Computer Science

Enhanced Security for Mobile User Authentication and Single Sign-On

Sanna Suoranta

Aalto University

DOCTORAL DISSERTATIONS

Aalto University publication series
DOCTORAL DISSERTATIONS 226/2016

Enhanced Security for Mobile User Authentication and Single Sign-On

Sanna Suoranta

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Science, at a public examination held at the lecture hall H304 of the school on 11 November 2016, at 12 noon.

Aalto University
School of Science
Computer Science

Supervising professor
Prof. Tuomas Aura

Preliminary examiners
Prof. Dr. Simone Fisher-Hübner, Karlstad University, Sweden
Prof. Chris Mitchell, Royal Holloway University of London, United Kingdom

Opponent
Prof. Valtteri Niemi, University of Helsinki, Finland

Aalto University publication series
DOCTORAL DISSERTATIONS 226/2016

ISBN 978-952-60-7102-2 (printed)
ISBN 978-952-60-7101-5 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-60-7101-5

Unigrafia Oy
Helsinki 2016

Finland

441 697
Printed matter

Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

Author
Sanna Suoranta

Name of the doctoral dissertation
Enhanced Security for Mobile User Authentication and Single Sign-On

Publisher School of Science

Unit Computer Science

Series Aalto University publication series DOCTORAL DISSERTATIONS 226/2016

Field of research Computer Science

Manuscript submitted 14 June 2016 **Date of the defence** 11 November 2016

Permission to publish granted (date) 14 October 2016 **Language** English

☐ **Monograph** ☒ **Article dissertation** ☐ **Essay dissertation**

Abstract

Single Sign-on (SSO) systems simplify user authentication for the many online services that we need to access every day. Solutions exist for both intra-organizational use and for the open web. While SSO systems meet their main goal of reducing the number of passwords that a user needs to memorize, many other aspects can still be improved. The goal of this thesis is to investigate how digital user identities are linked to real world identities, what opportunities and challenges mobile devices bring to the SSO systems, and how SSO sessions are managed after the initial authentication.

Many countries all around the world provide citizen authentication methods based on smart cards or other credentials. Most of these offer strong two-factor authentication and APIs for integration to private and commercial systems. However, organizations may want to implement strong authentication by themselves without relying on specific national identity systems. We designed and implemented a system that provides two-factor user authentication with mobile phone as a secure store for service-issued credentials. Mobile devices also give rise to questions about session mobility. Stateless web applications that are distributed between the browser and the cloud may store only authentication session information in the client device. We implemented session migration that allows SSO sessions to be moved from one device to another. This enables users to change to the best available device, such as switching between a desktop computer and a mobile device, and still continue working without reauthentication. Moreover, most SSO systems focus on the authentication at the beginning of sessions. We observe that the ending of sessions can be confusing and lead to security failures. We investigate logout in existing SSO systems and suggest separating the concepts of local and global logout.

As the computing environment changes, for example, applications move to mobile and cloud platforms, there is continuous need to update authentication technologies. This thesis proposes several incremental improvements to SSO systems and addresses various pain-points from the user's and developer's points of view.

Keywords computer security, authentication, single sign-on (SSO), identity management

ISBN (printed) 978-952-60-7102-2 **ISBN (pdf)** 978-952-60-7101-5

ISSN-L 1799-4934 **ISSN (printed)** 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Helsinki **Location of printing** Helsinki **Year** 2016

Pages 6+196 **urn** http://urn.fi/URN:ISBN:978-952-60-7101-5

Aalto-yliopisto

Tiivistelmä

Aalto-yliopisto, PL 11000, 00076 Aalto www.aalto.fi

Tekijä
Sanna Suoranta

Väitöskirjan nimi
Tietoturvaparannuksia mobiilikäyttäjän tunnistukseen ja kertakirjautumiseen

