D.3.1 TECHNOLOGY AND STANDARD REPORT

Authors:
Zoltán Hornák, István Nyilas, Dániel Petró (SEARCH-LAB Ltd)
Johann Schrammel, Peter Wolkerstorfer, Lars Ellensohn, Arjan Geven, Katrin Kristjansdottir
(CURE - Center for Usability Research and Engineering); Lothar Fritsch, Trenton Schultz, Habtamu Abie (Norsk Regnesentral – Norwegian Computing Center); Franziska Pürzel, Volker Wittstock
(Chemnitz University of Technology)

Version: 1.0
Date: 01/12/2010
Dissemination level: (PU, PP, RE, CO): PU

Project Co-Funded by the European Commission within the 7th Framework Programme
Abstract

“Where large sums of money are concerned, it is advisable to trust nobody.”

Agatha Christie

This document is primarily for internal use and its main objective is to help matching uTRUSTit goals with current and foreseeable technologies of relevance. Starting with a summary on the Internet of Things and Trust definitions, the document comes to an overview on the four main technological topics uTRUSTit builds on: accessibility, virtual reality, and security. This compilation also has a secondary objective: it is to form a useful technical knowledge-base which – amongst consortium partners – fosters a better understanding of the technologies as building blocks behind uTRUSTit, and provides initial input to the subsequent technical tasks and deliverables.

Before any constructive work is done, the first step must be to determine the key entities in scope, and to reach a common understanding of their meaning and characteristics. In the definition chapters, multiple existing descriptions are examined for the Internet of Things and Trust to provide a basis for reasoning out the most suitable definitions for uTRUSTit.

Virtual Reality helps in visualizing the uTRUSTit use case scenarios, enabling VR-based tests and measuring using real people, without having to build the whole scenario in real world beforehand. While it is an obvious goal to minimize the difference in user perception between VR and reality, it is important to make the “error” it entails measurable and predictable.

Accessibility guidelines play a key role when it comes to gaining and maintaining trust amongst users with disabilities. Being closely related to usability, it is one of the important goals that the project steers towards. The chapter dealing with accessibility in this document enlists different standards to align to achieve accessibility in uTRUSTit deliverables.

Security (and privacy) is another pillar that the project builds upon. Yet in the definition chapters a short study reveals the links between trust, security and risk, emphasizing the importance of balancing effective security of the system with the user’s trust in it to avoid lack of acceptance and thus business loss. Later a separate chapter deals comprehensively with common practices to gain trust and to raise security awareness, while a summary reviews typical solutions to achieve effective security and data privacy in a system.

The document finally concludes with emphasizing the importance of clarification of definitions as a substantial element in the assessment of uTRUSTit requirements and scenarios. It is not supposed however to deduce perfect matches between existing solutions and project goals, but to provide an overview on the recent alternatives, and offer valuable hints to compile project requirements, tests and scenarios.
# Table of Contents

D.3.1 TECHNOLOGY AND STANDARD REPORT .................................................................................................................. 1

1. **INTRODUCTION** ....................................................................................................................................................... 5

1.1 Background ................................................................................................................................................................. 5
1.2 Scope of this Deliverable ............................................................................................................................................... 5
1.3 The Internet of Things .................................................................................................................................................. 6
1.4 Definitions of the IoT in uTRUSTit .............................................................................................................................. 7
1.5 Internet of Things in uTRUSTit ................................................................................................................................ 8

2. **“TRUST” AND TECHNOLOGY IN THE CONTEXT OF THE INTERNET OF THINGS** .............................................. 9

2.1 Different definitions of trust in the IoT ........................................................................................................................ 9

2.1.1 Scope of Trust Definitions ........................................................................................................................................ 9

2.1.1.1 Trust between machines .................................................................................................................................. 9

2.1.1.2 Functions of machine-to-machine trust ............................................................................................................. 10

2.1.2 Technical Trust Definitions ................................................................................................................................... 10

2.1.2.1 TC-ErG/A Study ................................................................................................................................................ 10

2.1.2.2 Trusted Computing Group ............................................................................................................................... 10

2.1.3 Definitions used by the research funding bodies .................................................................................................. 11

2.1.3.1 EU FP7 ICT Research Work Program ............................................................................................................ 11

2.1.3.2 Norwegian Research Council VERDIKT program ......................................................................................... 11

2.1.4 Summary ................................................................................................................................................................. 12

2.2 Level of trust, security and risk .................................................................................................................................. 12

2.2.1 Level of trust ......................................................................................................................................................... 12

2.2.2 Level of Information Technology security ............................................................................................................ 13

2.2.3 Level of risk as a measure of security .................................................................................................................... 14

2.3 Balancing the user’s trust and security ...................................................................................................................... 14

2.3.1 Raising security awareness ................................................................................................................................... 16

2.3.2 Building trust ........................................................................................................................................................ 16

2.3.3 Balancing stakeholder interests from design into security specifications .............................................................. 17

2.3.3.1 Approaches to security and privacy engineering ............................................................................................ 17

2.4 Summary and conclusion .......................................................................................................................................... 17

3. **TRUST AND THE USER IN THE INTERNET OF THINGS** .......................................................................................... 21

3.1 Trust and the User in the Internet of Things ............................................................................................................... 21

3.1.1 Problems facing the IoT .......................................................................................................................................... 21

3.1.2 Privacy problems in IoT .......................................................................................................................................... 22

3.1.3 Who trusts who? ...................................................................................................................................................... 22

3.1.4 The individual trusting in the machine .................................................................................................................... 23

3.1.5 Things trusting in people ....................................................................................................................................... 24

3.1.6 Battling the trust in the IoT .................................................................................................................................... 24

3.1.7 Increasing awareness .............................................................................................................................................. 24

3.1.8 Maintaining an audit trail ....................................................................................................................................... 25

3.1.9 Conclusion ............................................................................................................................................................. 25

3.1.10 Security and the user in internet of things ............................................................................................................ 25

3.1.11 The user “The Weakest link” .............................................................................................................................. 25

3.1.12 “What does this mean?” ..................................................................................................................................... 26

3.1.13 “This is in my way” ............................................................................................................................................. 26

3.1.14 “It will not happen to me” ................................................................................................................................... 26

3.1.15 Mental Models ...................................................................................................................................................... 27
6.2.5 Capability .................................................. 29
3.2.6 Other Current Standards ............................................. 29
3.3 Summary and Conclusion .................................................. 29
4. VIRTUAL REALITY IN THE IOT ........................................ 30
4.1 Current technologies and best practices .................................. 30
4.1.1 Modeling .................................................... 31
4.1.2 Simulation ................................................... 31
4.1.3 Interaction .................................................... 31
4.2 Approaches in uTRUSTit ................................................ 32
4.2.1 Simulation/Visualization .......................................... 32
4.2.2 Interaction .................................................... 32
4.2.3 Testing ......................................................... 33
4.3 Summary and Conclusion ................................................ 33
5. ACCESSIBILITY IN THE IOT ........................................... 35
5.1 Standards and Technologies ............................................... 35
6. SECURITY AND PRIVACY IN THE IOT .............................. 38
6.1.1 Adaptive, Autonomic and Evolving Security ...................... 40
6.1.2 Dynamic/Adaptive Security Policies ............................... 41
6.2 Current technologies and best practices for achieving security and privacy .......... 43
6.2.1 Firewall and Intrusion Detection Systems ......................... 43
6.2.2 Virtual Private Networks ......................................... 44
6.2.3 Digital Rights Management (DRM) ................................ 45
6.2.4 Privacy Impact Assessment (PIA) ................................ 47
6.2.5 Privacy enhancing technology (PET) ................................ 47
6.2.5.1 Technology for protection of privacy - a brief history .......... 48
6.2.5.2 Overview of Privacy Enhancing Technology .................. 49
6.2.6 Privacy-respecting Identity Management ......................... 53
6.2.7 RFID privacy and data protection guidelines (e.g. COM/2009/3200) ............... 57
6.2.8 Privacy by Design principles ....................................... 58
6.3 Current technologies and best practices to gain user trust ..................... 59
6.3.1 User feedback .................................................. 59
6.3.2 Certifications ................................................... 68
6.3.3 Trust chaining mechanisms .......................................... 69
6.4 Summary and Conclusion ................................................ 70
7. GENERAL SUMMARY .................................................. 71
8. INDEX ............................................................................. 71
9. REFERENCES ..................................................................... 73
1. Introduction

1.1 Background

The main goal of the uTRUSTit project is to do constructive work on the field of trust between the IoT and its user. Trust in this context is mostly psychological: enabling the user to feel control, security and privacy when using such a smart environment. This does not necessarily refer to gaining trust by all means – as the above quote suggests, there are cases when our task is just the contrary: to learn how to ruin an unduly high level of trust in an insecure service leading to careless and misjudging behavior, exposing the user to attacks. As results of uTRUSTit, not only a feedback toolkit application will help users understand the underlying technical processes and information flow in a smart home or a smart office environment, but also new design guidelines will enable developers constructing ICT systems with a brighter view on user perceptions and trust.

This document is the resulting deliverable of T3.1 Technology and Standards Analysis, providing an overview on the technologies and practices that are serving as a basis of the project’s goals. Recent practices, publications and current standards are also tackled where relevant so that the results fit into the continuously evolving and changing environment of the industry and market.

1.2 Scope of this Deliverable

The Technology and Standards Report is an initial study, compiling the technologies and competences of relevance that the consortium brings to the project – on one hand – while on the other hand it uncovers current and foreseen practices of the kind.

This document is a prerequisite for further development work within uTRUSTit. It will be a direct input to the following deliverables:

- D3.3 Security Specification for the IoT
- D2.2 Definition of User Scenarios
- D2.5 Requirements for the Trust Feedback and Support Toolkit for the Three Scenarios
- D2.6 Design Guidelines on the Security Feedback Provided by the “Things”

Additionally, this document will indirectly assist to all WPs within the project by providing an overall knowledge-base over the technologies to be used, fostering constructive collaboration between the project partners.
1.3 The Internet of Things

The meaning of things lies not in the things themselves, but in our attitude towards them.

_Antoine de Saint-Exupéry_

Before any work is done, proper definitions are needed for the entities that the project will deal with. The first such is the _Internet of Things_. As today it is chiefly a concept than is to be evolved and implemented in everyday usage in the future, definitions and use-cases are also going through a continuous change. This is where we need to set fix points, which suit best uTRUSTit aims.

The Internet of Things has been defined by the CERP-IoT project (http://ec.europa.eu/information_society/events/shanghai2010/pdf/cerp_iot_clusterbook_2009.pdf). They define the IoT as follows:

“The Internet of Things is an integrated part of Future Internet and could be defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, virtual personalities, and use intelligent interfaces, and are seamlessly integrated into the information network”.

The vision of Future Internet based on standard communication protocols considers the merging of computer networks, Internet of Media (IoM), Internet of Services (IoS), and Internet of Things (IoT) into a common global IT platform of seamless networks and networked “things”. This future network of networks will be laid out as public/private infrastructures and dynamically extended and improved by terminals created by the “things” connecting to one another.

We envisage that the IoT will allow people and things to be connected Anytime, Anyplace, with Anything and Anyone, ideally using Any path/network and Any service. The concept of IoT can be regarded as an extension of the existing interaction between humans and applications through the new dimension of “Things” communication and integration. The main identified IoT application domains are:

- Aerospace and aviation,
- Automotive,
- Telecommunications,
- Intelligent Buildings,
- Medical Technology, Healthcare,
- Independent Living,
- Pharmaceutical,
- Retail, Logistics, Supply Chain Management,
- Manufacturing, Product Lifecycle Management,
- Oil and Gas
- Safety, Security and Privacy,
- Environment Monitoring,
- People and Goods Transportation,
- Food traceability,
- Agriculture and Breeding,
- Media, entertainment and Ticketing,
- Insurance,
- Recycling.
The main IoT technologies allow identifying the research and development challenges and outlining a roadmap for future research activities to provide practical and reliable solutions. This roadmap forms the basis for the research priorities presented and these IoT enabling technologies are:

- Identification Technology,
- Internet of Things Architecture Technology,
- Communication Technology,
- Network Technology,
- Network Discovery,
- Software and algorithms,
- Hardware,
- Data and Signal Processing Technology,
- Discovery and Search Engine Technologies,
- Relationship Network Management Technologies,
- Power and Energy Storage Technologies,
- Security and Privacy Technologies,
- Standardization.

1.4 Definitions of the IoT

As we will also see at the definitions of trust (see Section 2.1), the Internet of Things (IoT) is also a term with multiple definitions. For example, the Summary of EU Legislation website gives the following definition.

IoT is composed of a series of new independent systems operating with their own infrastructures which are partly based on existing Internet infrastructures. IoT can be implemented in symbiosis with new services. It covers three types of communication which can be established in restricted areas (“Intranet of things”) or made publicly accessible (“Internet of things”):

- things-to-person;
- thing-to-thing;
- Machine-to-Machine (M2M).

IoT currently covers several applications such as:

- web-enabled mobile phones equipped with cameras;
- unique serial numbers or bar-codes on pharmaceutical products;
- smart electrical metering systems which provide a consumption report in real time;
- “Intelligent objects” in the logistics sector (eFreight), manufacturing or retail.

(From: http://europa.eu/legislation_summaries/research_innovation/research_in_support_of_other_policies/si0009_en.htm)

The United Nations agency for information and communications technology (ITU) provides a different definition:

Today, developments are rapidly under way to take this phenomenon an important step further, by embedding short-range mobile transceivers into a wide array of additional gadgets and everyday items, enabling new forms of communication between people and things, and between things themselves. A new dimension has been added to the world of information and communication technologies (ICTs): from anytime, anyplace connectivity for anyone, we will now have connectivity for anything.

The vision of IoT will make it easy to access data and easy to aggregate and correlate data from numerous different sources of things. While this makes life-easier for law-abiding citizens, it might facilitate misuse and the violation of individuals’ privacy. The advent of more complex IoT services that involve multiple service providers further exacerbates the privacy concerns as it raises the potential of personal information being shared across these providers in ways that weren't intended by and consented with the owner of the information. The primarily focus of IoT solutions must thus be on privacy preservation in the context of such complex IoT services that involve multiple IoT service providers.

### 1.5 Internet of Things in uTRUSTit

The above sections have shown the manifold understanding and versatility of the IoT concept. Now efforts have to be put to form the uTRUSTit perspective and understanding on IoT. This document will only contain our preliminary expectations from the IoT we work with at this early stage. This initial approach should be common and flexible, but it must already have the most important aspects that uTRUSTit aims to build upon. After these, the uTRUSTit definitions for thing and Internet of Things are as follows:

**Thing:** A real or virtual object (or service, like a web service).

**Internet of Things:** The Internet of Things (IoT) is a group of things that communicate with each other and occasionally over infrastructure (other networks, Internet, etc.).

As the basic definitions evolve through time (e.g. in the requirements and scenarios assessment phase), the above simple, abstract and flexible sentences mature and multiply, creating a solid basis to rely on.
2. “Trust” and Technology in the context of the Internet of Things

If we said in the last section that IoT definition is manifold, this is even more so in the case of trust. To approach our own definition of trust that is to be used in uTRUSTit, an appropriate start-up is reviewing different understandings of trust, along with other terms which are in close relation to it.

2.1 Different definitions of trust in the IoT

Trust in our common understanding is a human feeling that affects our decisions, our behavior. When trust is present, we feel comfortable in the current situation and are more willing to act as required or provide sensitive information about us. Lack of trust causes the feeling of insecurity or danger, entailing retraction, refusal to proceed as a consequence.

There are attributes which we assign to the notion of trust:
- A subject: one may feel trust relating to another person, a company, a government, a device or a service;
- A measure: one can find a limit up to which one trusts (e.g. the amount of money we lend to someone without the doubt that we will get it back soon)

Trust can be understood as a measure of the feeling of security. In this context, security is also introduced – as a relating technical term it refers to the attack potential that a system can resist. It therefore can be interpreted as the required preparedness of the attacker, the available time and resources to perform an attack and finally the probability of a successful attack.

The third factor is risk, calculated as the product of attack probability and the damage it can cause. Risk is a key factor when assessing our rate of exposition to threats and helps in mitigating the most serious threats. The higher risk is perceived (regardless whether it is real or imaginary), the less trust is present.

Over the time the notion of trust has been enriched by multiple interpretations. Below are summarized those that to some extent relates to the technical focus of uTRUSTit.

2.1.1 Scope of Trust Definitions

This section features multiple scopes of trust definitions. First, machine-to-machine trust is tackled via examples, then it shows relevant instances of technical trust definitions, which already includes human perceptions. Finally it deals with definitions used by the research funding bodies. Without the need of exhaustiveness, it therefore covers different scopes that are to some extent relevant to uTRUSTit and provide a basis for further clarification of the project’s own approach.

2.1.1.1 Trust between machines

Examples for trust functions between machines
- Digital Rights Management
- Remote attestation
- Trusted Platforms
- Certification
- PKI
2.1.1.2 Functions of machine-to-machine trust

- Build secure federations of devices
- Check that the other machine/service is „real“
  - Belongs to where it claims
  - Fulfills function it claims
  - Keeps expected security levels

2.1.2 Technical Trust Definitions

In the following subsections, we quote the trust definitions from a couple of groups of security groups that have attempted to define trust. One is Sirrix AG, a security company in Germany. Sirrix AG ran a study to find different ways that trust models and security concepts could be used in computer systems. The other definition comes from the Trusted Computing Group, an international organization whose works on specifications that are then published to the industry.

