *The Economics of Information Security and Privacy*, 211-236.

Felt, A. P., Egelman, S., & Wagner, D. (2012). I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 33-44). ACM.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 3). ACM.

Fiore, U., Palmieri, F., Castiglione, A., Loia, V., & De Santis, A. (2014). Multimedia-based battery drain attacks for Android devices. *Consumer Communications and Networking Conference (CCNC)* (pp. 145-150). IEEE.

Garfinkel, S., & Lipford, H. R. (2014). *Usable Security: History, Themes, and Challenges.* Synthesis Lectures on Information Security, Privacy, and Trust, 5(2).

Greenstein, S. (2014). The Economics of Information Security and Privacy. *Journal of Economic Literature, 52(4)*, 1177-1178.

Gross, J. B., & Rosson, M. B. (2005). Looking for trouble: understanding end-user security management. *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology* (p. 10). ACM.

Hallinan, D., & Friedewald, M. (2012, 4th Q.). Piblic Perception of the Data Environment and Information Transactions: a selected survey analysis of the European public's views on the data environment and data transactions. *Digiworld Economic Journal, 88*, 61.

Han, B., & Windsor, J. (2014). USER'S ADOPTION OF FREE THIRD-PARTY SECURITY APPS. *Journal of Computer Information Systems, 54(3)*.

Harper, S., Strumpf, E., Burris, S., Smith, G., & Lynch, J. (2014). The Effect of Mandatory Seatbelt Laws on Seat Belt Use by Socioeconomic Position. *Journal of Policy Analysis and Management, 27*(8), 141-161.

Harvard Business Review. (2015). *Harvard Business Essentials: Strategy: Create and Implement the Best Strategy for Your Business* . Harvard Business School Press.

Hassenzahl, M. (2010). Experience design: Technology for all the right reasons. *Synthesis Lectures on Human-Centered Informatics, 3(1)*, 1-95.

Hassenzahl, M., Diefenbach, S., & Göritz, A. (2010). Needs, affect, and interactive products–Facets of user experience. *Interacting with computers, 22(5)*, 353-362.

Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144). ACM.

Hogben, G., & Dekker, M. (2010). *Smartphones: Information security risks, opportunities and recommendations for users. .* European Network and Information Security Agency, 710(01).

How to Make Smart Wireless Choices and Avoid Problems. (2014, 05. 26). Retrieved from Consumer Action: http://www.consumer-action.org/english/ articles/cell_phone_ savvy_training_manual/#protect-info

Jentzsch, N., Preibusch, S., & Harasser, A. (2012). *Study on monetising privacy: An economic model for pricing personal information.* ENISA.

Johnson, G. S. (2008). *Exploring Corporate Strategy.* Prentice Hall.

Kim, S., & Malhotra, N. (2005). Predicting System Usage from Intention and Past Use: Scale Issues in the Predictors. *Decision Sciences, 36*(1), 187-196.

Kraus, L., Fiebig, T., Miruchna, V., Möller, S., & Shabtai, A. (2015). Analyzing End-Users' Knowledge and Feelings Surrounding Smartphone Security and Privacy. *Proceedings of the Workshop on Mobile Security Technologies (MoST).*

Kraus, L., Hirsch, T., Wechsung, I., Poikela, M., & Möller, S. (2014). Poster: Towards an Instrument to Measure Everyday Privacy and Security Knowledge. *Symposium On Usable Privacy and Security (SOUPS).*

Kraus, L., Wechsung, I., & Möller, S. (2014). A Comparison of Privacy and Security Knowledge and Privacy Concern as Influencing Factors for Mobile Protection Behavior. *Workshop on Privacy Personas and Segmentation, Symposium On Usable Privacy and Security (SOUPS).*

Kraus, L., Wechsung, I., & Möller, S. (2014). Using Statistical Information to Communicate Android Permission Risks to Users. *Proceedings of the 4th Workshop on Socio-Technical Aspects in Security and Trust (STAST)* (pp. 48-55). IEEE.

Lewicki, R., & Bunker, B. (1996). Developing and Maintaining Trust in Work Relationships. (R. K. Tyler, Ed.) *Trust in Organizations: Frontiers of Theory and Research*, 114-139.

Lippert, S. (2007). Assessing post-adoption utilisation of information technology within a supply chain management context. *International Journal of Technology and Management, 7*(1), 36-59.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15(4)*, 336-355.

Mannheim, K. (1952 - first published 1923). The Problem of Generations. *Journal of Social Issues, 30*(3).