Julkaisija Perustieteiden korkeakoulu

Yksikkö Tietotekniikan laitos

Sarja Aalto University publication series DOCTORAL DISSERTATIONS 226/2016

Tutkimusala Tietotekniikka

Käsikirjoituksen pvm 14.06.2016 **Väitöspäivä** 11.11.2016

Julkaisuluvan myöntämispäivä 14.10.2016 **Kieli** Englanti

☐ **Monografia** ☒ **Artikkeliväitöskirja** ☐ **Esseeväitöskirja**

Tiivistelmä

Kertakirjautumisjärjestelmien (SSO) tarkoitus on yksinkertaistaa käyttäjien tunnistamista verkkopalveluissa. Erilaisia SSO-ratkaisuja on tarjolla sekä organisaation sisäiseen käyttöön että avoimille web-palveluille. Niiden ensisijainen tavoite on vähentää muistettavien salasanojen määrää, mutta järjestelmien suunnitteluun liittyy muitakin tekijöitä, joita voidaan kehittää edelleen. Tämän väitöskirjatutkimuksen tavoitteena on selvittää, kuinka käyttäjän digitaaliset identititeetit ovat linkittyneet todellisen maailman identiteetteihin, mitä mahdollisuuksia ja haasteita mobiililaitteet tuovat kertakirjautumisjärjestelmille, ja miten kertakirjautumisjärjestelmän istuntoja hallitaan käyttäjän tunnistamisen jälkeen.

Useissa maissa on otettu käyttöön kansallisia järjestelmiä kansalaisten tunnistamiseen sähköisissä palveluissa esimerkiksi älykortteihin ja varmenteisiin perustuen. Nämä järjestelmät toteuttavat yleensä vahvan kaksivaiheisen todennuksen ja tarjoavat palvelurajapintoja yksityisille ja kaupallisille järjestelmille. Kansalliset varmenteet eivät kuitenkaan aina sovellu yksityisten organisaatioiden ja palveluiden käyttöön. Tässä työssä suunnittelimme ja toteutimme kaksivaiheisen käyttäjän tunnistuksen, jossa matkapuhelin toimii turvallisena talletuspaikkana palvelun antamille varmenteille.

Mobiililaitteiden myötä herää myös kysymys käyttäjän istuntojen liikkuvuudesta. Selaimen ja pilven välille hajautetut tilattomat web-sovellukset tallettavat usein pelkän istuntoevästeen käyttäjän laitteelle. Käytimme tätä hyväksi kertakirjautumisistuntojen siirtämiseksi laitteelta toiselle. Käyttäjä voi vaihtaa käyttämäänsä laitetta tarpeen mukaan, esimerkiksi tietokoneen ja mobiililaitteen välillä, ja jatkaa työskentelyä ilman uudelleenkirjautumista.

Suurin osa käytössä olevista SSO-järjestelmistä keskittyy käyttäjän tunnistamiseen istunnon alussa. Istunnon päättymiseen on kiinnitetty vähemmän huomiota. Uloskirjautumista on usein vaikea ymmärtää, mikä johtaa tietoturvaongelmiin. Väitöskirjan osana tutkimme uloskirjautumisen ongelmia ja ehdotamme ratkaisuksi palvelukohtaisen ja yleisen uloskirjautumisen käsitteiden erottamista toisistaan.

Käyttäjän todentamisen tekniikat vaativat jatkuvaa kehittämistä, kun niiden toimintaympäristö muuttuu, esimerkiksi palvelut siirtyvät mobiililaitteille ja pilvialustoille. Tässä väitöskirjassa esitetyt ratkaisut tuovat useita pieniä parannuksia kertakirjautumisjärjestelmiin ja korjaavat ongelmakohtia käyttäjän ja kehittäjän näkökulmista.

Avainsanat tietoturvallisuus, tunnistus, kertakirjautuminen, identiteetinhallinta

ISBN (painettu) 978-952-60-7102-2	**ISBN (pdf)** 978-952-60-7101-5	
ISSN-L 1799-4934	**ISSN (painettu)** 1799-4934	**ISSN (pdf)** 1799-4942
Julkaisupaikka Helsinki	**Painopaikka** Helsinki	**Vuosi** 2016
Sivumäärä 6+196	**urn** http://urn.fi/URN:ISBN:978-952-60-7101-5	

Preface

Writing this thesis has taken a long time, but it has given me time to think and really learn a lot. I want to thank everybody who has supported me during this time.

First of all, I want to thank my supervisor, Prof. Tuomas Aura, who has tirelessly been able to help me, especially to express my thoughts in English. When he defended his thesis in 2000 and gave a copy of it, he inscibed it to me “Sannalle opiksi ja esimerkiksi”. Since mid 1990’s, he gave interesting security courses together with Dr. Arto Karila and Dr. Pekka Nikander. Thanks to their entusiasm, I found the field of computer science that interest me. I also wish to express my gratitude to Prof. Antti Ylä-Jääski for his support over the many years.