2.1.2.1 TC-ErG/A Study

The following is a quote from the TC-ErG/A study on trust. The report was originally published in German; this is a translation into English.

Trust is a frequently-used term in the security business. Unfortunately, trust in people is as frequently confused with trust in security models or systems. When IT security people discuss trust, they consider it in technical systems. For example, the trust that an automatic update of virus definitions by an anti-virus program will include meaningful and useful virus definitions rather than sabotage the anti-virus tool. One usually assumes that the vendor of the anti-virus software has enough incentive to develop business where security in the program is a high priority. Hence, the anti-virus trust model requires the assumption that the update server is trustworthy because the vendor wants his business to survive. Trust in people is a problematic perspective. Usually one must trust people despite this. They can always talk, photograph screens, steal printouts or manually enter data into a different system. Hence, trust models deal with trustworthiness of the technical infrastructure.

Trust in IT security always reads as “trust in the correct function of a technical component which is important for the system security”. In this definition, the 1990ies brought some scientific work on trust management in IT systems and distributed systems. Focus of the work was mostly the authentication of systems or software as a trust-enabling measure.

http://www.sirrix.de/media/downloads/56275.pdf,download

2.1.2.2 Trusted Computing Group

As mentioned at the beginning of this section, the Trusted Computing Group works on specifications that are later published for the industry to use. The following comes from the Developer Glossary available on their website, but this is also part of the ISO-11889-1 standard (Trusted Platform Module).

Transitive Trust
(From: http://www.trustedcomputinggroup.org/developers/glossary)
Also known as “Inductive Trust”, in this process the Root of Trust gives a trustworthy description of a second group of functions. Based on this description, an interested entity can determine the trust it is to place in this second group of functions. If the interested entity determines that the trust level of the second group of functions is acceptable, the trust boundary is extended from the Root of Trust to include the second group of functions. In this case, the process can be iterated. The second group of functions can give a trustworthy description of the third group of functions, etc. Transitive trust is used to provide a trustworthy description of platform characteristics, and also to prove that non-migratable keys are non-migratable.

Trust
Trust is the expectation that a device will behave in a particular manner for a specific purpose.

Trusted Computing Platform
A Trusted Computing Platform is a computing platform that can be trusted to report its properties.

2.1.3 Definitions used by the research funding bodies
In the following sections, we take a look at how trust is defined by several of the funding bodies for research. We include two definitions here. One comes from the EU’s 7th Framework Program for ICT Research. The second is from the Norwegian Research Council’s definition from its ICT program (VERDIKT).

2.1.3.1 EU FP7 ICT Research Work Program
The EU’s 7th Framework Program for research in ICT includes several different areas that the EU are interested in funding additional research. These areas have been grouped up in the form of challenges. The challenge relating to security and trust (Challenge 1) is quoted below.

Networks and service platforms will become increasingly vulnerable as current developments lead to more complex and large-scale heterogeneous networks with massive distributed data storage and management capacity. They need to be made trustworthy which is defined in this context as: secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in his security management. Trustworthiness needs to be considered from the outset rather than being addressed as add-on feature. Societal and legal issues increasingly impact technological choices. ICT must be developed to ensure a society based on freedom, creativity and innovation, whilst providing security for its citizens and critical infrastructures.
(Challenge 1: Pervasive and Trustworthy Network and Service Infrastructures, Introduction section in document Work Programme 2009-10)

2.1.3.2 Norwegian Research Council VERDIKT program
The following is a quote from Norway’s ICT research program.

Trust in the Norwegian perspective is a property that materializes in the use of computers by people. Trust is perceived as trust in the correct function of the IT system, and the absence of threats or risks posed by the IT system or any other party involved.
2.1.4 Summary

As we can see from this selection of organizations, there are many definitions for trust. We can choose to focus on trust in a purely technical way, but this neglects the user completely. Trust is then relegated to algorithms and specifications and the user has no chance to be inserted in the trust chain. On the other hand, we cannot go to a completely human definition either because there will be no way that we can guarantee that people actually have security when they are using items in the IoT. Clearly, our final definition of trust needs to encompass human needs and technical needs that will be recognizable to both parties.

2.2 Level of trust, security and risk

Below we reason about defining the level of trust, security and risk and how to measure them.

2.2.1 Level of trust

Experiments confirm ([Booth 1989]) that human brain handles practical problems – which one needs for “surviving” in the modern society – much quicker and more precisely. A good example is handling cash and cheques. However, when such a problem is abstracted – i.e. when one starts to talk about cards or transactions instead of value-holding money – this magic is lost.

Similar effect applies to trust: When a user trusts a system, they will use it. Otherwise, uncertainty and lack of trust prevents him from using the system. In the case of a solution which is indeed insecure, this is just the desired user behavior, whereas in the case of a secure solution this entails measurable business loss.

Based on the previous sections, it is worth comparing trust with some similar but different expressions:

- “Trusted” – (meaning: “without additional control”)
- “Trustworthy” – (meaning: “it proved to be”)
- “Secure” – (meaning: “protected by technological measures”)
- “Safe” – (meaning: “does not cause catastrophic damages”)

Trust in this context is something different, an attribute that does not belong to the system, but to the user, and their perceptions. It is on one hand a belief, the fact that one thinks a system/solution/etc. is secure. On the other hand, it is fear, paranoia, the fact that one thinks it is dangerous.

Trust is influenced by multiple factors through which it can be approached, understood and measured. Such are conscious and subconscious decision separation, informed decisions and uncertainty, mental models and human feelings.

Experiments also show that we can find a limit up to which one trusts something. This trust level determines the decision that someone will do something or refuse an operation because of the lack of trust (e.g. the biggest amount of money we would lend someone).
There are numerous methods and practices available for measuring trust, driven by different ideas and depending on the different definitions of trust. However, the trust that uTRUSTit targets seems to be best measured via empirical methods and thus needs experimenting and involvement of real persons.

2.2.2 Level of Information Technology security

It is often claimed that an activity cannot be managed well if it cannot be measured [Payne 2006]. Security measurements can be developed to assess (i) the degree to which an implemented and operated system meets the security design goals and (ii) the degree to which the security design goals, as implemented, meets the needs of users. System designers and operators require sufficient and credible evidence that the system under investigation implements the intended security level or performance. An improvement in the value of a measurement result thus makes it more likely that the related objective or sub-objective will be met [Savola 2010].

Metrics and Measurements: Measurement is the process by which numbers or symbols are assigned to attributes of real world entities in such a way that describes them according to clearly defined rules [Fenton 1997]. In general, measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing two or more measurements taken over time with a predetermined baseline [Payne 2006].

Use of Metrics: Security metrics can be used for decision support, particularly in assessment, monitoring, and prediction. Security measurement targets can include a technical system, service, or product, or an organization, its processes, and resources. Some of the ways in which security metrics can be used include [Savola 2010]:

- Risk management activities for mitigating security risks,
- Comparison of security-enforcing mechanisms or solutions,
- Obtaining information about the security posture of an organization, process, or product,
- Security assurance (analysis, testing, monitoring) of a product, organization, or process,
- Security testing (functional, red team and penetration testing) of a system,
- Certification and evaluation of a product or organization,
- Adaptive security monitoring and management during system operation, and
- Intrusion detection and prevention in a system.

However, if the goal is to develop security metrics for a human audience, it is important to visualize the result and the final metrics should be clearly understandable.

Criticisms and Challenges: Security metrics are not without criticisms and challenges. A metric simplifies a complex socio-technical situation down to numbers or partial orders. Such simplification might have side effect [McHugh 2002]. While Bellovin [Bellovin 2006] states that defining metrics is hard, if not infeasible, because an attacker’s effort is linear and exponential security is needed. Burris and King Burris [Burris 2000] argue that luck plays a major role in security especially in the weakest links of information security solutions. There are also a number of challenges in developing security metrics: Complexity of software systems (where all potential state transitions are not known), uncertainty (it is hard to assess how likely transitions between states are), non-stationarity (security risks can vary, even rapidly, over time), limited observability (It is hard to observe, measure and to correctly detect all events), and maliciousness (Security threat agents can be strategically intelligent).

Avižienis et al. [Avižienis 2004] presented a detailed taxonomy of security and dependability quality attributes that can be used in the selection of adequate dimensions to be investigated [Savola 2009]. Further surveys of security metrics can be found in [Herrmann 2007], [Jaquith 2007], [Savola 2008], [Bartol 2009], [Jansen 2009].
2.2.3 Level of risk as a measure of security

Risk is used as a negative measure of security. As a proper definition, we can say that risk is the expected value of the damages caused by incidences of threats during a given period of time. Accordingly, it can be expressed by a mathematical formula as follows:

\[ R = \sum_{t \in T} p_t \cdot d_t \]

where

- \( R \) : Risk
- \( T \) : Threats
- \( p_t \) : Probability of the incidence of threat \( t \)
- \( d_t \) : Damage caused by the incidence of threat \( t \)

Risk is an inherent part of any security or trust system. Risk adaptive security is an emerging technology that adapts its decision based on a computation of security risk. At a conceptual level within the maintenance of high levels of trust, reliability and security in the presence of threats to IoT critical infrastructures, resources are, however, sometimes restricted in terms of computing infrastructure. A comprehensive risk assessment might therefore be appropriate to assess what components and/or levels require the highest level of protection in order to reduce the overall effect, or at least to mitigate, the worst threats of those events whose effects it would take the longest time to process [Abie 2010].

2.3 Balancing the user’s trust and security

Trust is a necessary prerequisite basis for a decision to interact with an entity. “Good behaviour” builds trust slowly, while “bad behaviour” erodes trust quickly. Trusting an entity is always associated with risk since there is always a chance that the entity will behave contrary to expectations. The traditional ways of establishing and maintaining trust such as the use of cryptography, digital signatures and digital certificates had been efficient in computing till the need for IoTs to automate decision taking arose and the levels of re-configurability are required to respond to changing contexts. Once the trust is established and the environment is in use, in IoT we may observe novel and unexpected behaviors which may not fall within the existing rules of trust establishment and maintenance, and user’s trust perception. Trust management processes in the IoT must evaluate such behaviors and decide whether they are to be promoted as a beneficial innovation, tolerated or suppressed, creating new trust management rules and policies to be managed thus creating fruition environment. The fruition will take place when the new environment supports the fulfillment of the shared and dynamically evolving “intentions” of users. These aspects of IoT demand effective and reliable algorithms for estimating the relative trustworthiness of information sources in trust and security solution evaluation using knowledge level and level of expertise trust variables, and learning, anticipating, and adapting to a changing environment at run-time in the face of changing threats [Houmb 2006], [Abie 2009]. Chess, Palmer, and White outline a number of security and privacy challenges facing those designing and developing autonomic systems, and also a number of ways that autonomic principles can be used to make systems more secure than they are today [Chess 2003].

Trust builds confidence in the value of a business and potentially provides security. Security supports the process of establishing and maintaining trust through the provision of a secure and trustworthy environment. Security also reduces the rate and severity of security compromises by continuously adjusting and responding to constantly emerging and changing threats. Based on these relationships of cause and effect as a foundation, user’s trust and security can be balanced.
What is finally the relation between security and trust?

Security has much more power over trust than vice versa. If the user overtrusts a system – i.e. believes it provides more security/privacy than it does in fact – or underestimates the danger it is exposed to, this false feeling of security leads to the user’s higher vulnerability to attacks. Similarly, if the user overestimates the level of risk, an ungrounded paranoia will lead to lost opportunities in business.

Consequently, misjudging a system’s security level has a high influence on its user. It is therefore an important goal to establish the balance between user trust and security. Our goal in uTRUSTit is to maintain this balance in the Internet of Things.

How do we maintain the balance? Let us handle the two cases differently.

When trust unduly exceeds the system’s effective security level, appropriate measures are necessary for Raising Security Awareness. These solutions warn the user of potential threats and risks, in an informative yet user-friendly way. Of course, raising the security level itself is also a solution, if possible.

Contrarily, in the case when a system – of otherwise high security level – lacks the necessary level of trust from the user’s part, we will rely on Trust building solutions. These techniques are not necessarily technologies, but rather User Interface (UI) tricks and techniques to enhance trust, via supporting informed decisions by decreasing uncertainty in the user.

To achieve the best results, such methods must go far beyond being informative; they ideally include psychological tools of education and trust-influencing (e.g. rewards or punishments).

In certain scenarios – and uTRUSTit is such a scenario – it is also important to consider a complementary aspect of trust: the trust towards the trust-feedback and trust-enhancing methods themselves. The uTRUSTit framework is not only to gain (or ruin) trust related to the IoT, but also to make the user believe in the dependability of the framework’s judgments when it comes to security and privacy.
Boiling down the above reasoning, trust depends not on the actual security of a system, but on the user perception of it. Our goal in uTRUSTit is not to invent or implement security enhancing technologies, but to methodize, implement and evaluate trust enhancing solutions for the IoT.

The question now is: what are those solutions, which build trust or raise awareness in the IoT?

### 2.3.1 Raising security awareness

There are numerous methods for raising security awareness, which – if successful – have the ability to ruin trust in a systems’ user that was based on misjudging the system’s security level. We must not forget however, that this is only halfway to successful trust management: our goal is to keep the balance between security and the perception of security, which – in the security context – we called trust.

To raise security awareness, the probably most straightforward solution is textual communication to the user, keeping them up-to-date about the security and privacy aspects of their activities in the system (browsing the web, sharing data, etc). As we will see in section 3.4.2.1, there is still a lot to improve in the field of security feedbacks.

Raising security awareness and building trust, no matter how strongly they are tied to technologies and systems, dig deep into the science of psychology. A good example is that you can even raise security awareness by doing nothing, just having an insecure system without giving alerts about security issues.

### 2.3.2 Building trust

Building trust is the focus of the uTRUSTit project. As mentioned above, this cannot be achieved without raising security in the scope. It is just the reverse: if a system has the ability to do both well, and thus is able to balance between user perceptions and reality, then users of this system will feel trust.

Let us have an example from the car business. Our intelligent car can teach us to fasten our seatbelts by punishing us whenever we forget to do so – for example by playing an annoying alarm sound until we fasten it. And still it builds trust in us.

There is a huge marketing push on system security, as people are looking for safety when buying cars more and more. Marketing can strengthen user perception of security (by, for instance, playing crash test videos and displaying security statistics), and it is also true that security does not sell itself without marketing – trust has to be built in people.

On the other side, similar ways build false trust in us. Strict screening on airports make us feel more secure, but it is probably not true. Bank card payment service sends a confirmation and/or feedback SMS upon transaction, making the user feel control, which is also just partially true in fact. And as mentioned above, security warnings also face challenges in maintaining the appropriate balance between trust and effective safety and security of the user.

What is to be done then about it? It simply has to be done better. Make the user feedback mechanisms able to build trust. Align the real actual security level and the displayed information. Avoid ambiguity in messages and signs, help to decrease uncertainties, provide support for informed decisions from the user’s part.

Regarding the user perception of the applied security controls: establish the feeling that the user has the control. And only raise security awareness (i.e. punish), when necessary.
2.3.3 Balancing stakeholder interests from design into security specifications

In accordance with „Privacy by Design” (see 6.2.8 Privacy by Design principles), the design process of trustworthy IoT shall consider all stakeholder’s interests when coming up with a security specification. As IoT and its applications are, mostly, a future technology, one of the first challenges is the identification of a sufficient set of stakeholders. In uTRUSTit, we had to extract probable stakeholders from our scenarios, and we had to make assumptions about their interests derived from related businesses and business models.

![Diagram](2-1 A process for building trusted, privacy-respecting infrastructures (from [Fritsch 2007]).)

2.3.3.1 Approaches to security and privacy engineering

This section will present approaches for security and privacy engineering for information systems. Few complete frameworks or approaches have been published, namely KPMG's model in [KPMG 2003], a security framework in [Zuccato 2005], and a design process in [Fritsch 2006]. The work on risk modeling in [Hong 2004] also provides insight on requirements engineering. In particular, the interdisciplinary nature calls for a model that provides a frame for knowledge in important disciplines as well as a way of integration of application-specific knowledge. Several approaches towards 4th-generation design methods for IT security in information systems exist. Siponen describes the requirements engineering and design process as a socio-technical process in [Siponen 2002]. Beyond security, Sommerlatte describes in [Sommerlatte 2002] the concept of Maieutik. Here, a process with strong user interaction and rapid prototyping cycles is used to ensure that information systems match their user’s requirements. The lack of metrics for privacy in information systems as well as the lack of standards (there are some ISO activities, but so far the application of ISO 15408 “Common Criteria” for privacy evaluation is only under research in [Kohlweiss 2004] and in ISO/IEC/JTC1/SC27/WG3 [Brand 2005]. A suitable approach to collect interdisciplinary security requirements is Multilateral Security [Rannenberg 2000], applied by Fritsch and Scherner in [Scherner 2005]. It is applied according to the application requirements and the first high-level design of an information system is made. Its goal is to develop multilaterally satisfying security and privacy requirements. Several research groups have proposed platforms to manage privacy, for example [Huber 2003], [Jorns 2004], and [Koelsch 2005]. These architectures were specified for a specific application purpose, but solely from a technician's view.