Marshall, C., & Rossman, G. B. (2010). *Designing qualitative research.* Sage publications.

McKnight, D. H. (2005). Trust in Information Technology. (G. B. Davis, Ed.) *The Blackwell Encyclopedia of Management - Management Information Systems, 7*, 329-331.

Mohr, J., Sengupta, S., & Slater, S. (2005). *Marketing of High-Technology Products and Innovations (2nd ed.).* Upper Saddle River, New Jersey: Pearson Education International.

Möller, S. (2005). *Quality of telephone-based spoken dialogue systems.* Springer Science & Business Media.

Moore, G. (1999). *Crossing the chasm: marketing and selling high-tech products to mainstream customers* (Rev. ed.). New York: Harper Business.

Moses, L. B. (2005). Understanding Legal Responses to Technological Change of In Vitro Fertilization. *MINN. J.L. SCI. & TECH., 6*(2), 506-617.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security (34)*, 47-66.

Mylonas, A., Theoharidou, M., & Gritzalis, D. (2013). Assessing privacy risks in Android: A user-centric approach. *Proceedings of the 1st international workshop on risk assessment and risk-driven testing (RISK),* (pp. 21-37). Springer International Publishing.

Nielsen, J., & Molich, R. (1990). Heuristic evaluation of user interfaces. . *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 249-256). ACM.

Norman, D. A. (2002). *The design of everyday things.* Basic books.

Overstreet, R., Cegielski, C., & Hall, D. (2013). Predictors of the intent to adopt preventive innovations: a meta-analysis. *Journal of Applied Social Psychology, 43*(5), 936-946.

Park, Y. J. (2011). Digital literacy and privacy behavior online. . *Communication Research*.

Paul, D., & MsDaniel, R. (2002). A field study of the effect of interpersonal trust on virtual collaborative relationship performance. *MIS Quarterly, 28*(2), 183-227.

Pavlou, P. (2003). Comcumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce, 7*(3), 69-103.

Pavlou, P. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of electrponic Commerce, 7*(3), 101-134.

Peraza, Y., & Zwakman, G. (2013). *Cloud Computing Overview Report 2013.* 451 Market Monitor.

Pickton D.W., W. S. (1998). What's SWOT in Strategic Analysis? *Strategic Change*(Vol. 7), 101-109, 105-106.

Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies, 71(12)*, 1133-1143.

Rogers, E. (2002). Diffusion of Preventive Innovations. *Addictive Behaviours, 27*(6), 989-993.

Rogers, E. (2003). *Diffusion of Innovations (5th ed.).* New York: New York Free Press.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American psychologist, 55(1)*, 68.

Sarma, A., Velthausz, D., & Leijtens, A. (2012). Strategic Research Agenda. 9.

Shabtai, A., Fledel, & U. Kanonov, Y. E. (n.d.).

Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., & Dolev, S. (2009). *Google android: A state-of-the-art review of security mechanisms. .* arXiv preprint arXiv:0912.5101.

Sheldon, K. M., Elliot, A. J., Kim, Y., & Kasser, T. (2001). What is satisfying about satisfying events? Testing 10 candidate psychological needs. . *Journal of personality and social psychology, 80(2)*, 325.

Shin, D. (2010). The Effects of Trust, Security and Privacy in Social Networking: A Security-based Approach to understand the pattern of adoption. *Interacting with Computers, 22*(5), 428-438.

Ståhlbröst, A. (2008). *Forming future IT: the living lab way of user involvement.* PhD Thesis 2008:62, Lulea University, Lulea, Sweden, 2008.

Thatcher, J., McKnight, D., Baker, E., & Arsal, R. (2011). The role of trust in postadoption exploration: An empirical investigation of knowledge management systems. *IEEE Transactions on Engineering Management, 58*(1), 56-70.

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013). QRishing: The susceptibility of smartphone users to QR code phishing attacks. *Financial Cryptography and Data Security* (pp. 52-69). Springer Berlin Heidelberg.

Vredenburg, K., Mao, J. Y., Smith, P. W., & Carey, T. (2002). A survey of user-centered design practice. *Proceedings of the SIGCHI conference on Human factors in computing systems: Changing our world, changing ourselves* (pp. 471-478). ACM.

Wash, R. (2010). Folk models of home computer security. *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 11). ACM.

Whitten, A., & Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. . *Usenix Security .*

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43(3)*, 389-418.

Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional Role of Trust in Internet Banking Adoption. *The Service Industries Journal, 29*(5), 591-605.