I would also like to thank my preliminary examiners, Prof. Dr. Simone Fischer-Hübner and Prof. Chris Mitchell, for their thorough review of my dissertation and help in expressing the result better. I thank Prof. Valtteri Niemi for accepting invitation to act as official opponent of the public defence of my thesis.

I have had the great pleasure to work for Helsinki University of Technology and its successor Aalto University. The funding of this thesis has mainly came from Department of Computer Science where I have been working as university lecturer. In addition, this work has been supported by Tekes as part of the DIMECC Cyber Trust program and the SESSI project, which was funded by Tekes, Nokia, Elisa and FINNET.

I would like to thank all my co-authors in the publications: Linda Staffans (Källström), Ph.D. Simone Leggio, Prof. Jukka Manner, Prof. Tommi Mikkonen, Prof. Kimmo Raatikainen, Jussi Saarinen and Prof. Antti Ylä-Jääski and all the others who worked on the SESSI project about ten years ago; Jani Heikkinen, Pekka Silvekoski, André Andrade and others working in Data Communications Software research group at De-

partment of Computer Science and Engineering at Helsinki University of Technology / Aalto University, and Asko Tontti, Joonas Ruuskanen, Kamran Manzoor, Lauri Haataja and other students who have worked with me. Also, I owe my gratitude to Mari Tyllinen for helping to set up the usability tests.

I wish to thank Henry Haglund and Ursula Koivikko for proofreading my text and, for example, removing “threads” that I sometimes tried to defend against instead of “threats”. Moreover, Dr. Satu Elisa Schaeffer, Natalia Kaijalainen, Rosana De Oliveira Sorva and Jian Liu helped me by translating source documents for Publication VI. Liisa Hirvisalo took the photo of me in Figure 2.1.

I am grateful for all my friends, for example Krista Lankinen, Maikku Sarvas and Ursula Koivikko, who have supported me during my life. I also wish to thank ladies of #tikmammat and people of #assarit and !cs for discussions and help.

Last but not least, I would not have succeeded without my family. My mother Kaija and my father Alpo have supported me during my whole life with everything. Most recently, my mother took care of our kids and laundry, and my father made meals for us when I was finilizing text of this thesis. My brother Santeri listened me when I have had hard times. My mother-in-law, Erika, took care of our children when I was studying and my father-in-law, Tuomo, has offered quiet place to study without the distraction of the Internet in his homestead Hossola. Our kids, Agata and Beata have brought a lot of joy and variation to my life (and hopefully the third one will be patient and wait until after the dissertation day). Finally, Jaakko — I own you everything.

Espoo, October 19, 2016,

Sanna Suoranta

Contents

Preface **1**

Contents **3**

List of Publications **5**

Author's Contribution **7**

List of Figures **9**

List of Abbreviations **11**

1. Introduction **15**

1.1 Motivation 16

1.2 Scope of this Thesis 17

1.3 Research Questions 20

1.4 Research Methodology 20

1.4.1 Proof-of-Concept Prototyping 21

1.4.2 Usability Testing 22

1.4.3 Survey of strong authentication deployments 23

1.5 Summary of Contributions 25

1.6 Organization of the Dissertation 26

2. Network Environment and Online Identity **27**

2.1 The Heterogeneous Network Environment 28

2.2 Key Concepts of Identity Management 29

2.3 Lifecycle of a Digital Identity 33

2.3.1 From Real World to Online Identity 34

2.3.2 Provisioning and Managing an Online Identity 36

2.3.3 Online Authentication and Authorization Methods . 37

2.3.4 Sessions in a Service 40

2.3.5 Accounting and De-provisioning 42
2.4 Single Sign-on and Federated Identity Management 43

3. Improvements to User Authentication and Single Sign-on 53
3.1 Establishing Online Identity 53
3.2 Strong Authentication 56
3.3 Heterogeneous Environment and Ad-hoc Networks 59
3.4 Session Migration between Devices 62
3.5 Logout 64

4. Discussion 67
4.1 Contributions 67
4.2 Possible Future Work 72

5. Conclusion 75

References 77

Publications 87

List of Publications

This thesis consists of an overview and of the following publications which are referred to in the text by their Roman numerals.

I Linda Källström, Simone Leggio, Jukka Manner, Tommi Mikkonen, Kimmo Raatikainen, Jussi Saarinen, Sanna Suoranta, and Antti Ylä-Jääski. A Framework for Seamless Service Interworking in Ad-hoc Networks. *Computer Communications*, 29, pp 3277-3294, Elsevier, June 2006.

