SCOTT:
Secure COnnected Trustable Things

Trust Technology Advances

Document Type	Deliverable
Document Number	D22.3
Primary Author(s)	Maunya Doroudi Moghadam | UiO Toktam Ramezani | UiO
Document Version / Status	1.0 | Final
Distribution Level	PU (public)

Project Acronym	SCOTT
Project Title	Secure Connected Trustable Things
Project Website	www.scottproject.eu
Project Coordinator	Michael Karner | VIF | michael.karner@v2c2.at
JU Grant Agreement Number	737422
Date of latest version of Annex I against which the assessment will be made	2019-03-15

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

CONTRIBUTORS

Name	Organization	Name	Organization
Maunya D. Moghadam	UiO	Josef Noll	UiO
Toktam Ramezani	UiO	Maghsoud Morshedi	EyeSaaS

FORMAL REVIEWERS

Name	Organization	Date
Boning Feng	OsloMet	2020-01-23
Johanna Kallio	VTT	2020-01-27

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
v0.1	2019-08-12	Maunya D. Moghadam / UiO	Inputs
v0.2	2019-10-24	Toktam Ramezani / UiO	Inputs
v1.0	2020-01-18	Josef Noll / UiO	Overview

TABLE OF CONTENTS

LIST OF FIGURES

1 EXECUTIVE SUMMARY

In this document the advantage and importance of creating trust in technology are discussed. The definition of trust in SCOTT is reviewed. Societal trust as an important topic in society level is considered in further studies. Then the technology side of trust, its advances and the Technology Acceptance Model (TAM) are mentioned. The SCOTT suggestions for trust including Trustworthiness Assurance Cases (TACs) from WP28 are presented. Finally, the trust labelling with an example in remote management is briefly explained.

Keywords: trust, technology, business-to-consumer relation, business-to-business relation, societal trust, trust labelling, trustworthiness assurance cases, technology acceptance model, trust models.

2 INTRODUCTION

Security and trust are critical challenges, especially in Internet of Things (IoT). “Things” including electronic devices, software, sensors, and actuators are connected and communicate with each other, enabling them to be deployed in a variety of environments and domains such as home and buildings, smart infrastructure, health, and mobility, i.e. in the whole society.

In many traditional businesses, trust is based on a combination of judgment resulted from face-to-face meetings or opinions of other people and colleagues, friends and business partners. Currently, the migration from centralized information systems to internet-based applications and further to IoT has changed the traditional perception of trust because transactions have to span a range of domains and organizations, not all of which might be trusted to the same extent. Moreover, it is required to support trust in Internet services, which generally are not just based on human but technology interactions. The list of new technologies being released is amazing from biosciences field to the Artificial Intelligence (AI), social media, smart homes and cars, financial services and online services, etc. This intense amount of new technologies is a challenge for users. In general, trust in complex technologies has become a significant enabler for the use and adoption of new technologies and systems. However, trust can be won if each technology becomes part of normal life and develops in a way that consumers can easily follow. Businesses can help this process by raising awareness and educating consumers. There are early adopters which are really interested in experiencing each new product release. And beside them there are more prudent users which usually waiting to see if a new technology deserves their time and money. The more technology enters our lives, the more critical the issue of trust becomes. No one buys anything unless he/she trusts it. Advertisers spend a fortune building trust, and designers work hard to foster it [4].

Building trust in technology takes time. It needs familiarity with a product and confidence about the results. As the comprehension grows, trust builds. The process can move slowly in the early steps. Companies want to build their business around the certain perception. That perception can be like a technology partner, but it can also be a trusted entity, or it can be a trust provider and in total it is about the presentation. As an example, trust in product means get what you expect, and this expectation is made from the presentation of the product. Therefore, developing trust in companies, who are focusing on developing technologies, is a key part of building the company-consumer relationships [11].