2.4 Summary and conclusion

So far we have examined the concept of trust from different approaches, and, taking the trust approach that is the most relevant to uTRUSTit – the security-based approach – we have given an overview on the
necessity and practices to balance it with reality. This was not only important for short-term trust maintenance, but for establishing trust and anticipating business loss on the long run as well. We also concluded before that both system-centric and user-driven approach are important when assessing trust.

For a better understanding of what uTRUSTiT should mean by ‘trust’, it is beneficial to set out from a short, yet flexible and abstract initial definition, as we did in the case of IoT:

**Trust:** The expectation that a thing will do what it claims it will do without bring harm to the trusting user. This also includes the perception of being secure (e.g., resilient to attack). It also includes that the user:

- knows who is being spoken to,
- knows what is happening,
- feels in control of what is happening, and
- understands to the necessary extent the involved distributed services.

To nourish this definition for our purposes, we will – on one hand – consider the aspects needed to achieve the project’s goals, while we keep relying on the pre-existing descriptions of trust.

Complementing and summarizing the above, below is introduced a conceptual model of different approaches to trust by [Wiedmann 2010]. Dealing with so-called “IT-Ecosystems” (ITEs), Wiedmann separates system-centric trust definitions from user-driven components, in order to conclude with a comprehensive model above both. Below is [Wiedmann 2010] cited.

In an attempt to structure existing definitions, structural approaches, antecedents, and consequences of trust, we will rely on six key constructs of trust as defined by [McKnight-Chervany 1996]. These six trust-related constructs are 1) system trust, 2) dispositional trust, 3) situational trust, 4) trusting beliefs, 5) trusting intentions, and 6) trusting behavior. They form a group of trust dimensions that are conceptually distinguishable but are interrelated to each other in specified ways [McKnight-Chervany 1996].

Especially as we consider the interdependency between trust and the adoption of ITEs, distinguishing between I) technology-driven and II) user-driven components of trust, these six constructs include the most important elements of perceived trust as represented in our conceptual framework and our propositions. For the purpose of our study, we categorize the six trust-related constructs into one of two groups:

**Technology-driven Components of Trust in ITEs**

The first set of trust-related constructs encompasses system trust, dispositional trust, and the situational component of trust. In general, these components of trust have to do with institutional phenomena and impersonal structures [Lewis 1984], [Luhmann 1991], [Shapiro 1987] and specific situations [Baier 1986], [Garfinkel 1967], [Lewis 1984]. They are conceptualized as cross-situational or cross-personal [Harnett 1980], [Wrightsman 1991]. In our context, they are related to the technological characteristics that influence an individual’s trust in ITEs.

- **System Trust:** Defined as the extent to which an individual believes that proper impersonal structures like structural assurances (e.g., regulations, guarantees, or contracts) and situational normality (which reduces uncertainty) enable an individual to anticipate a successful future endeavor, an individual’s willingness to trust the components of an ITE is an important technology-driven element of trust in ITEs [Lewis 1984], [Luhmann 1991], [McKnight-Chervany 1996], [Shapiro 1987].
- **Dispositional Trust:** Based on a cross-situational, cross-personal conceptualization of trust, dispositional trust refers to generalized expectations and a consistent tendency to trust an ITE
across a broad spectrum of situations and persons [Harnett 1980], [McKnight-Chervany 1996], [Wrightsman 1991].

- Situational Decision to Trust: This component of trust has to do with the extent to which an individual intends to trust every time a particular situation arises; the situational component of trust entails the user’s decision to trust the ITE without taking into account the specific attributes of the other party involved [McKnight-Chervany 1996], [Riker 1971].

**User-driven Components of Trust in ITEs**

The second set of trust-related constructs – trusting beliefs, trusting intentions, and trusting behavior – is widely studied in social psychology and is based on the theory of reasoned action [Ajzen 1980]: Certain beliefs and attitudes lead to behavioral intentions that become manifest in actual behavior. According to this belief-attitude-intention-behavior pattern in our context, an individual with trusting belief in another person or component is more willing to depend on that person or component and will behave in ways that manifest that reliance [Currall 1995], [Dobing 1993], [McKnight-Chervany 1996]. In our study, these components of trust relate to the individual and social aspects that influence a user’s perceived trust in ITEs.

- Trusting Beliefs: Including cognitive beliefs/intentions and belief-related confidence in the other ITE components’ traits and intentions, trusting beliefs indicate the extent to which an individual believes and feels confident that the other component is trustworthy and willing to act in the individual’s best interests in a given situation [McKnight-Chervany 1996], [McKnight-Cummings-Chervany 1996].

- Trusting Intentions: The intentional component of user-centric trust in ITEs can be defined as the extent to which an individual is willing to depend on the other ITE component in a given situation with a feeling of relative security, even when negative consequences are possible [McKnight-Chervany 1996].

- Trusting Behavior: Supported by trusting intentions, the behavioral component of user-centric trust in ITEs is the extent to which the individual voluntarily feels secure in depending on the other components of the ITE, even when negative consequences are possible [Lewis 1984], [McKnight-Chervany 1996].

Here we concentrate on two sets of propositions with regard to technology-driven and user-driven components of trust in ITEs based on a multidimensional model as presented in 2-2. The propositions consider trust in ITEs on a global level and are not specific to the different components of trust presented in our conceptual model.
2-2 Conceptual Model of Trust in IT Ecosystems
3. Trust and the User in the Internet of Things

One important conclusion of the above chapters is the importance of user perception of trust within the IoT, its measurability, management and balancing with the system’s effective security. The following lines will dig deeper into this topic, outlining relevant problems and solutions, different user aspects of trust and uTRUSTit’s relating conceptions. The chapter ends with a list of usability standards of relevance.

3.1 Trust and the User in the Internet of Things

Systems are becoming more and more ubiquitous and pervasive and as a result, users lose track of which “things” are connected to the Internet and communicate with it. Therefore, one problem facing the users is lack of trust in such systems because the functionality of the whole system is unclear to them. Nevertheless, user trust in the Internet of Things is a prerequisite for successful adoption of this technology in users’ daily lives.

One focus of uTRUSTit is to prevent users from losing the overview and increasing the trust in IoT. In order to achieve better transparency and to increase trust, the user will be placed into the trust chain and thus be able to make decision about trustworthiness and trust in a much more direct way. Most current research activities pay attention to the technical aspects of the trust chain (e.g. technical devices) in order to achieve trustworthiness in the chain of connections. Although this in itself is already a challenging task, it neglects the trust chain between the technology and the user, which can diminish the quality of trust of the entire system. Users often have wrong or incomplete assumptions about trust chains and the technical aspects associated with it. To toil against users wrong or incomplete assumptions and increase their trust in IoT it is necessary to develop a transparent access to IoT for users.

The growth of the Internet is an ongoing process, only twenty-five years ago it was connecting about a thousand hosts, since then it has grown to link billions people through computers and mobile devices. One major step in this development is to progressively evolve from a network of interconnected computers to a network of interconnected objects, from cars to books, from electrical appliances to food, and thus create an ‘Internet of things’ (IoT) [ITU 2005], [Ducatel 2001]. These objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment (e.g. food products that record the temperature along the supply chain) or use actuators to interact with it (e.g. air conditioning valves that react to the presence of people). The scope of IoT applications is expected to greatly contribute to addressing today’s societal challenges: health monitoring systems will help meet the challenges of an ageing society; connected cars will help reduce traffic congestion and improve their recyclability, thus reducing their carbon footprint. This interconnection of physical objects is expected to amplify the profound effects that large-scale networked communications are having on our society [CEC 2009].

3.1.1 Problems facing the IoT

Using the IoT sounds like an ideal world created, however the IoT has an awfully complex nature. First, IoT should not be seen as a mere extension of today’s Internet but rather as a number of new independent systems that operate with their own infrastructures (and partly rely on existing Internet infrastructures). Second, as detailed in a recent ISTAG report (2009), IoT will be implemented in symbiosis with new services. Third, IoT covers different modes of communication: things-to-person communication and thing-to-thing communications, including Machine-to-Machine (M2M)
communication. These connections can be established in restricted areas (‘intranet of things’) or made publicly accessible (‘Internet of things’) [CEC 2009].

The IoT will create a dynamic network of billions or trillions of wireless identifiable “things” communicating with one another. Everything will be connected through the IoT from individuals, groups, communities, objects, products, data, services and processes. In the IoT, “things” are expected to become active participants in business, information and social processes. Where they are enabled to interact and communicate among themselves and with the environment by exchanging data and information “sensed” about the environment, while reacting autonomously to the “physical world” events and influencing it by running processes that trigger actions and create services with or without direct human intervention [de Saint-Exupery 2009].

Furthermore, the number of connected devices is increasing, while their size is reduced below the threshold of visibility to the human eye. Another factor is mobility as objects are ever more wirelessly connected, carried by individuals where ever they go and geo-localisable [CEC 2009].

3.1.2 Privacy problems in IoT

Although the IoT will provide help in many areas, it will usher in its own set of challenges some that will directly affect individual users. For example, some application will handle information related to an individual whereabouts while others may be closely interlinked with critical infrastructures such as the power supply. Connectivity will become in the IoT a kind of service not owned by any private entity and available to all at an especially low cost. In this context, there will be a need to create the right situation-aware development environment for stimulating the creation of services and proper intelligent middleware to understand and interpret the information flow to ensure protection from malicious attack and fraud and to guarantee privacy to users [de Saint-Exupery 2009]. These societal changes will have to be addressed by European policy-makers and public authorities to ensure that the use of IoT technologies and applications will stimulate economic growth, improve individuals well-being and address some of today’s societal problems [CEC 2009].

3.1.3 Who trusts who?

At the heart of the Internet of things vision lays an inherent contradiction. On the one hand, a computing environment must be highly knowledgeable about a user to match to his or her needs and desires without explicit interaction—almost reading the user’s mind. On the other hand, a system that is truly ubiquitous will encompass numerous users, physical regions, and service providers. At such large scale, perfect trust among all parties is an unattainable ideal [Satyanarayanan 2003].

Privacy issues have been researched and discussed in many related areas e.g. [GKC 2004], [Hildebrandt 2010], [Langheinrich 2009], with the field of ubiquitous computing being the closest. In the IOT however new sets of potentially sensitive data becomes available through profiling of the “things”, and questions regarding what this data is telling about the user and who should be allowed to see and use this information have to be raised. The key issue is “how one is being read (and interpreted in a possibly mismatching context) by someone else” [Hildebrandt 2010]. Another new dimension of privacy aspects in the internet of things is the vast amount of objects and data that has to be dealt with. Due to the amount and hiddenness of information new dimensions of complexity in the formulation of privacy concepts, the engineering of privacy policies, and the management of information privacy both for data processors and users emerge. Research has shown that information on social networking sites has the potential for severe consequences, and that users have difficulties to correctly understand and interpret possible long-term effects of their behaviour [AG 2004]. Therefore even more severe problems and consequences have to be expected for a wide-scale application of IoT-concepts [Schrammel 2011].
3.1.4 The individual trusting in the machine

Privacy and security are already thorny problems in distributed systems. A variety of problems plague us, ranging from spam to identity theft. Pervasive computing provides many new avenues of attack. Mechanisms such as location tracking, smart spaces, and the use of surrogates require continuous monitoring of user actions. As a user becomes more dependent on a pervasive computing system, the system becomes more knowledgeable about that user’s movements, behaviour patterns, and habits. Exploiting this information is critical if the system is to be proactive and self-tuning [Satyanarayanan 2003].

The privacy of citizens has always been in sharp contrast with making humans traceable by tagging them. Despite this, some tendencies are coming up, where people allow themselves to be tagged with implantable RFID tags in order to distinguish themselves from the crowd. On the other side of the spectrum, there exist valid usability reasons to implant such a chip, e.g., for chips that can determine the blood sugar level (diabetics), or internal cardioverter-defibrillators for certain patients, curfewed offenders, etc., [de Saint-Exupery 2009]. If users are to be persuaded to participate in a ubiquitous network society then they will need to be given a reason to trust that their privacy will be protected at all times. The challenge is daunting if we consider the privacy concerns and mistrust that have followed from the introduction of RFID tags and smart cards into the marketplace [ITU 2005].

Closely related to these privacy issues is the question on how a basic level of trust can be supported and achieved within the IoT. Little is known on how models of trust that are formed both in interaction in human society and in the context of desktop computing can be transformed towards the IoT, and which specific difficulties, misconceptions and challenges might arises, and how they can be accounted for from a design perspective. Currently, trust is often anchored in a strict technological context, which is easily misinterpreted by humans and miscommunicated by system vendors and owners. Another specifically challenging aspect of the IoT is that only very limited feedback and interaction possibilities to communicate the current status of the system and the data exchange exist. Due to the pervasive and ubiquitous nature of the everyday objects they only can be enhanced with little information bits, thereby making it extremely challenging to communicate complex patterns of data transmission and privacy status. The typical communication bandwidth of an object within the IoT might be one bit: on or off, possibly displayed by use of a LED or similar means. Here the question is how much (status) information regarding privacy issues can be communicated with such restricted possibilities, and what other means to keep user informed and aware of what’s going on can be utilized in the IoT context [Schrammel 2011].

When everyday items come equipped with some or all of the five senses (such as sight and smell) combined with computing and communication capabilities, concepts of data request and data consent risk becoming outdated. Invisible and constant data exchange between things and people, and between things and other things, will occur unknown to the owners and originators of such data. The sheer scale and capacity of the new technologies will magnify this problem. Who will ultimately control the data collected by all the eyes and ears embedded in the environment surrounding us? [ITU 2005]. Another issue is the ‘things’ that a government imposes on its citizens to give them access to certain facilities, such as healthcare insurance (wireless medi-cards), the ability to travel (passports with built-in chips) or identification (eID cards or eID/RFID implants). For each of these technologies, the privacy and security impact should be evaluated. On a consumer level, it remains to be investigated how much information can be extracted from consumer electronics with sensors, and to which extent this can be regulated by law. In any case, there’s an enormous potential for enhancing the user experience, based on the ‘things’ in his surrounding [de Saint-Exupery 2009].

To promote a more widespread adoption of the technologies underlying the Internet of Things, principles of informed consent, data confidentiality and security must be safeguarded. Moreover, protecting privacy must not be limited to technical solutions, but encompass regulatory, market-based and socio-ethical considerations. Unless there are concerted efforts involving all government,
civil society and private sector players to protect these values, the development of the Internet of Things will be hampered if not prevented. It is only through awareness of these technological advances, and the challenges they present, that the future benefits of a fair and user-centric Internet of Things can be apprehended [ITU 2005].

3.1.5 Things trusting in people

On the other hand the things in the IoT also have to trust in its user. That is that the user is who he says he is. For example, with electrical access keys connected to the internet, the thing will have to trust that only its rightful user is having access to restricted areas. Therefore, establishing trust is a two-way problem. Just as users must be confident of their computing environment’s trustworthiness, the infrastructure must be confident of a user’s identity and authorization level before responding to requests. It is difficult to establish this mutual trust in a manner that is minimally intrusive. This will become a key requirement as pervasive computing moves from the lab to the real world. Without a reliable and accurate way to establish identity and authorization, service providers won’t have incentives for deploying the infrastructures and services necessary for pervasive computing. At the same time, frequent demands for passwords or other proofs of authenticity from the user will destroy the essence of pervasive computing—namely, its ability to disappear into the user’s subconscious. It is critical to develop techniques that balance these divergent requirements [Satyanarayanan 2003].

How do we express security constraints, such as “Only the person currently using the projector in this room can set its lighting level” or “Only employees of our partner companies can negotiate with properties in this smart space”? Clearly, the security and privacy challenges of pervasive computing will keep researchers, designers, and implementers busy for a long time [Satyanarayanan 2003].

3.1.6 Battling the trust in the IoT

Deciding a common strategy and a policy for future Internet of Things is a priority. The European Commission (2009) considers that each datum itself in its integral parts is not a threat but this could become a threat when associations are built via accessed databases such that sensitive relationships are revealed or discovered, resulting in damage or potential for damage [de Saint-Exupery 2009]. Network and data anonymity can provide a basis for privacy, but at the moment, these technologies are mainly supported by rather powerful equipment, in terms of computing power and bandwidth. A similar argument can be made for authentication of devices and establishing trust.

As part of its 2009 Work Programme, in support of EU policy, the European Network and Information Security Agency (ENISA) has undertaken to identify emerging risks affecting trust and confidence, in particular regarding RFID. This constitutes as a first step in the understanding of the privacy and security risks that will impinge on IoT. Another key aspect to building trust is the capability to adjust the functioning and properties of technological systems to individual preferences (within safe boundaries). Studies have shown that giving users a sufficient level of control improves their level of trust and plays an important role in the uptake of the technology [CEC 2009].

3.1.7 Increasing awareness

A small step in the right direction towards increasing trust in the internet of things would be to make users more aware of their current privacy exposure level. For example, a handheld computer could unobtrusively indicate what information the system is exporting to its surroundings. For example, is the system sharing a user’s identity or allowing its location to be tracked? Are network transmissions
encrypted? A user uncomfortable with the current exposure level should able to temporarily restrict the export of certain kinds of information. This would undoubtedly hurt invisibility but it offers the user an explicit way to over-ride an erroneous system choice [Satyanarayanan 2003].

3.1.8 Maintaining an audit trail

The system should maintain an audit trail of privacy-related interactions. What service requested a particular piece of information, where and when? On what grounds was the information released? Who demanded user authentication and when? How was the request satisfied? Maintaining a comprehensive privacy audit trail should thus be feasible even on resource-limited mobile hardware. Although auditing cannot prevent privacy violations, it can help provide clues for forensic analysis of how a particular violation occurred. Additionally, the fear of being discovered can sometimes serve as a useful deterrent [Satyanarayanan 2003].

3.1.9 Conclusion

Internet of Things needs to be built in such a way as to ensure an easy and safe user control. Consumers need confidence to fully embrace the Internet of Things in order to enjoy its potential benefits and avoid any risks to their security and privacy [de Saint-Exupery 2009].

Privacy is clearly a value that is important in modern societies and will likely remain so for some time to come. The difficulty lies in establishing a balance between the rights of the community and those of the individual, particularly in the face of new technologies that dramatically increase our ability to collect and use personal information. In many cases, this ability is a desirable innovation to the extent that it can improve the efficiency of governments and businesses, thereby reducing costs to citizens and consumers. On the other hand, such technological developments threaten to sustain a surveillance society involving pervasive data collection from our public lives and unwanted intrusions into our private actions through data mining of our ever-expanding information trails [ITU 2005].

Closely related to these privacy issues is the question on how a basic level of trust can be supported and achieved within the IoT. Little is known on how models of trust that are formed both in interaction in human society and in the context of desktop computing can be transformed towards the IoT, and which specific difficulties, misconceptions and challenges might arise, and how they can be accounted for from a design perspective. Currently, trust is often anchored in a strict technological context, which is easily misinterpreted by humans and miscommunicated by system vendors and owners [Schrammel 2011].

3.1.10 Security and the user in internet of things

Internet of Things needs to be built in such a way as to ensure an easy and safe user control. Consumers need confidence to fully embrace the Internet of Things in order to enjoy its potential benefits and avoid any risks to their security and privacy [de Saint-Exupery 2009].

3.1.11 The user “The Weakest link”

Even though every company spends considerable amount of money each year on security, and that security measures are implemented early in the process of development. Buying and deploying security products does not automatically lead to improved security. This seems to be because many users can’t be bothered
with security measures or use them wrongly. For example people tend to disclose their passwords, don’t use encrypting for personal messages or switch virus checkers off. This is thought to happen because the user does not understand the importance of data or software, have problems with the security tools or simply do not believe their asset is at risk or that their behaviour is putting their assets at risk [Sasse-Flechais 2005].

3.1.12 “What does this mean?”

As computing systems are used more and more in the daily life of the common user and will increase with the internet of things, the security solutions have to be made more understandable. Historically security solutions have been designed with a highly trained technical user in mind, leading to problems for the common user to understand. The negative impact that usability problems can have is higher for security and privacy applications than for many other types of systems. If the security operation is too complex that the users can’t understand it costly error will occur [Karat-Brodie-Karat 2005]. Studies have shown that mechanisms for encryption, authorisation and authentication can be difficult for people to understand or use and that users are much better at following security policies when they are given explanations on both the real security threats and the goals of the security policies [Adams-Sasse 2005].

3.1.13 “This is in my way”

Security tasks must not make demands on users that conflict with the demands of their production tasks. The current reality is that security mechanisms are often chosen without consideration of production tasks, and individual users are often left to make a choice between complying with security regulations or getting the job done, and the choice they make is predictable. It is unfortunate that usability and security are often seen as competing design goals in security, because only mechanisms that are used and used correctly, can offer the protection intended by the security designer. Furthermore, tradeoffs between production tasks and security should not be made by security experts, who naturally prioritise security over efficiency [Sasse-Flechais 2005]. Users would like privacy and security systems and controls to be as transparent as possible. On the other hand users want to be in control of the situation and understand them. There lies the dilemma security systems should be visible to the user when needed but they should not get in the way of the user finishing his or her tasks [Karat-Brodie-Karat 2005]. Moreover, Patrick, Briggs and Marsh [2005] argued that users should not have to arcane issues of security to be able to allow access to some personal data online, they don’t have to do so in the real world and so it should be online.

3.1.14 “It will not happen to me”

It is not enough to simply ask people about trust, privacy or security, because what people say and what people do are two different things [Patrick-Briggs-Marsh 2005]. Human decision making has been a topic of study in social sciences from economics to psychology for over a century. The net sum of that research suggests that individuals are often less than optimal decision makers when it comes to reasoning about risk [West 2008]. West [West 2008] gathered some of the main reasons why users do not follow security instructions and concluded that users simply don’t think they are at risk, i.e. people generally believe that they are at less risk than others, they believe they are better than average driver, and live beyond the average age [Slovic-Fischhoff-Lichtenstein 1986]. Therefore, any computer user has the preset believe that they are at less risk of computer vulnerability than others. Additionally, users are unmotivated as people have limited capacity for information processing and multitask. People favour quick decisions and learned rules as that minimises the effort and the outcome is good enough most of the time. Users do not want to spend too much time thinking about security when they don’t believe they are at any risk.
3.1.15 Mental Models

In the following section we will introduce Mental Models, which will be one approach uTRUSTit uses to get a comprehensive picture on user behavior when dealing with IoT.

3.1.15.1 Introduction to Mental Models

The psychological context we base our research on is the theory of mental models, which was founded in the early 1940s by Kenneth Craik. Some years later they become popular to the HCI community through Norman’s book the Design of Everyday Things. In his point of view the user’s mental model is what the user develops to explain the operation of the system [Norman 1988] and how the user interacts with a special system. For example, on Windows terminals ALT+Q is the shortcut for ‘@’, on Mac the same combination (Apple + Q) closes the current window. So if a Windows user is working on a Mac-system then he will have the wrong mental model concerning the shortcut-function.

3.1.15.2 Mental Models in the Area of Security and Privacy

Since technology gets more and more involved in our daily live, security, privacy and protection of private data become much more important.

In the last years some papers where published which demonstrate the incorrect mental models of users basically concerning security but also privacy, such as [Wash 2008] [Sasse 2001] [Weirich 2001] [Klasnja 2009], which show that users are not aware of security and privacy risks or have wrong opinions concerning these.

Klasnja et al. [Klasnja 2009] showed that users are not aware of security risks when using Wi-Fi, for example that users are unaware of the possibility that information will be transmitted unencrypted and can be intercepted by others. Another point of this paper is that the most feared danger in the internet is hackers. So, on the one hand the participants are afraid of an attack from hackers and the burglary of their financial information. But on the other hand they have no idea what happens to their data when using unencrypted Wi-Fi.

Wash [Wash 2008] presented in his work that users are aware of contagion dangers from the internet but they don’t differentiate between these dangers. All threats are described as viruses, no matter if the meant worm, Trojan horses, adware, and so on. Another incorrect mental model is that viruses just exist in the internet like biological viruses exist in the environment. Participants in this study were afraid of hackers; Wash called it the Burglar Model. Users belief that hackers break into computers like burglars into houses, and they leave the computer after looking for interesting data.

Sasse et al [Sasse 2001] and Weirich and Sasse [Weirich 2001] concentrated on the position of people in the security chain. Their results are that users have mental models that disagree with the security guidelines of many offices. Many users think that security policies run by their organizations are unrealistic and their behavior is common practice. As a consequence, users share their passwords with co-workers, because this is a sign of trust. If someone declines to share passwords within the organisation, the person obtains an image of being untrustworthy. Users’ views on hackers and hacking were also investigated by Sasse et al, indicating that users think that hackers are typically high profile and find always a way into the system. Most users are unaware to the fact that social engineering is one of the key working strategies of serious hackers. Weirich and Sasse also found out that users are afraid of becoming a “Nerd”-image if they behave security-conscious.
3.2 Current and foreseen standards

In the following sections are enlisted multiple standards relevant to usability. These categorized lists might serve as a technical/legal background to rely on when developing and implementing usability-related features in the course of the uTRUSTit project.

3.2.1 Use in context

- ISO 20282-1: Ease of operation of everyday products -- Part 1: Design requirements for context of use and user characteristics
- ISO 9241-11: Guidance on Usability

3.2.2 Interface and interaction

- ISO 9241: Ergonomic requirements for office work with visual display terminals. Parts 3-9
- ISO/IEC 10741-1: Dialogue interaction - Cursor control for text editing
- ISO 9241: Ergonomic requirements for office work with visual display terminals. Parts 10-17
- ISO/IEC 11581: Icon symbols and functions
- ISO 11064: Ergonomic design of control centres
- ISO 12646: Graphic technology -- Displays for colour proofing -- Characteristics and viewing conditions
- ISO 14915: Software ergonomics for multimedia user interfaces
- ISO/IEC 14754: Pen-based interfaces - Common Gestures for text editing with pen-based systems
- ISO/IEC 18021: Information Technology - User interface for mobile tools

3.2.3 Documentation

- ISO/IEC 18019: Guidelines for the design and preparation of user documentation for application software
- ISO/IEC 15910: Software user documentation process

3.2.4 Development process

3.2.5 Capability

- ISO TR 18529: Ergonomics of human-system interaction - Human-centered lifecycle process descriptions

3.2.6 Other Current Standards

- ISO 9241-1: Part 1: General Introduction
- ISO 9241-2: Part 2: Guidance on task requirements
- ISO 10075-1: Ergonomic principles related to mental workload - General terms and definitions
- ISO 10075-2: Ergonomic principles related to mental workload -- Part 2: Design principles
- ISO 9241-17: Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility

3.3 Summary and Conclusion

The success of applications today depends on whether users perceive those applications to be credible. It is important to make users aware of the protection offered to them by building a sense of credibility in the mind of the user [McDonald-Smith 2004].

A sense of control is what makes people feel secure. It produces a physical and emotional experience that encompasses predictive awareness and freedom from threat. Therefore, control is what makes the intersection of security and internet of things so challenging. The benefit of a secure user experience for the end-user is largely out of their control. Whether the intrusion detection systems, redundant firewalls, or strict password expiration policy works or not, most users of “secure” systems know that it is out of their hands. It is in the hands of some good guys tailing logs in a data centre, or bad guys writing the newest malware for spamming and shakedowns [Grossman 2006].

Building secure user experiences is about respect for the user. It is about openly communicating security considerations within an interaction, whether or not they are controllable, and reducing anxiety by increasing awareness. That means there is high need to design for security in internet of things both in terms of the emotional interpretations and functional tasks of the people using the system. This approach is especially important considering that security models tend to overwhelmingly reflect the perceived agenda of an authority, rather than an individual person [Grossman 2006].
4. Virtual Reality in the IoT

This chapter gives a quick – uTRUSTit-centric – overview on Virtual Reality, which plays a main role in testing and measuring interaction between users and the IoT, via the simulation of use case scenarios.

Virtual Reality (VR) in the context of this project means the three dimensional (3D) visualization of objects in scale 1:1. The user is able to interact with all objects in that computer generated VR-environment. He can e.g. virtually walk through the scene and insert, move or delete objects – all in real time. So VR provides the possibility to immerse into the virtual scene. The 3D-impression is generated by stereo projection using either two projectors and polarization filter glasses (passive stereo) or one projector synchronized with so called shutter glasses (active stereo). Figure 1 shows two research assistants reviewing a VR-model of a factory for machine tools in the 5-sided CAVE at the Virtual Reality Laboratory (Virtual Reality Center Production Engineering – VRCP) of the Chemnitz University of Technology’s Institute for Production Engineering and Production Processes.

![Two research assistants immerse in the VR-visualization of a machine tool factory](image1.png)

4-1 Two research assistants immerse in the VR-visualization of a machine tool factory

A CAVE (Cave automatic virtual environment) is, because of its five or six projection sides, the VR-system with the highest degree of immersion. Other VR-Systems are e.g. an L-Bench with two projection sides or a Powerwall with just one. Figure 2 shows examples for VR-Systems.

![Examples for VR-Systems – from left to right: L-Bench, 5-sided CAVE, Powerwall](image2.png)

4-2 Examples for VR-Systems – from left to right: L-Bench, 5-sided CAVE, Powerwall

4.1 Current technologies and best practices

Currently VR-Technology is mainly used within industry sectors like automotive or aircraft industry and production technology. There the main focuses of application are design review on the one hand and marketing purposes on the other. For design reviews it is necessary to visualize components as accurately as possible and in great detail to help designers, commissioning engineers, quality engineers or safety engineers to assess the design with all aspects. For marketing purposes the visualization focus lays on
photorealistic surfaces of objects and the realistic simulation of processes. So the VR-Model can be used to explain e.g. the function and advantages of a machine to possible customer.

4.1.1 Modeling

Starting point for the development of such VR-Models is – in most cases – data out of the CAD-Program. In very few circumstances it is possible to load CAD data directly into a VR-Program. Otherwise the CAD needs to be imported into a modeling-software, like Autodesk 3dsMax, where all simulations have to be added and surfaces upgraded. From there it can be exported as a standard VR-format (VRML) so that it can be used within different VR-software.

The VRCP uses different VR-software such as VDP2008 (by IC:IDO GmbH), Instant Reality (by Fraunhofer IGD) or Livingsolids (by LIVINGSOLIDS GmbH), depending on the visualization purpose.

4.1.2 Simulation

Simulation in VR does not only mean the “animation” of processes and component movements. It also refers to the integration of “real” simulation results into the VR-environment. Examples for such simulation results are the visualization of energy flow data, results of FEM analysis [Neugebauer-Wittstock 2010] or NC-simulations [Neugebauer-Klimant 2010], [Wittstock 2010].

4.1.3 Interaction

The standard interaction devices for the VR-environment are tracking glasses and Flystick (4-3). The flystick is used to navigate through the VR-scene, to grasp or to move objects etc. The silver balls on glasses and flystick are necessary for tracking. Several infrared cameras use them to capture the position of the user and the flystick to update the VR-scene. This allows that the main user always has the optimal view on the VR-scene. In addition the flystick has two buttons – one to activate a menu and one to select a certain action.

4-3 VR-user with tracking glasses and flystick

To minimize or even overcome new users’ inhibition, current research projects try to use consumer hardware – e.g. a Nintendo Wii controller [Schou 2007] – to interact with the VR-Scene.

In a former research project at the VRCP, a tablet was used to interact with the VR-scene. 4-4 shows a user using the tablet pc as a virtual magnifying glass, which helps him to investigate a certain component in greater detail and better resolution.
4.2 Approaches in uTRUSTit

4.2.1 Simulation/Visualization

The contribution of Virtual Reality to uTRUSTit is the simulation/visualization of the IoT. This means to visualize the scenarios smart home and smart office – developed for the “real world” – with all their furniture and of course the smart devices. In contrast to the visualization of e.g. machine tools there is no CAD-Data as basis. It also is not necessary to visualize all components in great detail, as long as the surface looks quit realistic.

The VR-scenarios are than used to provide an environment to test the interaction devices, which are to be developed during the project, in an early development stage. Therefore the feedback the interaction devices or smart systems are supposed to provide for the user after a certain input, needs to be simulated. In this way it is possible to test the users’ reaction to the feedback before the real interaction devices are fully developed and before all communication protocols and security features are established. It will be possible to test the users’ development or loss of trust after certain feedbacks given by smart devices or interaction tools.

4.2.2 Interaction

To be able to test the user reaction to the device feedback, the “real” devices – those who will be developed, whose security features will be improved during the project – need to be simulated within the VR. As the VR needs an interaction device anyway, the goal of the project is to develop a multifunctional VR-interaction device. As this device should represent various “real” interaction devices or smart systems, the basic idea is to use a tablet pc. This tablet pc can be used to interact with the VR-environment as well as to represent the “real” devices. Therefore new graphical user interfaces, which represent the “real” devices as realistic as possible, need to be developed.
Another approach which might be used during the project is the use of a motion capture system to allow the user to interact with the VR-scene using his or her natural movements. A motion capture system is a – in most cases optical – system which allows capturing human motion in real time. At the VRCP we use an inertial motion capture system called XSENS MVN (for more information regarding this system, visit the company’s website [Xsens 2010]). Using this system the test person wears a suit including the motion capture sensors [Weidlich 2009]. When we succeed to couple the motion capture system to our VR system, the test person can use his or her own movements to interact with the VR scene.

4.2.3 Testing

In the first place the developed multifunctional VR-interaction device needs to be tested. On the one hand it needs to be verified that it can be used to interact with the VR-environment. On the other hand graphical user interfaces for the representation of different “real” devices needs to be established as well.

To find out how realistic the user tests in the VR-environment are, the results are compared to the results coming from the real world user tests.

4.3 Summary and Conclusion

Virtual Reality plays a main role in testing and measuring interaction between users and the IoT, via the simulation of use case scenarios. In uTRUSTit VR will be used to to visualize the scenarios smart home and smart office. In contrast to the visualization of e.g. machine tools there is no CAD-Data as basis. It also is not necessary to visualize all components in great detail, as long as the surface looks quit realistic. The VR-scenarios are then used to provide an environment to test the interaction devices, which are to be developed at an early stage of the project. In this way it is possible to test the users’ reaction to the feedback before the real interaction devices are fully developed and before all communication protocols and security features are established.