2.1 Trustability as Defined in SCOTT

As the term trust is widely used in different contexts and perspectives and carries various meanings, it is important to clarify what is meant by it. Trust is viewed as a relation between a trustor and a trustee which is a technical system within the SCOTT project. The relationship is influenced by the characteristics of the trustor, the context, task, and the trustee. Trust issues are negative trust attitudes that stand against establishing a trust relation with the trustee. SCOTT will not deal with just 'things that are connected', but 'trustable things that are connected' (D28.3). Developing trusted wireless systems and systems that rely on wireless components is one of the main objectives of the SCOTT project. Systems with wireless components are often complex and stakeholder trust becomes a significant enabler for their use and adoption. In general, technical systems that people use and buy for work and leisure have reached a level of complexity that goes

beyond most humans' abilities to understand them. Therefore, these stakeholders may experience considerable risk in relying on such technologies. Risk is here understood in terms of vulnerability and uncertainty of using a system for a specific purpose and in a specific environment. For example, when stakeholders share sensitive data with online systems or perform safety critical tasks or tasks of high criticality, they are highly vulnerable if the system fails. Here stakeholder trust becomes an important consideration especially under conditions of voluntariness when stakeholders have the ability of choose other products or services instead. Especially, systems that contain wireless technology components can experience scepticism concerning their reliability and security as well as complexity in comparison to traditional wired solutions. This trust may have direct impact on the acquisition decision concerning a system that utilizes wireless components. The baseline has been described in detail in D28.1, "Foundations for Building Trusted Systems". In addition, in the SCOTT project Trust factors are identified as Reliability, Availability, Maintainability, Safety, Integrity, Security, Privacy, Predictability, Reputation, Configurability, Consistency, Acceptability, Usability, Functionality, and non-technical trust factors: Confidentiality, Reputation, Acceptability and Privacy.

Given the grouping of SCOTT parameters, it is needed to address the SCOTT use cases with respect to business-to-consumer (B2C) relations and business-to-business (B2B) relation.

2.2 Trust in Products (B2C)

"Get what you expect"

Trust is a vital element of every business transaction. Customers must trust those producers that provide the services they advertise and those that do not disclose private information such as name, address, credit card details, purchases, etc. of the customers. On the other hand, producers must trust that the buyer is able to pay for goods or services, is authorized to make purchases on behalf of an organization, or is not underage for accessing service or buying certain goods [7].

In business relations, IoT and autonomous processes break up the boarders between companies and customers. Building trust in product is a long process, but it's an investment that always pays off. In business, trust is earned and not given. When consumers trust a product, they are happier and more engaged to become a permanent customer and user acquisition becomes easier. However, trust can be elusive. It is tricky to build and easily lost.

Trust in B2C environment can be covered by privacy labels, such as in WP21 which is medical use case. There are some medical regulations which are important. It means everything you bring out on medical has to be compliant with medical regulations. From that point of view, trust in a medical device is not that obvious.

It is the trust in the service provision which is important for WP21. In WP21 which focuses on fall sensors, opening the door, informing the neighbors, from that point of view, the transparency of knowing what are the effects which will open the door, what are the effects which trigging at the neighbors, etc. are very important.

The research [12] found that older people's habits and norms do not need to be disrupted by the ambient system. What is of more importance is the relationships between the older

person and her or his ‘monitor’ based on trust, as well as institutional providers who need to instill or earn trust.

2.3 Business Perception (B2B)

Trust is vital in B2B interactions as business relationships between companies work very differently from relationships between businesses and consumers. First, B2B relationships are often more long-term and designed to meet a continuous demand which is important to the success of the business. Second, business owners often rely strongly on the service or products provided in order for their own business to operate. These business relationships should not be taken easily, because contracts often become active and the unaware business owners may finally lose money if the service or terms are not in favor.

For example, WP9 which is facilities management has a goal to simplify these procedures by introducing the self-aware wireless network of smart components for access control and facility monitoring with integrated identification and authorization capabilities. The main objectives are related to detection, identification and localization of different objects and their behavior within facilities or areas of critical infrastructure. The other issue is extending the access control in physically separated locations with virtually defined areas with locally defined rules (e.g. customized area and behavior definition, virtual fences etc.). The business requirements (from the industry perspective) indicate an urgent need for easy deployment of systems that allows for precise monitoring and tracking of objects (people, vehicles, tools, equipment etc.) in virtually defined areas of an industrial facility in order to support its business operations and processes with respect to safety and security. In order to have a long-term work and meet a continuous demand required in facilities management, providing a trustable relationship between businesses who are involved is necessary.

2.4 Societal Trust

There is an analysis about the relation between societal trust and open innovations which confirm strong evidence that greater societal trust is associated with higher levels of subsequent open innovation. The effects of societal trust on open innovation are also economically significant. For example, an interquartile shift in societal trust measure (i.e., a shift from the 25th to the 75th percentile) is associated with a nearly 25.31% increase in open innovation activities. These findings are consistent with the notion that societal trust plays an important role in promoting open innovation activities by reducing coordination costs and the perceived risks of opportunism [3].