To be able to test the user reaction to the device feedback, the “real” devices need to be simulated within the VR. The basic idea is to use a tablet pc, which should represent various “real” interaction devices or smart systems. This tablet pc can be used to interact with the VR-environment as well as to represent the “real” devices. Therefore new graphical user interfaces, which represent the “real” devices as realistic as possible, need to be developed. Another approach which might be used during the project is the use of a motion capture system to allow the user to interact with the VR-scene using his or her natural movements. The developed multifunctional VR-interaction device needs to be tested. To find out how
realistic the user tests in the VR-environment are, the results are compared to the results coming from the real world user tests.
5. Accessibility in the IoT

In this section we will look at standards and technologies that are available for helping users to access to the Internet and the Internet of Things. This includes looking at the current assistive technologies that available to mobile devices.

5.1 Standards and Technologies

When looking at accessibility, it is hard not to look at standards and technologies at the same time. This is because several different actors need to work together. A general breakdown could be the following:

- Operating system and Assistive technology engineers define interfaces between each other
- Library writers define an interface between the operating system and applications
- Application developers follow libraries guidelines for making their applications accessible to the operating system
- Standards writers help define what should be accessible and point out issues to be aware of in an application or service.

In some ways, the standards are important because they set a requirement about a certain level of accessibility. Yet, the underlying infrastructure also needs to be there so that things indeed do become accessible.

Another issue is to consider that following guidelines or standards are a necessary condition for success, but they are not sufficient. While, you can guarantee that your application is technically accessible (i.e., your application or service passes all automated tests and validators), it still can be inaccessible to some groups.

Web Standards

One place where a lot of accessibility work is taking place is on the World Wide Web. The Web Accessibility Initiative (WAI), which is part of the World Wide Web Consortium (W3C), does the majority of this work. The most well known standard is the Web Content Accessibility Guidelines (WCAG), but they have also created the Accessible Rich Internet Applications (WAI-ARIA), the Authoring Tool Accessibility Guidelines (ATAG), and the User Agent Accessibility Guidelines (UAAG).

The WCAG contain information about how Web content (e.g., textual information, pictures, and other parts of a web page) should be made accessible. The guidelines include information and techniques on how things should be done. The current version of the guidelines is 2.0, which was published in December 2008. This version supersedes the original 1.0 guidelines released in May 1999.

The WCAG 2.0 divides its twelve guidelines into four principles: perceivable, operable, understandable, and robust. Each guideline has success criteria with different levels of success from the lowest, A, to the highest, AAA. These guidelines were written in such a way so they could be automatically tested. This can make it difficult for a non-developer to understand the guidelines.

With the introduction of technologies like AJAX for viewing a web page and generating dynamic content, some additional work was needed to make items accessible. The result is the WAI-ARIA (or simply ARIA) that in an attempt at developing a protocol between browsers, assistive technologies, and developers of new web libraries and technologies. The only disadvantage with the WAI-ARIA is that it is still being developed. There are working drafts available for most of the parts, but support among
browsers and assistive technologies are still in the earlier phases.

The information contained in the ATAG is targeted at developers building tools for authoring content on the Web. This includes things like “What You See Is What You Get” (WSYWIG) editors in wikis, blogs or email programs on the Web, desktop applications that generate content, multimedia tools, or site management tools. Basically, anything that allows you to generate content that will eventually end up on the Web. The guidelines are divided up into checkpoints with a priority of 1 (essential) to 3 (beneficial). Conformance (A–AAA) is then judged based on how many of the checkpoints are met. ATAG 1.0 is the current standard and was finished in February 2000. The 2.0 standard, which should include updates to be more in-line with the WCAG 2.0, is expected to be ready in 2011.

The final standard we will mention here is the UAAG, which defines how to create accessible user agents. A user agent can be any sort of browser or media player. The UAAG is laid out in a similar method to the ATAG; each guideline has checkpoints with a similar 1 to 3 priority for how they should be addressed. It also has a 1.0 version to correspond with WCAG 1.0 and is being updated to a 2.0 version to better match the WCAG 2.0. The WAI claims it might be done in 2010, but it looks like that isn't going to happen.

Other Standards

One important standards in the United States is the Section 508 standards. The United States Government uses these standards when making decisions in how to distribute information and purchase equipment and services.

Current Technologies on Mobile Platforms

For simplicity, we'll look at the accessible technologies that are available on mobile platforms, specifically mobile phones, but we'll also take a look at other mobile devices.

Mobile Phones

In areas like Scandinavia, it can be taken for granted that nearly everyone has a mobile phone—including people who have some sort of disability. In this section we do a quick survey over the different methods available for accessing a mobile phone. We'll look at the current popular brands based on operating system. We work with the assumption that the devices themselves have necessary parts that make them accessible (such as bumps on buttons to indicate certain buttons, an ability to find proper sides of the device, etc.).

Android

Android provided accessibility support starting with version 1.6 of its operating system and has improved support since then. There are currently several accessibility aids that provide spoken (TalkBack), auditory (SoundBack), or haptic (KickBack) support. There is also an API available for developers to ensure that their applications are accessible. The only issue that may be difficult is getting the accessibility turned on for the phone in the first place.

iOS

Since the summer of 2009, Apple's new iPhones, iPads and iPod Touchs include a screen reader and other accessibility features such as high contrast white on black, voice control, and zoom by default. The only requirement is that someone has to turn it on. Apple also provides developers with an API and tools for checking that their application is accessible.

Symbian

Symbian phones provide some built-in accessibility features, but items such as a screen reader must be purchased separately. Currently, there are two screen readers for Symbian (MobileSpeak by Codefactory and Nuance Talks). There is no API for third-party developers to ensure their applications are accessible.
WebOS
There currently are no assistive technologies for WebOS devices. Since applications on these devices use a combination of HTML and JavaScript, it should be possible to follow guidelines like the WCAG to make applications accessible when assistive technologies become available for these devices. There has been some preliminary work on some text-to-speech, so it is only a matter of time before WebOS gets this functionality.

Other Devices
Since operating systems like Android, iOS, and WebOS are used in devices besides phones, their accessibility technologies can be used on them as well.

When it comes to things like RFID or NFC there's nothing inherently inaccessible about them „out of the box.” It's more how they are used. For example, in can be difficult to use an RFID when the places for validating them all are different and not easily locatable.

Current Laws
In the EU, probably the most interesting item regarding universal design and technology is the Riga Declaration from June 2006 (IP/06/769). The declaration sets up goals for providing Internet access to everyone. This includes ensuring that public websites are accessible (set as a goal for 2010).

In Norway, this declaration is manifest in the Diskriminerings- og tilgjengelighetsloven (Discrimination and accessibility law). In particular of interest which is section 11, which spells out rules for technologies and systems. Section 11 states that from the July 1st, 2011 new systems that are used by the public must be universally designed; all existing systems must be made universally accessible by January 1st, 2021. For web sites, this means that they must handle all AAA and AA items in the WCAG 2.0.
6. Security and privacy in the IoT

We have seen above that security and privacy play an essential role, when it comes to trust in IoT. This chapter is focusing on these, and their relation to trust and IoT.

Any work that has to deal with security as either a partial or a main focus must raise the same question first: what does “secure” mean in this context?

To have a useful approach considering a certain system or environment of our target, several classification practices decompose the notion of “security”. Besides the common and general aspects of security (CIA: Confidentiality, Integrity and Availability) we can also categorize threats, e.g., with Microsoft’s STRIDE model: the six letters in STRIDE each represent a particular risk. These are used in security bulletins to describe the nature of a security vulnerability.

- **Spoofing Identity** means illegally obtaining access and use of another person’s authentication information, such as a user name or password, that is, impersonate another user.
- **Tampering with data** means malicious modification of data. An attacker who maliciously changes data is often much harder to detect, and does much more damage, than a smash-and-grab Web site defacer or disk reformatter. Why? First, you might not find the modified data until some time has passed; once you find one tampered item, you’ll have to thoroughly check all the other data on your systems to ensure that nothing else was tampered with.
- **Repudiation** represents the risk that a legitimate transaction will be disowned by one of the participants. **Non-repudiation** means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively.
- **Information disclosure** means that an attacker can gain access, without permission, to data that the owner doesn’t want him or her to have.
- **Denial of service (DoS)** means an explicit attempt to prevent legitimate users from using a service or system. It involves the overuse of legitimate resources. You can stop all such attacks by removing the resource used by the attacker, but then real users can’t use the resource either.
- **Escalation of privilege** means an unprivileged user gains privileged access. An example of privilege elevation would be an unprivileged user who contrives a way to be added to the Administrators group.

(from [http://teck.in](http://teck.in))

This classification method is intentionally unspecific, but at the same time lends a good startup for examination. In order to enable this, let us now take a close look at the Internet of Things. [Mayer 2009] organizes IoT features into “topics” as follows:

![Diagram of IoT topics](image)

**6-1 Topics in the IoT context**
Going behind these topics, we find a host of technologies and practices implementing these very „building blocks” of IoT. We can also easily see that RFID spans multiple topics (which was the fact that probably led to the misbelief that IoT is not more than versatile usage of the RFID technology):

6.2 Comprehensive map of topics and technologies related to current IoT, emphasizing the important but not exclusive role of the RFID technology

Now that we have general topics, and that we decomposed IoT in such a way, let us bring this together with security again, and answer the question: how sensitive are these topics to security and privacy? The table below summarizes the results of such reasoning, displaying security properties as columns and IoT topics in the rows.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Integrity</th>
<th>Authenticity</th>
<th>Confidentiality</th>
<th>Privacy</th>
<th>Availability</th>
<th>Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>+++</td>
<td>+++</td>
<td>+++</td>
<td>++</td>
<td>+++</td>
<td>+</td>
</tr>
<tr>
<td>Sensors</td>
<td>+++</td>
<td>+</td>
<td>+</td>
<td>+++</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Actuators</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Storage</td>
<td>+++</td>
<td>+++</td>
<td>+++</td>
<td>+++</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>Devices</td>
<td>+++</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+++</td>
<td>++</td>
</tr>
<tr>
<td>Processing</td>
<td>+</td>
<td>++</td>
<td>+</td>
<td>+++</td>
<td>+</td>
<td>+++</td>
</tr>
<tr>
<td>Localization/Tracking</td>
<td>+</td>
<td>+</td>
<td>+++</td>
<td>+++</td>
<td>+++</td>
<td>++</td>
</tr>
<tr>
<td>Identification</td>
<td>++</td>
<td>+</td>
<td>+++</td>
<td>+++</td>
<td>+++</td>
<td>++</td>
</tr>
</tbody>
</table>

6.3 Sensitivity of the topics to security and privacy
Examples:

- Communication has high sensitivity to confidentiality (I don’t want others to read my data)
- Sensors have low sensitivity to confidentiality (can always place my sensor near and sense the same physical property, therefore sensing in itself is not confidential)

It is one understanding to decompose IoT into technologies and define and measure its security by the security properties of the technologies it consists of. However, [Mayer 2009] eventually states that looking at topics, not directly at technologies can make it easier to develop a Security & Privacy model, and encourages construction of generic S&P mechanisms to mitigate the risks and increase security within the IoT.

In the following sub-chapters, we move forward by introducing the concept of adaptive, autonomic and evolving security, after which we come to dynamic/adaptive security policies.

6.1.1 Adaptive, Autonomic and Evolving Security

**Adaptive security** refers to a security solution that learns and adapts to the changing environment during run-time in the face of changing threats, and anticipates threats before they are manifested. **Autonomic security** refers to the application of the idea of flexibility to the security space itself, which involves automating reconfiguration of the protection mechanisms, resulting in a self-protected system running with minimal user intervention. **Evolving security** refers to the modification of existing security functions and the generation of new functions for long-term adaptivity in a non-disruptive way.

**Adaptation forms:** Adaptation can take the form of parameter adaptation in which adaptation is achieved by specific variations in the control parameter vector, structure adaptation in which adaptation is achieved by dynamic changes in the structure of the system, goal adaptation in which adaptation is achieved by formally defining specific constraints on the state of the system, or by any combinations of these. Adaptation can take place at any layer or cross-layers, i.e., vertical cooperation among multiple system layers, horizontal cooperation among multiple platforms, and universal adaptation - combination of vertical and universal adaptation [Samimi 2004].

**Special Requirements for Adaptation:** The special requirements for adaptation are that the adaptive algorithm must respond to changes in the system on the fly, the activities of the adaptive algorithm must cause only minimal deviations from the normal mode of operation of the system, and the adaptation must address the reconfiguration of functional logic, the reconfiguration of the architecture as a whole, and the handling of conflicts. Some notable obstacles to the implementation of adaptive algorithms are the complexity of the correct definition of goals and restrictions, the necessity for the on-going identification of both system and environment, and the required minimum reaction time of adaptive algorithms. Among those methods proposed in [Shnitko 2003] are redundancy and optimization, the usage of expert and analytical data, and special algorithms from Control Theory.
Driving Factors and Needs for Dynamic Adaptation: The driving factors for adaptation are (i) the convergence of advanced electronic technologies (wireless, handheld, sensors, etc) and the Internet, (ii) the promise of instant access to data and computing no matter where or when, (iii) the changing nature and behavior of the environment, and (iv) the need for systems to operate in the face of failures and attacks. The need for dynamic adaptation is due to (i) the heterogeneity of hardware, network, software, etc., (ii) the dynamics of the environmental conditions, especially at the wireless edge of the Internet, (iii) the limited resources (such as battery lifetime), and (iv) the software adaptation technologies for detecting and responding to environmental changes, and strengthening self-auditing capabilities of “always-on” systems [Samimi 2004].

Advantages and disadvantages of Adaptivity: Adaptivity has a number of advantages in a security context. It contributes to real-world security with fuzzy definitions and under uncertain conditions. It affords access to methods and tools from Control Theory. It provides solutions to the problem of limitations in the robustness and resilience of a system, and its performance. Finally, it provides a solution that learns and adapts to changing environments during run-time in the face of changing threats without significantly sacrificing the efficiency, flexibility, reliability and security of the system. This improves the reliability, robustness and dependability of critical systems and infrastructures. Adaptivity has a number of potential positive impacts [Samimi 2004], [Abie 2009]. It can increase the robustness of group communication between users with disparate devices and networks. It can provide secure self-healing systems that support mission-critical communication and computation under highly dynamic environmental conditions, and self-auditing systems that can report the state inconsistencies, and the incorrect or improper use of components. It can allow the allocation of resources securely and dynamically in devices limited by battery-lifetime, bandwidth, or computing power. It can allow the systematic secure evolution of legacy software so that it can accommodate new technologies and adapt to new environments. It can also enable systems to operate through failures and attacks. Adaptivity does have a few disadvantages. It depends for its effectiveness on the correct definition of security goals, it requires additional resources to carry out the adaptation processes, and it is not always able to ensure only minimal deviations in the system’s normal mode of operations during adaptation.

6.1.2 Dynamic/Adaptive Security Policies

Security policy is a definition of what it means to be secure for a system, organization or other entity (Wikipedia).

In internet of things (IoT) due to the mobility of users/things/agents, things/agents cannot be predetermined and resource availability frequently varies, even unpredictably, which complicates the specification of policies and resource access controls. Furthermore policies cannot be defined based on entity’s identities/roles, "as in traditional security solutions, or be specified a priori to face any operative run-time condition and require continuous adjustments to adapt to the current situation." [Toninelli 2007]. Therefore an adaptive and holistic approach of policies is needed.

A holistic approach to adaptive security policy (including service level agreement) management comprises technical, operational, market mechanisms and administrative controls and the required assessments to establish their efficacy in managing policies adaptively. An adaptive policy management is a system which is capable to learn, adapt, prevent, identify and respond to unknown threats in critical time. It allows the development of dynamic models that attempt to make predictions about the impacts of alternative policies. It can also provide an adaptive policy approach to dealing structural uncertainty in security policymaking, i.e. security policies will be adjusted as the world changes and as new information becomes available by taking those actions now that cannot be differed, preparing to take actions that may later become necessary, monitoring changes in the world, and taking actions when the monitoring process shows they are needed. Such dynamic models are best implemented using smart agents.
Existing smart agents/things have introduced methodologies for negotiating policies, service level agreements and semantics, and for calculating trust and trustworthiness. However, the lack of self-protection against malicious attacks and/or the leakage of sensitive information during negotiation are challenges in existing approaches. Future study should improve the abilities of the smart agents to detect in real-time unknown threats, respond to them, and adapt to the complex environment and changing degree of security policy breaches by the introduction of new self-protecting protocols, adaptive policies, newly gained knowledge, and metrics for quantitative security assessment and predicative security, guided by objectives and needs of stakeholders.

Here we give a brief survey of the state of the art research on technologies that address the need for dynamic adaptation of policies.