Trust in large companies like Facebook, Google, Amazon, etc is low as they show distrust in digital. Focusing on empowering people by digital capacity and making technology transparent is very necessary for societal trust. In fact, trust in digital systems is needed to protect the societies which are under stress, cybercrime, IoT attacks, threats, etc.

The Nordic region has the highest levels of social trust in the world which benefits the economy, individuals and society as a whole, however nowadays this trust is under threat [15]. However, it is still in the top level and would be helpful for other European countries to consider Norway´s achievements in social trust.

2.5 Technology Advances

In this section we mainly focus on the side of technologies.

Study findings about trust and technology suggest that through an ongoing relationship, trust evolves and is shaped over time and can form a competitive capability that may not be easy for competitors to replicate. Both trust and technology are found to have significant impact on supply chain collaboration and on firms' operational performances [10].

There are some discussions about trust-free systems based on blockchain technology which promise to revolutionize interactions between peers that require high degrees of trust, usually facilitated by third party providers. Peer-to-peer platforms for resource sharing represent a frequently discussed field of application for "trust-free" blockchain technology. However, trust between peers plays a crucial and complex role in virtually all sharing economy interactions [9].

Recently, the Bitcoin-underlying blockchain technology gained prominence as a solution that offers the realization of distributed trust-free systems, where economic transactions are guaranteed by the underlying blockchain. It is still at an early stage and thus require a deeper understanding of how the blockchain potentials can be realized, and what are the opportunities and challenges in so doing. Following a design science approach, they developed a proof of concept prototype that has the potential to replace a trust-based coffee shop payment solution that is based on an analogue, pre-paid punch card solution. The demonstrator provides a starting point to evaluate the strengths and weaknesses of the blockchain technology when replacing a trust-based by a trust-free transaction system. It can be concluded that the secure and trust-free blockchain-based transaction has the potential to change many existing trust-based transactions systems, but that scalability issues, costs, and volatility in the transaction currency are hindrances. Even though the blockchain gained prominence with the emergence of Bitcoin in 2009 and has thus existed now for about six years, we are still at the beginning to fully understand it's potential. Innovative solutions that go beyond crypto-currencies such as Bitcoin may have the potential for fundamentally changing society and they might witness right now the dawn of cryptographically secured trust-free transactions economy. The Economist just coined the blockchain "the trust machine", thereby indicating that the blockchain takes care of trust issues, thereby freeing them from the necessity of implementing mechanisms to signal or convey trust (Economist, 2015). In other words, the created system is running without trust concerns, making a transaction "trust free", once it is settled as an agreement in the blockchain. While the Bitcoin blockchain was just the beginning, with the increasing availability of generic, self-programmable blockchains, as offered by foundations such as Ethereum, blockchains are now used in other areas beyond crypto-currencies as well. This paves the way of utilizing the features of the blockchain such as its trust-free, transparent, and highly secure nature in other application areas. For example, IBM and Samsung announced to experiment with the Ethereum-based blockchain to power Internet of Things (IoT) solutions [2].

On the other hand, there is an issue about technology readiness. A study examines how individuals in different technology readiness segments differ in the level of perceived trustworthiness that they assign to service providers. Using a large dataset of 1,866 responses from business decision-makers, the study interrelates the theory-driven constructs of technology readiness and perceived trustworthiness. The study focuses on understanding the differences in the level of perceived trustworthiness, composed of ability,

integrity and benevolence among five technology readiness segments: explorers, pioneers, skeptics, hesitators, and avoiders. The study finds that explorers have the highest overall technology readiness and the highest level of perceived trustworthiness of service providers, and hesitators and avoiders have the lowest level of technology readiness and perceived trustworthiness [8].

In addition, there is a model named the Technology Acceptance Model (TAM) which uses an information systems theory to model how users embrace and use a technology. The model suggests that when users face to a new technology, a number of factors affect their decision about how and when they will use it, notably they are Perceived usefulness (PU) and Perceived ease-of-use (PEOU). Perceived usefulness was defined by Fred Davis as "the degree to which a person believes that using a particular system would enhance his or her job performance and Perceived ease-of-use was also defined by Davis as "the degree to which a person believes that using a particular system would be free from effort". Figure 1 shows that these two factors affect the attitude towards using a new technology and the behavioral intention to use and finally actual system use.