Liu et al. [Liu 2008] have developed a dynamic policy based network management scheme in mobile environment that adapts parameters dynamically according to changes of network states, and applied it to resource allocation in mobile environment to improve the availability of the network thus increasing the efficiency and flexibility of mobile network management. Chatterjee et al. [Chatterjee 2009] have developed a hybrid access control framework that integrates dynamic policy-based access control and for trust-based based access control in P2P applications that introduces multi-levels and unequal roles for Peers at each level in self-organizing groups and Peers are permitted to collaboratively frame and modify policies at various levels. Dunlop et al. [Dunlop 2001] have introduced a dynamic policy model for the management of large, open evolving enterprises. The model includes novel concepts in support of enterprise including enterprise domain, policy space and policy authority that are helpful to support dynamic policy-based management and is able to cope with the high rate of change inherent in such environment. Naldurg et al. [Naldurg 2002] have described a framework for constructing dynamic policies. Through policy development lifecycle the model uses suitable formal notations and methods for the specification, verification and validation of these policies. Quinn et al. [Quinn 2006] have explored the creation and use of dynamic policies that had trust conditions embedded through the introduction of trust meta-policies that expose the trust conditions explicitly. Abie [Abie 2009] and Abie et al. [Abie 2010] have developed adaptive policy management for adaptive security and trust management for messaging middleware for business critical systems, and dynamic resilience policy for optimal mirroring message brokers to minimize the quantified risk of overload to the system in cases of surges in demand or attack. Walker et al. [Walker 2001] suggested an adaptive policy approach that allows policymaker to cope with the uncertainties that confront them by creating policies that respond to changes over time and that make explicit learning. The authors state that this approach implies fundamental changes in what they call the three major elements of policymaking: the analytical approach, the types of policies considered, and the decision-making process, and describe in detail their rationale. Toninelli et al. [Toninelli 2007] present a semantic context-aware adaptive policy model that enables dynamic adaptation of policies depending on context changes by combining two design guidelines, i.e., context-awareness which allows operations on resources based on context visibility and semantic technologies which allow the high-level description and reasoning about context/policies. Bahati and Baur [Bahati 2009] explored how reinforcement learning in adaptive policy driven autonomic management model can be adapted to accommodate changes such as “whether a model 'learned' from the use of one set of policies could be applied to another set of 'similar' policies or whether a new model must be learned from scratch as a result of changes to an active set of policies?” The authors have demonstrated the value of reinforcement learning in enabling an autonomic management system to improve its use of policies.

In the world of IoT there is a need for advancing these by integrating policy management, trust management and risk management as a synergy framework for the automated management of dynamic policies that will adapt to changing environment (threats, requirements, new services, or stakeholders) with appropriate metrics for measuring the efficiency and effectiveness of automated policy solutions. Such an integrated policy management model should define three levels of policies: A global policy for general management of system-wide smart agents, group policy that only applies to a group of smart
agents, and local policy that only applies to a particular smart agent and contains an application specific policy. The group and local policies inherit the properties of the global policies. These adaptive policies can be designed to function more effectively under complex, dynamic and uncertain conditions and will anticipate the array of future conditions through robust up-front design using (a) integrated and future-looking analysis (b) multi-stakeholder deliberation and (c) by monitoring key performance indicators to trigger automatic policy adjustments. The effect of this synthesis and combination is to increase the strength of the security of and the degree of trust in the policy system, and to reduce the rate and severity of compromises and leak of policy information.

6.2 Current technologies and best practices for achieving security and privacy

In this chapter a selection of the most important technologies establishing security and privacy are introduced. As uTRUSTit’s primary focus is not on achieving security and privacy itself, but to consolidate trust in the user that such aspects are well taken care of, the following subsections do not aim to go deep in technical details, but to give an overview on what types of measures are typical and usual today in the field of security and privacy.

6.2.1 Firewall and Intrusion Detection Systems

A Firewall is a computer, router or other communication device that filters access to the protected network. Cheswick and Bellovin define a firewall as a collection of components or a system that is placed between two networks and possesses the following properties:

- All traffic from inside to outside, and vice-versa, must pass through it.
- Only authorised traffic, as defined by the local security policy, is allowed to pass through it.
The firewall itself is immune to penetration.

6-5 Firewall Schematics

Such traditional network firewalls prevent unauthorised access and attacks by protecting the points of entry into the network. As Figure 1 shows, a firewall may consist of a variety of components including host (called bastion host), router filters (or screens), and services. A gateway is a machine or set of machines that provides relay services complementing the filters. Another term illustrated in the figure is "demilitarised zone or DMZ". This is an area or sub-network between the inside and outside networks that is partially protected. One or more gateway machines may be located in the DMZ. Exemplifying a traditional security concept, defence-in-depth, the outside filter protects the gateway from attack, while the inside gateway guards against the consequences of a compromised gateway. Depending on the situation of the network concerned, there may be multiple firewalls, multiple internal networks, VPNs, Extranets and perimeter networks. There may also be a variety of connection types, such as TCP and UDP, audio or video streaming, and downloading of applets. Different types of firewall configuration with extensive practical guides can be found in. There are also many firewall products on the market from different vendors. See for an updated list of products and vendors. (from: Abie, H. An Overview of Firewall Technologies)

The Intrusion System (IDS) is traditionally deployed to monitor traffic in vital segments in the network, generating alerts when an intrusion is detected. The importance of the IDS has grown significantly as the industry recognizes that 90 percent of attacks in recent years have exploited application vulnerabilities. The traditional stateful inspection firewall, based largely on matching packet header information against Access Control Lists (ACLs), is ineffective to fend off such attacks. A good IDS, on the other hand, can expose these application layer attacks.

But detection alone is insufficient—it is also important to terminate the attack upon detection. Hence, the trend is to evolve the IDS into an Intrusion Prevention System (IPS), which takes detection to the next level and stops the detected attacks, including application attacks.

In addition to the IDS/IPS, application content security arsenal in an enterprise may also include antivirus, anti-spam and content filtering devices.

6.2.2 Virtual Private Networks

Virtual Private Networks (VPNs) have become a critical security tool for higher education institutions as an increasing number of professors, staffers and students require access to the campus data network over the Internet. VPNs allow IT departments to create a private tunnel over the Internet, so remote users or users in satellite campuses can securely connect and transmit data to the main campus’ local area network (LAN). VPNs authenticate users and then encrypt the traffic between their computers and the college network.
The two dominant VPN technologies — IPSec (Internet Protocol Security) and SSL (Secure Sockets Layer) VPNs — have their strengths and weaknesses. Some educational institutions have deployed one or the other, while other colleges are choosing to take advantage of both, giving their diverse community of users multiple ways to connect to the campus network.

To help you determine which VPN works best for your campus, this white paper will explain the different VPNs available, their advantages and disadvantages, and the latest technological advances.

**VPN’s Role**

VPNs have two common uses: remote access for users and site-to-site connectivity. There are two types of site-to-site connections. An intranet VPN links users from satellite offices to the main network, while an extranet VPN connects outsiders, such as partners, contractors or suppliers, to the LAN.

In the past, before the Internet explosion, universities and colleges had limited ways to extend their LANs beyond their campus’ boundaries, and those methods were either difficult to manage or cost prohibitive. Colleges, for example, subscribed to costly leased lines to connect different sites together. They also installed remote access servers, featuring modems that users dialed into to connect to the LAN. But the Internet’s growth has changed everything. In the 1990s, the technology industry introduced VPN technology using IPSec as a more cost-effective way to connect offices in different locations. Enterprises also began using IPSec for remote access for individual users. An IPSec VPN requires users to download, install and configure a software client onto their computers before they can establish a secure connection with their campus networks. Today, IPSec VPNs have the largest installed base because it was the only VPN technology available for the longest time. In recent years, a new VPN technology that uses the SSL protocol has captured the limelight and seen its market share skyrocket. The biggest benefit of SSL VPNs is ease of use. Instead of requiring users to install a separate software client, SSL VPNs allow users to connect through standard Web browsers. SSL is an encryption technology that is embedded in browsers, such as Internet Explorer and Firefox. With VPNs, students can get secure remote access to their e-mail and also get personal files from their departments’ file servers and library servers. They can even send print jobs to campus printers. Likewise, staffers can connect to critical business applications and data, while faculty can access online gradebooks and other educational applications. VPNs can also bolster security for open-campus Wi-Fi networks. They can protect voice traffic for colleges that have deployed Voice over Internet Protocol (VoIP) and allow professors and staffers to access their office phone numbers from home or while traveling. VoIP transmits digitized voice as a stream of data, so it’s protected by encryption like other data packets.

Today, institutions of higher education house tremendous amounts of sensitive and private information, from students’ financial and educational records and faculty research data to employees’ Social Security numbers. IT administrators face a difficult task in securing the network, while simultaneously providing the remote access that its diverse community of users need. For optimal security, IT departments must deploy layers of security throughout their technology infrastructure, and VPNs play a huge role through their ability to create secure tunnels between users’ computing devices and campus servers. Whether you choose IPSec, SSL or both, the result is secured data transmissions for remote users. (from: Virtual Private Networks – Improving network security for a diverse user community – White paper)

### 6.2.3 Digital Rights Management (DRM)

In today’s fast-changing digital environment and future Internet where global communications transcend national boundaries, and where digital products are sold on an international market, the development of DRM in order to protect Intellectual Property Rights (IPR) is still an increasingly important global issue, and is a formidable challenge since the different national laws, policies and practices must interoperate and be reconciled. IPR governs the commercial and legal relationship between the seller (owner) and the buyer (user) of certain IPR-based products. DRM is a complex and multifaceted concept which is affected by many disciplines which it, in turn, affects [Abie 2007]. IoT research should investigate and
address those factors that impact on and affect the uptake and economics of DRM: technology, business models, policies and laws, and societal issues.

**Business issues:** The process of DRM includes a number of different business models ranging from the secure sharing with employees, partners and clients of content for business collaboration, to conducting electronic commerce where trust is absolutely, hence different trust models must be researched and integrated with the DRM model. Therefore, we shall investigate how a DRM solution can be made flexible enough to adapt itself to different business models, to support any changes in the business models and to work for the new emerging business models [Jamkhedkar 2005].

**Privacy and identity management issues:** Consumers are still worried about their privacy, and this unfortunately well-founded concern inhibits the growth of e-commerce. IoT research should therefore investigate how a DRM system can ensure the protection of consumer privacy, and enable consumers to control how personally identifying information is obtained, and used or distributed. Robust identity management (IdM) for the identification and description of object and subject is an essential part of DRM. Since static IdM architectures are not able to maintain the IdM constraints or the proper balance between security of IdM and performance in rapidly changing environments, the investigation and adoption of Adaptive IdM (AIdM) in IOT can play a pivotal role in this connection by being able to adapt to ever-changing threats and identity information such as contexts (personal, social, enterprise, commerce, government, etc), meta attributes (privacy, policies, validity, access, trust, security, etc), and controllers (owner, known third party, unknown third party, etc). Digital policy management is concerned with the design, analysis, implementation, deployment and use of efficient and secure technology that handle digital information in accordance with the relevant rules and policies. Therefore, different business, trust, security, privacy and AIdM policies can be developed and integrated into DRM systems.

**Risk management issues:** The improvement in decision making and the implementation of policy depends on an improved risk analysis, assessment and management processes. Therefore, DRM systems can be extended with a specialized and improved adaptive risk management module containing a risk management process and risk analysis and assessment methodologies.

**Trust issues:** Trust is one of the most important elements in human relationships, a critical basis for consumer-to-provider relationships, to wit providers need to establish trust and confidence in their products and services, and consumers need to protect their privacy and information, and assess the trustworthiness of their providers. Therefore effective trust management is vital to the acceptability of DRM-enabled applications and businesses in future IoT systems. This includes, among other things, (a) the development of formal social cognitive theories of trust and reputation, and the exploration of the role of reputation in the evolution of altruism and co-operation in human societies, (b) the facilitation of the emergence of widely acceptable trust management processes for open DRM systems and applications, and (c) the exploration of the role of attitudes towards a DRM-based transaction, which is defined as the overall evaluation of the desirability of a DRM-based transaction as experienced by an agent. The salient goal of this is to develop a trust model that will help each IoT user to judge whether authenticity and provenance evidence of the transaction make a digital content sufficiently trustworthy and economically useful.

**Societal issues:** There is a balancing act between the rights of the provider or rights holder and the end-user in the perspective of society, where promotion of electronic trade may be a separate policy objective. Societal questions include privacy, information access, digital divide, fair-use, private-use, community-use, cultural issues, freedom of speech, and societal acceptance and awareness or customer’s benefits from DRM. It follows from this that any true understanding of DRM must be holistic and broad not only to derive the full benefit of the current uptake of DRM, but also to gain insight into the future of DRM-enabled networked IoT digital media.
It is evident from the above that the synergy effect of all these must be investigated, evaluated, formalized and exploited if any future IoT IPR business is to flourish [Zhang 2009], [Abie 2007]. Doing so will enable society and the market to evaluate and discover by experiment what is most useful and best for ensuring balance between the interests of all concerned parties [Varian 2007], and to determine mechanisms for ensuring interoperability, compliance, and the evolution of DRM-based IoT systems.

### 6.2.4 Privacy Impact Assessment (PIA)

ISO 22307:2008 provides a privacy impact assessment structure (common PIA components, definitions and informative annexes) for institutions handling financial information that wish to use a privacy impact assessment as a tool to plan for, and manage, privacy issues within business systems that they consider to be vulnerable.

ISO 22307:2008 recognizes that a privacy impact assessment (PIA) is an important financial services and banking management tool to be used within an organization, or by “contracted” third parties, to identify and mitigate privacy issues and risks associated with processing consumer data using automated, networked information systems.

ISO 22307:2008 describes the privacy impact assessment activity in general, defines the common and required components of a privacy impact assessment, regardless of business systems affecting financial institutions, and provides informative guidance to educate the reader on privacy impact assessments.

A privacy compliance audit differs from a privacy impact assessment in that the compliance audit determines an institution's current level of compliance with the law and identifies steps to avoid future non-compliance with the law. While there are similarities between privacy impact assessments and privacy compliance audits in that they use some of the same skills and that they are tools used to avoid breaches of privacy, the primary concern of a compliance audit is simply to meet the requirements of the law, whereas a privacy impact assessment is intended to investigate further in order to identify ways to safeguard privacy optimally.

ISO 22307:2008 recognizes that the choices of financial and banking system development and risk management procedures are business decisions and, as such, the business decision makers need to be informed in order to be able to make informed decisions for their financial institutions.

(From [ISO 22307:2008])

### 6.2.5 Privacy enhancing technology (PET)

Privacy enhancing technology (PET) is a family of components that provide technical solutions for privacy protection, transparency and control in systems that process personal information (PI). Originally designed to hide communication relationships, PETs today offer a wide variety of technical functions that help PI processing systems to meet privacy goals. The presence of PETs, and their visibility to and perception by the end users is an important factor in gaining trust. Especially in the IoT, where the ownership, function and purpose of other ‘things’ are not always clear to the end users, the presence and perception of PET components can have a strong impact on user trust into the ‘things’. The following sections motivate the subject of PETs, illustrate the background they have been created from, and provide an overview of existing PET approaches. It finishes with an outlook into a specifically important aspect of the IoT and trust – location privacy and how it can be guaranteed using PET.
6.2.5.1 Technology for protection of privacy - a brief history

PET as a research topic has been opened by David Chaum in 1981. In [Chaum 1981], he describes a method for anonymous and unobservable delivery of electronic messages called „Mix“. Chaum uses security protocols and subsequent layers of encryption to provide privacy protection by „mixing“ several people’s e-mail traffic in encrypted form. The concept later was implemented in the MixMaster e-mail anonymization system [MCP 2004], which is the first practically available PET system. The appearance of technological measures for privacy protection coincides with strengthening legal regulation of the use of personal data on information systems. Starting in the 1970ies, regulatory regimes were put on computers and networks. Starting with government data processing, along the lines of computerization of communication and workflows, explicit rules like the European Data Protection Directive [Eur 2002] have been put in place. With the adoption of Internet and mobile telephony in society in the past decade, the privacy challenges of information technology came to everyday life. Hence in the 1990ies, research efforts on PET increased, with Chaum’s concept being adapted to internet data traffic [Pfitzmann 1986] (PPW1991), [Goldschleg 1996] and call routing in ISDN [Jerichow 1998] or mobile telephony [Federrath 1997].

Along with several publicly funded research projects [Lacoste 2000], [PRIME 2003], (FID2003), several companies turned privacy protection into a business model (Anonymizer.com, Zeroknowledgesystems.com, dossier services, XeroBank, Anti-Spyware, Virus tools). Researchers investigated cryptography and information hiding technology to produce privacy-supporting protocols such as anonymous credentials [Camenisch 2002]. A milestone in this development is the appearance of a „Handbook on Privacy-Enhancing Technologies“ [Blarkom 2003] written by representatives of the regulatory authorities, not by PET researchers or technicians.

With the globalization of the economy and the IT infrastructure supporting it, in the years staring the 3rd millennium privacy management has turned into a matter of corporate governance and compliance, with legislation targeting this issue (in various directives, e.g. [Eur 2002], see [Buchta 2004] for more legal references ). Standardization bodies and interest groups such as ISO [Bramhall 2007], W3C and IETF (Müll2004) initiate privacy technology standardization work. Global players such as IBM and HP target corporations with their privacy compliance services related to the IBM Tivoli and HP Select product lines. In this context, recent efforts on using Trusted Computing [TCG 2007] to implement privacy-compliant data handling [Chaum 1981] show the path to the future of information privacy as a matter of compliance.

The PET research perspective was mostly on the legal foundations of privacy protection, determined by constitutional and fundamental human rights that should be protected using technology. This view is shown in an analysis of the PET vocabulary in [Koch 2006]. As rights are granted to individuals, much of the research has focused on the user-side, e.g. visible in a well-quoted terminology paper [Pfitzmann 2007]. The legal view is propagated into contemporary frameworks like the Canadian [Treasury 2002] and Dutch [Coo2001] privacy legislation, which both define privacy audit schemes with detailed
procedural definitions and responsibilities, but neglect to provide a decision support method for managers that would enable them to make feasible decisions about privacy needs based on quantifiable risks. Most of these criteria, including schemes like Datenschutz-Gütesiegel [Una 2003], provide checklists with questions for the auditors. They inherently call for competent and “well-paid” external experts when they are used by a company, but are rarely based on empirical data or metrics. The PET award winning taxonomy of privacy [Solove 2006] is very visibly structured along the legal view on privacy.