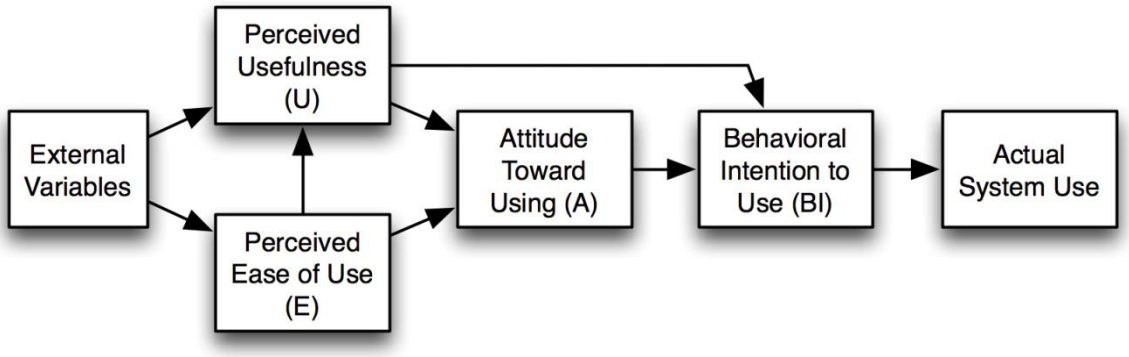

Figure 1. The Technology Acceptance Model [6]

3 SCOTT SUGGESTIONS FOR TRUST

Significant efforts are currently expected to improve wireless system reliability and the associated perception of trustworthiness to increase their acceptance. What is missing so far, are guidelines that allow developers to determine how trustworthy products could be produced. This is the purpose of the SCOTT trust framework which brings together human users, operators, engineering, and management and have been described in WP28 deliverables.

To facilitate the trust assurance process, Trustworthiness Assurance Cases (TACs) are developed jointly by the SCOTT use case owners and the trust worthiness assurers. To help the formulation of these use cases, the deliverable provides an overview of trust research and trustworthiness principles from a review of literature. In the trust assessment process, the use case owners provide up-to-date use case descriptions and the trustworthiness assurer provides critical trustworthiness considerations. Both together develop the TACs that reflect trustworthiness considerations within the context of the use case. In the next step, the SCOTT use case owners evaluate each of the TACs for the likelihood and severity with which they impact the trustworthiness of the system. The trustworthiness assurers the reviews these recommendations and classifies them according to their trustworthiness. The result is trustworthiness conclusions about the status of the use case [19].

D28.5 describes the application of this process for nine of the SCOTT use cases and provides the evaluations of use case owners, trust assurers, and the associated TAC trustworthiness recommendations. The results indicate that from 38 TACs that were assessed altogether, 16 TACs (42%) should still be addressed within the SCOTT project, 12 (32%) do not require further action. The remaining 10 (26%) could be addressed outside of the SCOTT project. Overall, a process is presented to quantify and measure trustworthiness of wireless products. The results indicate that while significant process has been made since the beginning of the SCOTT project, further actions are needed to increase trustworthiness of the SCOTT use case solutions. The findings are expected to be helpful to identify where to put efforts to further increase trustworthiness within SCOTT and applicable to wireless product developments outside of SCOTT.

3.1 Trust in the SCOTT Bubble Concept

While current infrastructures have difficulties in the diversity of services and configurations, trust specification and management, especially for smart infrastructure as a goal in SCOTT, poses even bigger challenges; one of which is a different understanding of trust even in systems in one domain. Besides, trusted communication between systems in different domains is another significant challenge. What is needed is a well-established trusted communication across different industrial domains. However, there is a need for a more formalized approach to trust establishment, evaluation, analysis, and management to provide trustable domain synergy in SCOTT.

Each SCOTT domain may need to support a range of different trust relationships and thus be capable of supporting different types of policies to achieve that. To explain examples of trust concepts in some domains and viewpoints such as vehicle, sensor network, and organizations, we can first take a look at different factors that result in a different view of the trust concept.

3.1.1 Factors Affecting Trust

Several factors affect the viewpoint to trust in each SCOTT domain or bobble concept. Examples of these factors are:

- Mobility: If the entities have the mobility option, the speed and delay will affect the communication and thus trust.
- Dynamicity of the Network Topology: If the topology of entities changes, it will affect malicious or untrusted entity recognition.
- Real-time Constraints: If the communication and information transmission have a time limit range, it means there is also a limitation to making the decision about how to trust the information.
- Computing and Storage Capability: The amount of possible information transmission among devices or entities in each domain determines the computing and storage capability and must be considered in computing trust measurements.
- Volatility: the length and number of communications for a limited period of time will also affect the expectation and trust.

[13] shows how these factors can affect trust in a vehicle while trust between vehicles implies how a vehicle can trust other vehicles and the received messages from them. As an example, when a vehicle broadcasts a warning message to warn the vehicles behind that it is out of control, it is crucial for the vehicle receiving this warning message to determine the trustworthiness of the message and take a quick response. In such a case, it is impractical to ask neighbor vehicles or a trusted third party (TTP) for help due to the strict time constraint, mobility, and dynamic network topology.

Based on the concept of each bobble, there are different trust models.

3.1.2 Different Trust Models in Each Concept

Centric Trust Models or Data-Centric Trust Models for vehicles. In ad-hoc and sensor networks, trust and reputation-based approaches result in two trust models called node-centric trust models, and system-centric trust models. They are used to detect malicious or selfish behavior of nodes that cannot be detected by traditional security schemes [1].

3.1.3 Human Factors Affect Trust

Apart from technology, human factors are playing an important role in information security and thus in trust. Therefore, effective risk management in organizations to deal with the insiders and prevention actions such as limiting outsourcing are so effective to increase trust. It is because outsourcing can result in the fragmentation of protection barriers. Moreover, due to the legitimate access to facilities and information, insiders impose security risks because they have the knowledge about the organization and the location of valuable assets, and they know how to achieve the greatest impact whilst leaving little evidence [5]. In this Regard, [16] show how trust can be increased by providing Information Security Culture to considering human aspects of trust.

3.2 Trust Labeling

Digital Europe.org IoT has defined a trust label which is a binary representation (0/1) of trust. Based on our discussion in SCOTT this labeling is not sufficient. The reason is that there is no black/white boundary in trust. Due to the variety of trust parameters, as pointed out in the previous sections, trust indicators or labels need to represent the scale of trust.

WP28 proposes in a white paper that trustworthiness labeling from an independent and unbiased trustworthiness rating agent will help establish trust between end-users and products as well as provide guidance and certification services to development organizations how to create trustworthy products and maintain them. In contrast to existing labeling efforts, this one is inherently user centered and intends to create usable and effective trust solutions.

A suggestion is to exemplify in practice and catch the problem in different use cases. For example, in elderly care use case we need to give trust to people, if elderly stay at home and fall, they get the care that they need. Therefore, we build a system which gives trustworthiness to all the component of the system, such as technical aspects (sensors. communications, door opener, etc.) and human aspects (end user perspectives, caretaker organization, etc). In this way we classify trust levels by using bottom-top approach as we have in security classification and privacy labelling methods.

3.3 SCOTT Example: Trust in Remote Management

Trustable remote monitoring and management systems are required to establish a controlled environment for new services and devices in order to 1) improve the quality of existing services and *2)* enable novel services. However, monitoring and remote management can cause security and privacy concerns and thus affect the trust formation between customer and service provider [14].

The paper [14] introduces a trust model considering institutions as mediators to assess trustability of remote monitoring and management systems. The proposed model considers governance as an approach to audit remote monitoring and management systems and accordingly provides institutional assurance in form of certificate or labels in order to facilitate trust decision making and motivate trustworthy behaviors. The proposed model utilized the multi-metric method to measure governance criteria objectively and represent level of trustworthiness with A-F labels. Meanwhile, issuing trustworthiness certificate or A-F labels will encourage service providers to improve trustability of their remote monitoring and management approaches, which improve acceptability and efficiency of managed services. The remote monitoring and management are a process of supervising and administration of information systems such as network devices, servers, mobile devices, and sensors. In remote monitoring, service providers enable the endpoint devices to report their operating information such as resource consumption, health checks, measured data of sensors by means of self-reporting or installing an agent on remote devices. In remote management, service providers administer remote devices to perform certain tasks such as software updates (e.g. patches, firmware updates and configuration changes), disable or enable specific services or functionalities, reboot or shut down the device, etc.

However, the key challenge is to build a trustable remote monitoring and management system in order to assure users regarding their security and privacy. In the absence of trust, users will be reluctant to use or enable remote monitoring and management services due to

growing security and privacy breaches. The mentioned paper provides existing trust issues in monitoring and management systems and defines objectives in order to build trustable remote monitoring and management systems by motivating trustworthy behaviors from services providers' side [14].