A recent interest in economics research picks up a different view on privacy. The cost of privacy management, the inherent value and cost of privacy for both businesses and users are modeled and studied. Varian examined the economic relevance of personal information in [Varian 1996]. He also presents basic transactions with personal information that are relevant. Laudon examined the market for personal information and proposed a national market for personal information in [Laudon 1996a] and [Laudon 1996b].

He cared for information trade with some control aspects. In addition, some of the costs of too little and too much privacy are discussed with their relevance to the information market. Some practical insight to Laudons market can be gained in Rubin & Lenard’s summary of the market for personal information in: [Rubin 2001]. The authors study players on the information market in detail, their effects on consumer privacy and the effects of privacy regulation on the United States of America information market. A transaction cost view of privacy is examined by Sholtz in [Sholtz 2003] and [Sholtz 2001]. Sholtz creates an analogue between transactions cost on environmental pollution and privacy. Kahn et al develop an economic model for privacy transactions in [Kahn 2000]. Another economic issue is quality signaling. No work on signaling of privacy properties in relation to economics exists, but Backhouse et al show in [Backhouse 2004] that there can be a Lemons Market for PKI in the absence of strong quality signals. It seems very likely to be the case with expensive privacy infrastructures, but has not been researched.

Much work has been done by Acquisti to find empirical foundations for the economic valuation of end-user privacy [Acquisti 2004], [Acquisti 2002]. Steps toward business cases for PET have been undertaken in [KPMG 2004] and [Clarke 2007]. Both papers suggest a view on value gained through PET deployment. [Fritsch-Abie 2008]

6.2.5.2 Overview of Privacy Enhancing Technology

Privacy enhancing technology (PET) is about the protection of privacy in information systems. The term privacy is used in many contexts, and with many possible interpretations. In the context of PET, privacy is either viewed from a legal view – by the data protection community. Or it is viewed as a technical challenge to information security, which relates to the cryptography and computer security community. The specific challenges in information privacy are described in D. Solove’s “A Taxonomy of Privacy” (Solove 2006), which has won the 2006 PET award. Here, the four basic challenges of information privacy are found to be:

1. Information Collection – The collection of personal information by some party.
2. Information Processing – The processing of personal information by some party.
3. Information Dissemination – The distribution of personal information by some party.
4. Invasion of privacy – Intrusion of private spaces – Influencing decision
Solove describes the four areas in further detail, whereby he identifies particular actions that produce threats to privacy (see 3-9).

A classification of privacy risks and the cost induced by these risks has not been done in convincing ways. Privacy risks are not well defined in the literature. Too low quality of a particular protection technology might destroy particular applications, as Friedmann shows in [FriedmannResnik 1999]. In [Gellman 2002], the business and consumer side of privacy risks and costs is examined. The author classifies risks and provides an example with monetary figures on how much cost is imposed on the average U.S. family through privacy breaches. The suggested risks are listed in Table 1. Noteworthy is the distinction in risks not only to the consumer, but also to businesses. Odlyzko agrees that a lack of privacy in consumer commerce settings leads to financial losses due to price discrimination [Odlyzko 2003].

<table>
<thead>
<tr>
<th>Businesses</th>
<th>Consumers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Losses Due to Lack of Privacy</td>
<td>Higher Prices</td>
</tr>
<tr>
<td>One Retailer’s Loss Is Another Retailer’s</td>
<td>Junk Mail, Telemarketing</td>
</tr>
<tr>
<td>Opportunity</td>
<td>Identity Theft</td>
</tr>
<tr>
<td>Lost International Opportunities</td>
<td>Internet Effects</td>
</tr>
<tr>
<td>Increased Legal Costs, Investor Losses</td>
<td>The Dossier Society</td>
</tr>
</tbody>
</table>

Table 1 – Privacy risks from [Gellman 2002]

**Terms and Definitions**
Terminology in the PET community is sometimes confusing. This section defines the most important terms and concepts that are used in this report. They are mostly taken from or inspired by Hansen & Pfitzmann’s long-term terminology effort [PfitzmannHansen 2003], which is also a good source for the translation of the terms into many other languages beyond English.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymity</td>
<td>Anonymity means that a subject is not identifiable within a set of subjects.</td>
</tr>
<tr>
<td>Identity</td>
<td>A person’s identity is either the person’s self-perception, or the person’s external categorization using attributes that are observable. In the sense of PET, the identity is a set of externally observable attributes and properties that – when taken all together – allow for the identification of a subject among others. The term “partial identity” is used to point out the fact that a subject in a certain role might use – or be identified by – a subset of his personal, externally visible attributes.</td>
</tr>
<tr>
<td>Identity management</td>
<td>Identity management is the process of administration of various partial identities of a subject. Privacy-preserving identity management systems keeps distinct partial identities of a subject separate from each other, and thus unlinkable.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Privacy in the sense of PET is the autonomy of a subject over his personal information. Privacy in information systems hence is the control over personal information that is being released to other parties. Additionally, transparency about what happens with the information at the other party and ways to limit actions on the information is considered a part of information privacy.</td>
</tr>
<tr>
<td>Pseudonym</td>
<td>A pseudonym is an alias name or other form of identifier that removes a subject’s real name, but serves as a means of relating to that subject. Pseudonymity is the state of using a pseudonym as an identifier. Pseudonyms can model roles, transactions, persons, relationships with different degrees of anonymity.</td>
</tr>
<tr>
<td>Unlinkability</td>
<td>Unlinkability of a pseudonym or a subject’s actions refers to a situation where a n actions or appearance of a subject on a system cannot be identified to belong to any other action of this subject.</td>
</tr>
</tbody>
</table>
| Unobservability           | Unobservability means that  
- a data object / transfer is not observable to parties uninvolved in the transaction;  
- the involvement of the subjects in the aforementioned data transfer is not observable to any other parties. |

**Classification of PET systems**

In recent research in the FIDIS project [FIDIS 2003], a functional distinction of privacy and identity protection in transparency tools and opacity tools was introduced [FIDIS 2007]. Transparency tools are intended to create insight into data processing. Their effect is a better understanding of procedures, practices and consequences of personal data processing at a data processor. Because they enhance understanding and visibility, they are called transparency tools. Opacity tools are intended to hide a user’s identity or his connection to personal data that occurs at a data processor. As they hide identities, reduce visibility, or camouflage connections, they are called opacity tools.
This classification originally conceptualized tools as legal framework and technical practice. But its adaption to a technical classification of PET systems only is useful. The distinction is introduced in Table 1.

The distinction above can be further elaborated by the analysis of PET functionality. A study for the Danish Government [MetaGroup 2005] divides privacy technologies in the two groups of “privacy protection” and “privacy management”, where the description of the technologies grouped by the two concepts goes along the transparency-opacity distinction. In Table 2, “privacy protection” lists opacity tools, while “privacy management” aims at the transparency tools. [FritschPET 2007]

<table>
<thead>
<tr>
<th>Transparency tool</th>
<th>Opacity tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definition</td>
<td>Tools that hide a person’s identity or his relationship to data as it is processed by someone else.</td>
</tr>
<tr>
<td>Legal rights to be informed about data processing;</td>
<td>Pseudonymous access to online services;</td>
</tr>
<tr>
<td>Privacy audits.</td>
<td>Election secrecy.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technical example</th>
<th>Transparency tool</th>
<th>Opacity tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database audit interfaces;</td>
<td>MixMaster anonymous e-mail;</td>
<td></td>
</tr>
<tr>
<td>Audit Agents;</td>
<td>TOR anonymizing web surfing;</td>
<td></td>
</tr>
<tr>
<td>Log files.</td>
<td>Pseudonyms.</td>
<td></td>
</tr>
</tbody>
</table>

This classification originally conceptualized tools as legal framework and technical practice. But its adaption to a technical classification of PET systems only is useful. The distinction is introduced in Table 1.

The distinction above can be further elaborated by the analysis of PET functionality. A study for the Danish Government [MetaGroup 2005] divides privacy technologies in the two groups of “privacy protection” and “privacy management”, where the description of the technologies grouped by the two concepts goes along the transparency-opacity distinction. In Table 2, “privacy protection” lists opacity tools, while “privacy management” aims at the transparency tools. [FritschPET 2007]
6.2.6 Privacy-respecting Identity Management

This section will illustrate the interdependence between privacy, privacy technology, information sparcity, data minimization and identity management in the IoT. It uses a location-based services scenario to describe and illustrate the interplay of these concepts.

An excursion into location privacy
Location of „things“ and connected users and services are important in the IoT in many ways. Here, we specifically look at three aspects of location:

1. Location disclosure as a threat, and measures to increase location privacy by using PETs and Data Minimization;
2. Location as part of the security model, e.g. as part of location-based blacklists and distance bounding protocols;
3. Location of the service providers with respect not to distance-bounding problems, but in relationship to a legal system, a financial clearing system, or the participation in some subset of a „cloud“ computing infrastructure.

The following sections will deal with these aspects.

Privacy Enhancing Technology for location privacy in the IoT
This chapter is based on a book chapter and an article:


This section will present a brief overview of the state of the art in privacy technology research, e.g. from the PRIME and FIDIS research initiatives and other scientific efforts. It also reviews the technology available and used in practice.

The protection against location profiling of „things“ and their users has three components: identity protection, camouflage and a legal and social framework for technology regulation. Each of the items will be discussed below.

Following the distinction in section 2.2 of [FIDIS 2005], protective measures are divided in opacity tools and transparency tools. Opacity tools serve the purpose of hiding personal information to enable unobsevable, individual freedom. Transparency tools are used to create open, understandable and fair practices when dealing with personal information.
I.1 Identity protection

A person’s identity should be protected while using location-based services. If the location track is not personalized, it cannot be combined with any other personal data. Furthermore, the amount of data that can be accumulated about a person should be limited. This prevents identity guessing from movement patterns, as described in [FritschP 2007]. Identity management systems with frequent pseudonym changes and anonymous access to services provide to reach these goals. The simplest form of identity management occurs in Figure 3-10. Here, the mobile operator offers pseudonym translation services for the user before the application data traffic is forwarded into cascades of anonymizing MIX [Chaum 1981] nodes (a form of router that denies observers from observing the content and the end points of data communication.

The use of several serialized MIX nodes as a cascade protects the communication from a corrupt single MIX. More advanced identity management approaches introduce policy management. Here, a user can set policy about location forwarding at her mobile operator, and at the same time issue anonymous credentials that identify the policy. The credential then is given to the LBS provider as a voucher. Please note that naive use of pseudonym change mechanisms can reveal all your pseudonyms used with a service though, as illustrated in Figure 3-11. To prevent this from happening, MIX-Zoning will be discussed later in this text (see Figure 3-15). Identity Management can be either an opacity or a transparency tool, dependent on its particular deployment in a context.

I.2 Camouflage

The generation of false information about identity, identifiable movement patterns and time disturbances will provide to protection from unauthorized geographic profiling. Camouflaging technologies exist for a long time, e.g. for MIX technologies with dummy traffic [Diaz 2004]. Early location hiding concepts have been suggested by Gruteser and Grunwald in [Gruteser-Grunwald 2003]. Concepts include:

Temporal cloaking: the time intervals for location queries are regulated to avoid micro-measurement of a user’s position. The concept is illustrated in Figure 3-12.
Spatial cloaking: precision of location information is reduced to a level tolerable by the application, but will not be delivered too precise. This intentional degradation of position precision prevents too precise information collection about a person’s movements on a high-resolution level. Spatial cloaking is illustrated in Figure 3-13.

MIX-zoning: To allow for unobservable change of pseudonyms (and solve the problem from Figure 3-11 with naive pseudonym change), a zone of unobservability is created where users can go to perform their pseudonym change. As soon as many users do this simultaneously, an anonymity set is created. The concept is inspired by Chaum’s MIX [Chaum 1981]. An example of MIX zoning for the purpose of pseudonym change protection is shown in Figure 3-14. Temporal cloaking ads uncertainty to the point in time the position or a person was measured. The relying service using the data does receive a position datum, but only knows this is not the person’s current position but from some time in the past. The usefulness of this approach is limited in terms of privacy protection. Only in contexts where a service tracks a person frequently (e.g. a pollen warning scenario, as used in [Koelsch 2005]), but with coarse requirements on resolution and timing, temporal cloaking seems applicable. Spatial cloaking is effective in circumstances where a tracking service does not require high-resolution position information (e.g. for pollen warning). Here, the information is intentionally degraded to a degree where no daily routine is contained anymore.
Location dummy traffic: MIX zones are effective to protect and obfuscate pseudonym changing event. Unfortunately, MIX zones might not always have enough people in them just at the moment when they are used. To improve on this problem, the concept of dummy traffic in MIX communication can be adapted. Location track dummy traffic is performed with dummy users that are artificially generated location tracks with a certain non-compromising behavior. The dummy pseudonyms are registered with the LBS application, and will be used for pseudonym changes. When a user wishes to change to a different pseudonym, the dummy system ensures that some of his alternative or dummy pseudonyms will cross the user’s path at a rendezvous point, where the change will happen.

The now unused pseudonym takes up a dummy life of its own, in temporary or permanent continuation of the previous path. This mechanism can take up a used pseudonym and carry it around the town virtually. The challenge here is the generation of realistic movement patterns that do not compromise the pseudonym owner by, e.g., entering the town’s red light district. The application of this protection measure is restricted to LBS infrastructures that allow for injection of artificially created position data.
(e.g. the GPS device scenario or some special instance of the intermediary scenario described in [Fritsch 2005]). A model and a prototype have been described in [Rensmann 2007].

6.2.7 RFID privacy and data protection guidelines (e.g. COM/2009/3200)

Below are some aspects and guidelines that are to foster establishing privacy and data protection in systems using RFID technology.

1 Accountability
An organization is responsible for personal information under its control and should designate a person who will be accountable for the organization’s compliance with the following principles, and the necessary training of all employees. Organizations should use contractual and other means to provide a comparable level of protection if the information is disclosed to third parties. Organizations that typically have the most direct contact and primary relationship with the individual should bear the strongest responsibility for ensuring privacy and security, regardless of where the RFID-tagged items originate or end up in the product life cycle.

2 Identifying Purposes
Organizations should clearly identify and communicate to the individual the purposes for collecting, linking to, or allowing linkage to personal information, in a timely and effective manner. Those purposes should be specific and limited, and the organizations and persons collecting personal information should be able to explain them to the individual.

3 Consent
Organizations must seek individual consent prior to collecting, using, or disclosing personal information linked to an RFID tag. To be valid, consent must be based upon an informed understanding of the existence, type, locations, purposes and actions of the RFID technologies and information used by the organization. Individual privacy choices should be exercised in a timely, easy and effective way, without any coercion. Consumers should be able to remove, disable or deactivate item-level RFID tags, without penalty. Automatic deactivation of RFID tags, at the point of sale, with the capability to re-activate, should be the ultimate goal. Consumers should be able to choose to re-activate them at a later date, re-purpose them, or otherwise exercise control over the manner in which the tags behave and interact with RFID readers.

4 Limiting Collection
Organizations should not collect or link an RFID tag to personally identifiable information indiscriminately or covertly, or through deception or misleading purposes. The information collected should be limited to the minimum needed to fulfill the stated purposes, with emphasis on minimizing the identifiability of any personal data linked to the tag, minimizing observability of RFID tags by unauthorized readers or persons, and minimizing the linkability of collected data to any personally identifiable information.

5 Limiting Use, Disclosure and Retention
Organizations must obtain additional individual consent to use, disclose or link to personal information for any new purposes. Personal information should only be retained to fulfill the stated purposes, and then securely destroyed. Retailers should incorporate the data minimization principles outlined above, into and throughout their RFID information systems.

6 Accuracy
Organizations should keep personal and related RFID-linked information as accurate, complete, and up-to-date as is needed for the stated purposes, especially when used to make decisions affecting the
individual.

7 Safeguards
Organizations should protect personal information linked to RFID tags, appropriate to its sensitivity, against loss or theft, and against unauthorized interception, access, disclosure, copying, use, modification, or linkage. Organizations should make their employees aware of the importance of maintaining the confidentiality of personal information through appropriate training. Although physical, organizational and technological measures may all be necessary, technological safeguards should be given special emphasis.

8 Openness
Organizations should make readily available to individuals specific information about their policies and practices relating to the operation of RFID technologies and information systems, and to the management of personal information. This information should be made available in a form that is understandable to the individual.

9 Individual Access
Organizations should, upon request, inform the individual of the existence, use, linkage and disclosure of his or her personal information, provide reasonable access to that information, and the ability to challenge its accuracy and completeness, and have it amended as appropriate.

10 Challenging Compliance
Organizations should have procedures in place to allow an individual to file a complaint concerning compliance with any of the above principles, with the designated person accountable for the organization’s compliance.

(From: [Cavoukian 2009])

6.2.8 Privacy by Design principles

In brief, Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems. This approach originally had technology as its primary area of application, but I have since expanded its scope to two other areas.