4 CONCLUSIONS

Security and trust are considerable challenges, especially in Internet of Things (IoT). Building trust in each technology takes time. It needs familiarity with a product and reliance about the results. It is helpful to consider the recent studies about trust and technology as both trust and technology are found to have significant impact on supply chain collaboration and on firms' operational performances.

Developing trusted wireless systems and systems that rely on wireless components is one of the main objectives of the SCOTT project. The purpose of the SCOTT trust framework which brings together human users, operators, engineering, and management, are guidelines that allow developers to determine how trustworthy products could be produced. In addition, Trustworthiness Assurance Cases (TACs) are developed jointly by the SCOTT use case owners and the trust worthiness assurers to facilitate the trust assurance process. Each SCOTT domain may need to support a range of different trust relationships and thus be capable of supporting different types of policies to achieve that. On the other hand, trustworthiness labeling from an independent and unbiased trustworthiness rating agent will help establish trust between end-users and products as well as provide guidance and certification services to development organizations how to create trustworthy products and maintain them. A suggestion is to exemplify the idea in practice and catch the problem in different use cases. Such as trustable remote monitoring and management which has used trust model considering institutions as mediators to assess trustability of remote monitoring and management systems.

The current trust relationships highlight the need for a flexible, general-purpose trust management system that can navigate the complex and different domains.

5 REFERENCES

[1] Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks. Frontiers of Computer Science, 9(2), 280–296.

[2] Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. (2016). Blockchain–the gateway to trust-free cryptographic transactions.

[3] Brockman, P., Khurana, I. K., & Zhong, R. I. (2018). Societal trust and open innovation. Research Policy, 47(10), 2048–2065.

[4] Campos-Castillo, C. (2010). Trust in Technology. Trust and Technology in a Ubiquitous Modern Environment, 145–159. https://doi.org/10.4018/978-1-61520-901-9.ch009

[5] Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? Information Security Technical Report, 14(4), 186–196.

[6] Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. Management Science, 35(8), 982–1003.

[7] Grandison, T., & Sloman, M. (2000). A survey of trust in internet applications. IEEE Communications Surveys & Tutorials, 3(4), 2–16.

[8] Hallikainen, H., Hirvonen, S., & Laukkanen, T. (2018). Are Technology-Ready Customers More Inclined to Trust?

[9] Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic Commerce Research and Applications, 29, 50–63.

[10] Jimenez-Jimenez, D., Martínez-Costa, M., & Sanchez Rodriguez, C. (2019). The mediating role of supply chain collaboration on the relationship between information technology and innovation. Journal of Knowledge Management, 23(3), 548–567.

[11] Kang, J., & Hustvedt, G. (2014). Building trust between consumers and corporations: The role of consumer perceptions of transparency and social responsibility. Journal of Business Ethics, 125(2), 253–265.

[12] Lie, M. L. S., Lindsay, S., & Brittain, K. (2016). Technology and trust: older people's perspectives of a home monitoring system. Ageing & Society, 36(7), 1501–1525.

[13] Lu, Z., Qu, G., & Liu, Z. (2018). A survey on recent advances in vehicular network security, trust, and privacy. IEEE Transactions on Intelligent Transportation Systems, 20(2), 760–776.

[14] Morshedi, M., Noll, J., & Kari, R. (2018). Building Trustable Remote Monitoring and Management Systems. 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 213–219. IEEE.

[15] NORDIC COUNCIL OF MINISTERS. (2017). Trust – the Nordic. Nordic Council of Ministers Analysis Report.

[16] Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. 14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings., 405–409. IEEE.

[17] SCOTT Deliverable D28.1 "Foundations for Building Trusted Systems", v2.1, 2017-12-21.

[18] SCOTT Deliverable D28.3 "Use Case Vulnerabilities", v1.0, 2018-05-22.

[19] SCOTT Deliverable D28.5 “Trustworthiness Assurance Cases for SCOTT”, v1.0, 2019-04-26.

A. ABBREVIATIONS AND DEFINITIONS

Term	Definition
AI	Artificial Intelligence
B2B	Business-to-Business
B2C	Business-to-Consumer
IoE	Internet of Every Things
IoT	Internet of Things
PEOU	Perceived Ease-of-Use
PU	Perceived Usefulness
TACs	Trustworthiness Assurance Cases
TAM	Technology Acceptance Model
TTP	Trusted Third Party