In total, the three areas of application are:

(1) technology; (2) business practices; and (3) physical design.

As a broad overarching concept, Privacy by Design encompasses many elements in practice:

1. Recognition that privacy interests and concerns must be addressed;
2. Application of basic principles expressing universal spheres of privacy protection;
3. Early mitigation of privacy concerns when developing information technologies and systems, across the entire information life cycle;
4. Need for qualified privacy leadership and/or professional input; and
5. Adoption and integration of privacy-enhancing technologies (PETs).

(From: [Cavoukian 2009])
6.3 Current technologies and best practices to gain user trust

As an explication of chapter 2.3.2, relevant technologies and practices are introduced for building user trust. Feeding back security and privacy issues to user, as the trust building practice probably most relevant to uTRUSTit, is explained longer in 6.3.1. The subsequent sections will tackle certification and trust chaining, as further examples for such practices.

6.3.1 User feedback

Below is a short on security feedback mechanisms, starting with Android’s built-in solution, followed by such features of today’s most common used web browser applications. The study has been done for the project uTRUSTit and is not a publication yet.

Currently, web browsers and mobile devices can produce both positive and negative security feedback to the user. However, in most cases such feedback contains too much technical information and cannot be easily processed by non-technical end users.

6-14 Security feedback when installing software onto an Android smartphone

Perhaps the best example of trust-related feedback when installing software is the Android approach: when installing software on Android smartphones (as seen on 6-14), a warning window presents the user with a generated list of dangerous activities that the software can potentially do. It is up the user to acknowledge the risks and accept that he trusts the software enough to have these abilities. Modern web browsers can also provide several kinds of positive and negative feedback about the trustworthiness of a particular site (or lack thereof). We examined five of the currently most popular web browsers: Firefox (Mozilla), Internet Explorer (Microsoft), Chrome (Google), Safari (Apple) and Opera.

We checked the reactions of each browser to the following test cases:
- Site has a valid SSL certificate (Class 1)
- Site has a valid SSL certificate (Class 3 – the site also has a ‘verified identity’)
- Site has an expired SSL certificate
- Site has an SSL certificate with an incorrect common name
- Site has a self-signed SSL certificate

Firefox 3.6.8
Firefox distinguishes between “trusted” and “verified” sites. All sites with a valid certificate (or sites where the user confirmed the validity of a problematic SSL certificate) are “trusted”; those with a verified identity are “verified”. The status of a site is readily apparent from the colored bar next to the URL field, which displays a window detailing the site’s security status when clicked (see 6-15). This is a very helpful indicator to the end user about the trustworthiness of a site.

6-15 Firefox trusted and validated sites

The Firefox browser presents a uniform screen when encountering a SSL-related problem (see 6-16). The “Technical Details” section contains a terse description of the problem, but otherwise the nature of the issue is not readily apparent.

6-16 Firefox security feedback when encountering an untrusted site

When adding an exception (see 6-16), the user has to click through several prompts; this does generate more awareness, but can also be annoying to the user.
6-17 Adding security exceptions for Firefox

Firefox connected to a site with a short (384-bit) key used in its certificate without giving any warnings or errors (other than the self-signed message). The main issue with Firefox’s approach is the relative inconvenience of getting understandable information to a non-technical user. Unlike solutions used by other browsers, clear color coding is not employed.

Internet Explorer 8.0.6001.18702
Internet Explorer 8 does not distinguish between “trusted” and “validated” sites; all sites with valid SSL certificates give the same feedback to the user, as seen below:

6-18 Internet Explorer trusted and validated sites
IE also displays notifications when certain actions that either create trust (entering a secure site) or violate trust (leaving a secure site, submitting unencrypted form data) are taken. However, this functionality can be disruptive to the normal browsing process, and therefore users might disable these notifications entirely. An example notification is shown below.

6-19 Browsing a secure site with Internet Explorer

On the other hand, IE provides good and highly visible feedback when encountering invalid SSL certificates. The warning bar and icon (as seen below) are easily ignored:

6-20 Internet Explorer warning bar when encountering an invalid certificate

6-21 Internet Explorer warning icon when encountering an invalid certificate

However, the URL field’s background is colored bright red, and a warning icon appears next to it; when the icon is clicked, it displays additional information about the exact problem with the certificate, as seen below:

6-22 Internet Explorer URL bar warning

The warning page displayed when an untrusted site is accessed for the first time (see 6-23) is similar to the Chrome implementation, but only gives a single line of terse information about the exact nature of the issue – this is not very helpful to the user.
Internet Explorer warning page when accessing an untrusted site

IE refused to connect to a site with a certificate using a short (384-bit) key:
6-24 Internet Explorer refusing to connect to a site with a cryptographically insecure certificate

In summary, IE has good user feedback; however, it does not distinguish between “trusted” and “validated” sites, and it only gives information about the nature of an untrusted site’s problem after the user has already chosen to accept the invalid certificate.

Chrome 6.0.472.55
Chrome does not distinguish between “trusted” and “validated” sites. All trusted sites give the same feedback (“https” text in green with a green lock icon appearing next to the text), and the window that appears when clicking the icon does not immediately specify whether a site’s identity was validated, as seen below.

6-25 Chrome security details about a trusted site

On the other hand, Chrome displays whether a site has been visited before; this is an added piece of trust-related feedback to the user.
If a site is untrustworthy due to having an invalid / self-signed certificate, it is very clearly visible in the address bar as seen below (even after the user chooses to accept it):

6-26 Chrome address bar for sites with invalid certificates

Navigating to an untrustworthy site also displays a “dramatic” page detailing the problem in a way understandable by non-technical users, as shown below. The previous version of Chrome (also shown below) also displayed a warning sign at the right end of the address bar; in the current version of Chrome this warning side is replaced with a red skull shown at the left end of the address bar.
Chrome security feedback when encountering an untrusted site

Chrome also refused to connect to a site with a certificate using a short (384-bit) key, giving an error message instead:

In summary, Chrome has a very visible and user-friendly feedback system for trusted and untrusted sites; however, it lacks support for “validated” sites.

Safari 5.0.1

Safari distinguishes between “trusted” and “validated” sites. Validated sites have their identity displayed on the URL bar in green, as seen below:

6-29 Safari trusted and validated sites

Sites the user has chosen to trust (despite certificate errors) are also displayed as trusted sites.
When encountering an untrusted site, Safari presented a pop-up window that did not have any details about the nature of the problem:

6-30 Safari security feedback when encountering an untrusted site

Safari refused to connect to a site with a certificate using a short (384-bit) key; it also gave a brief error message about the issue:

6-31 Safari security feedback when encountering a site with a cryptographically insecure certificate

In summary, Safari’s security feedback is lacking, although it does distinguish between “trusted” and “validated” sites and it does handle cryptographically insecure certificates better than most of the other browsers.

Opera 10.61
Out of all the evaluated browsers, Opera handles “trusted” and “validated” sites in the best way. Aside from an immediately visible color coded icon at the right end of the URL bar (yellow for trusted sites, green for validated sites), clicking the icon also shows detailed security information about the site in question.
Similar to Chrome, untrusted sites have a different icon in the URL bar (though not as obviously visible as Chrome’s version). Clicking that icon shows the problem (or problems) with the site’s certificate, see below:

When first accessing an untrustworthy site, Opera also presents a pop-up window (see below); however, this window provides a lot of information to the user and is fairly good about explaining those problems. Unlike all other evaluated browsers, Opera handles cryptographically insecure certificates as well.

Figure 6-33 – Opera untrusted sites
(however, this is not necessarily a good thing – IE / Chrome / Safari’s approach of silently refusing to connect is safer).

![Figure 6-34 – Opera security feedback when encountering an untrusted site](image)

In summary, Opera provides the most information and details to technical users; some of it is explained to non-technical users as well. However, the feedback for untrusted sites is not as “smooth” and visible as Chrome or (in some cases) IE.

### 6.3.2 Certifications

**Certification** refers to the confirmation of certain characteristics of an object, person, or organization. This confirmation is often, but not always, provided by some form of external review, education, or assessment.

In the world of information security certifications have mixed success. In case of physical safes they work fine, because of:

- Easy-to-understand levels
- Cash rating of burglary safes (E0-E7)
- Time rating of paper and data safes
- Directly tied to insurance risk levels.

At the same time, Common Criteria has moderate popularity, due to its complex certificates (protection profiles, security targets, evaluation assurance levels, …). Even the Public Key Infrastructure (PKI) has moderate success.
6.3.3 Trust chaining mechanisms

A chain of trust is designed to allow multiple users to create and use software on the system, which would be more difficult if all the keys were stored directly in hardware. It starts with hardware that will only boot from software that is digitally signed. The signing authority will only sign boot programs that enforce security, such as only running programs that are themselves signed, or only allowing signed code to have access to certain features of the machine. This process may continue for several layers. This process results in a chain of trust. The final software can be trusted to have certain properties, because if it had been illegally modified its signature would be invalid, and the previous software would not have executed it. The previous software can be trusted, because it, in turn, would not have been loaded if its signature would have been invalid. The trustworthiness of each layer is guaranteed by the one before, back to the Trust Anchor - the hardware.

It would be possible to have the hardware check the suitability (signature) for every single piece of software. However, this would not produce the flexibility that a „chain” provides. In a chain, any given link can be replaced with a different version to provide different properties, without having to go all the way back to the trust anchor. This use of multiple layers is an application of a general technique to improve scalability, and is analogous to the use of multiple certificates in a certificate chain.

In Computer Security, Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). [WikiTC]

A certificate authority (CA) is an entity that issues certificates. Before a CA issues a certificate, it may perform background or other checks to ensure the identity of the person or organization. Once identity has been certified, the CA issues a certificate and signs it. The certificate can then be widely distributed by its owner.

CAs can be either private or public. A private CA might issue certificates for an enterprise or organization. It issues certificates to its members who then are within the organization's trust system based on all certificates signed by the organization. Organizations can purchase complete CA implementation systems.

A public CA issues certificates for the general public. It may be run by the government or a private enterprise. Several countries, including Denmark and Australia, are working toward implementing a public CA. VeriSign, a U.S. company, operates a commercial public CA. There is no central CA in the trust that exists among a circle of friends or between two business partners. Here individuals certify each other. This system has the significant advantage of ease in setting up ad hoc groups because there is no central authority. However, it does not scale well and may be impossible to scale to the Internet.

In order to convey trust through certificate on a scale of millions, some hierarchy or chaining of trust is needed. No one certificate authority can provide all the certificates for the entire world. The basic idea behind trust or certificate chaining is that two parties decide they can trust each other on the basis of having a third party in common whom they both trust. Thus, you might trust that a person is who you think he is because the same CA has signed both of your certificates. In another example, you might have certificates signed by different CAs, but both of those CAs have elected to trust a third CA. The trust chains through the three CAs.

Another way to view trust chaining is as a hierarchy with a root. An individual decides she will trust a particular CA as a root and every individual, organization, or CA that trust is delegated to. Trust in the root has to start somewhere and is established independently of the secure e-mail system. One possibility is to meet the issuer/signer in person or over the telephone and verify that a certificate is valid, using something like a PGP fingerprint. Another possibility is to be given a root certificate by someone you
trust, like your ISP, MIS department, or system manager. You might also decide to trust a certificate because it is built into a particular piece of software you purchased or because you got it from the issuer yourself. Secure e-mail users who exchange mail with many other users across organizations are likely to place trust in many different roots. [Inet97]

The Certificate Hierarchy is a structure of certificates that allows individuals to verify the validity of a certificate’s issuer. Certificates are issued and signed by certificates that reside higher in the certificate hierarchy, so the validity and trustworthiness of a given certificate is determined by the corresponding validity of the certificate that signed it.

The Chain of Trust of a Certificate Chain is an ordered list of certificates, containing an end-user subscriber certificate and intermediate certificates (that represents the Intermediate CA), that enables the receiver to verify that the sender and all intermediates certificates are trustworthy.

One application of this mechanism is the Trusted Computing Group’s vision based on the Trusted Platform Module. Although its proponents (including Microsoft) claim many benefits from this trust, most are convinced that the primary application is Digital Rights Management.

6.4 Summary and Conclusion

This chapter showed that when it comes to trust in IoT, security and privacy play a most important role. The relation between these aspects has an essential role within this project. The chapter summarised what security means in different contexts, how a security feedback can be given to a user and also how the integrity of the privacy of a user can be maintained. One section covered definitions, which are necessary in order to have a common understanding when dealing with these issues in IoT.
7. General Summary

In this document we have reviewed the foreseen technologies and terminology that are to be built upon within uTRUSTit along with others that are to be aware of. This knowledge-base is for internal use, and its main objective is to enhance conscious technical collaboration amongst project partners.

Despite the fact that the science and terminology behind IoT is not strictly bounded in 2010, we tried to come to a conclusion what can mean a solid basis for future work. We tackled trust from many perspectives and have seen methodologies for balancing user trust perceptions with the security a certain system can establish. A study outlined the main trust problems to face within the IoT. The Accessibility chapter summarized related standards to be taken into consideration. After outlining Virtual Reality approaches for uTRUSTit’s project goals, we analyzed and weighed current practices for raising security awareness and managing trust. Apropos of this, latest web and mobile security feedback methods have been tested from the aspect of user perception and comprehension.

This study draws a picture of the origins and basis of uTRUSTit, and while it explains the need for a better trust management methodology, it provides ways and opportunities to create a cutting edge solution that enables systems to earn long-term trust from the side of its users.

8. Index

accessibility, 2, 34, 70
Adaptive Policy Manager, 42
awareness, 2, 16, 24, 27, 41, 59, 70
camouflage, 53
CAVE, 30
Certificate authority (CA), 68
certification, 9, 13, 67
Digital Rights Management, 4, 9, 44, 69, 81
FIDIS, 50, 52, 76
Flystick, 31
Identity protection, 53
Interaction, 4, 31, 32, 73, 74, 79
Internet of Things, 1, 2, 6, 7, 8, 9, 15, 21, 23, 25, 34, 37, 72, 73, 78
Intrusion Detection System, 42
IoT, 5, 6, 7, 8, 9, 14, 15, 16, 17, 18, 21, 22, 23, 24, 25, 30, 32, 34, 37, 38, 39, 41, 52, 70
Topics, 37
IT-Ecosystem (ITE), 18, 20, 74
Location dummy traffic, 55
Mental Models, 3, 4, 27, 80
MIX zone, 55
PKI, 9, 48, 67, 75
PRIME, 47, 52, 75, 78
privacy, 2, 5, 11, 14, 15, 16, 17, 22, 23, 24, 25, 26, 27, 37, 38, 42, 46, 47, 48, 49, 50, 51, 52, 54, 56, 57, 76, 77, 78, 80
history, 47
Privacy by Design, 17, 57
Privacy enhancing technology (PET), 46
Privacy Impact Assessment (PIA), 46
Public Key Infrastructure, 67
RFID, 23, 24, 36, 38, 56, 57, 72, 75
risk, 2, 9, 12, 14, 15, 17, 23, 26, 37, 41, 46, 67, 77
safe, 12
secure, 12, 44, 69, 72, 73, 75, 78, 80
security, 2, 3, 4, 5, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19, 21, 23, 24, 25, 26, 27, 28, 32, 37, 38, 39, 40, 42, 43, 44, 45, 47, 48, 52, 56, 58, 59, 60, 63, 64, 65, 67, 68, 70, 72, 73, 74, 75, 77, 79, 80, 81
adaptive, 39
awareness, 3, 45
dynamic, 40
evolving, 39
security awareness, 3, 16
security feedback, 70
Spatial cloaking, 54
SSL, 44, 58, 59, 60, 61
standards, 2, 4, 5, 17, 21, 28, 34, 35, 70
Temporal cloaking, 53, 54
Testing, 4, 33, 74
threats, 9, 11, 14, 15, 26, 28, 37, 39, 40, 49
tracking glasses, 31
trust, 2, 5, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18,
19, 21, 22, 23, 24, 25, 26, 28, 32, 41, 58, 61,
63, 64, 68, 69, 70, 72, 73, 74, 76, 80
Balancing, 3, 14, 17
between machines, 3, 9
Conceptual Model, 20

Technology-driven, 18
User-driven, 19
Trusting, 68
Trusted, 3, 9, 10, 11, 12, 47, 69, 73, 80
Trusted Computing Group, 3, 10, 69, 80
Trustworthy, 1, 11, 12
User feedback, 58
uTRUSTit, 1, 2, 5, 8, 9, 13, 15, 16, 17, 18, 21,
27, 28, 32, 42, 58, 70
Virtual Private Network (VPN), 43
Virtual Reality, 2, 30, 32, 70, 74
VRML, 31
XSENS, 33
9. References

TRUST AND THE INTERNET OF THINGS


[Hildebrandt 2010] Hildebrandt, M., An Ecosystem of Legal and Technological Protections, on: Trusted e-services for the citizen session, ICT Event 2010, Brussels


[ITU 2005] International Telecommunication Union (ITU), Internet Reports 2005: The Internet of Things Executive Summary Available at: www.itu.int/internetofthings.


VIRTUAL REALITY


SECURITY AND PRIVACY


[Chatterjee 2009] M. Chatterjee, G. SivaKumar, and B. Menezes, Dynamic policy based model for trust based access control in P2P applications, IEEE International Conference on Communications (ICC ’09), 14-18 June 2009