II Sanna Suoranta, Jani Heikkinen, and Pekka Silvekoski. Authentication Session Migration. *NORDSEC 2010 The 15th Nordic Conference on Secure IT Systems, LNCS 7127*, Espoo, Finland, pp. 17-32, Springer, October 2012.

III Sanna Suoranta, André Andrade, and Tuomas Aura. Strong Authentication with Mobile Phone. *Information Security, 15th International Conference, ISC2012, LNCS 7483*, Passau, Germany, pp. 70-85, Springer, September 2012.

IV Sanna Suoranta, Asko Tontti, Joonas Ruuskanen, and Tuomas Aura. Logout in Single Sign-on Systems. *Policies and Research in Identity Management, Third IFIP WG 11.6. Working Conference, IDMAN 2013*, London, UK, pp 147-160, Springer, April 2013.

V Sanna Suoranta, Kamran Manzoor, Asko Tontti, Joonas Ruuskanen, and Tuomas Aura. Logout in Single Sign-on Systems: Problems and

solutions. *Journal of Information Security and Applications*, 19, pp 61-77, Elsevier, February 2014.

VI Sanna Suoranta, Lari Haataja, and Tuomas Aura. Electronic Citizen Identities and Strong Authentication. *NORDSEC 2015. The 20th Nordic Conference on Secure IT Systems, LNCS 9417*, Stockholm, Sweden, pp. 213-230, Springer, October 2015.

Author's Contribution

Publication I: "A Framework for Seamless Service Interworking in Ad-hoc Networks"

The author developed the security solution for the framework together with Linda Källström and Timo Kiravuo. Jimmy Kurian implemented the ideas in his Master's thesis. Later, Juri Lumenko and Esa Virtanen improved and implemented slightly different versions of the security solution in their Master's theses, in which the author was the thesis advisor.

Publication II: "Authentication Session Migration"

The author specified the research problem of moving sessions of a service between devices in a way that does not require reauthentication and suggested that moving authentication session would be sufficient in web applications. Jani Heikkinen worked out how to do this by moving session cookies. Pekka Silvekoski implemented the ideas in his Master's thesis, in which the author was the thesis advisor together with Jani Heikkinen.

Publication III: "Strong Authentication with Mobile Phone"

The author designed the solution together with André Andrade and Tuomas Aura. André Andrade implemented the protocol in his Master's thesis, in which the author was the thesis advisor and Tuomas Aura was the supervisor.

Publication IV: "Logout in Single Sign-on Systems"

The author specified the research problem and analyzed the way logout is implemented in different systems including those used at the university. Asko Tontti filled in some technical details in his Bachelor's thesis, in which the author was the thesis advisor, and Joonas Ruuskanen continued the work in his Bachelor's thesis, in which the author acted as an inofficial advisor.

Publication V: "Logout in Single Sign-on Systems: Problems and solutions"

This publication extends Publication IV to solutions for logout. The author designed a solution that offers users both local and single logout in SSO systems that keep a session on the identity provider. Kamran Manzoor implemented a prototype of the author's solution. The author conducted the usability test.

Publication VI: "Electronic Citizen Identities and Strong Authentication"

The author wanted to investigate how real-world identity is linked to digital identity all around the world. Lari Haataja started the survey in his seminar project under the author's supervision. The author rewrote and extended considerably the survey of citizen authentication methods to the G20 countries.

List of Figures

1.1 Lifecycle of a digital identity 17
1.2 Summary of this thesis 19

2.1 Example of an identity, identifier and other attributes. . . . 31
2.2 Kerberos authentication protocol [85]. 44
2.3 Federated network identity and circles of trust [23]. 46
2.4 Service provider initiated communication for SSO Authentication [95]. 47
2.5 OpenID protocol overview [90]. 50

3.1 Trust in Government and Business in 27 countries [32]. . . . 55

List of Abbreviations

3G	The third generation mobile communication system
4G	The fourth generation mobile communication system
AAA	Authentication, Authorization, and Accounting
BAN	Body Area Network
CA	Certificate Authority
DN	Distinguished Name
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
EDGE	Enhanced Data for GSM Evolution
eIDAS	EU Regulation 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
FIM	Federated Identity Management
GAA	General Authentication Architecture
GBA	Generic Bootstrapping Architecture
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HMAC	Hashed Message Authentication Code
HOTP	HMAC-based One-Time Password
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
IBC	Identity-Based Cryptography
IdM	Identity Management
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMD	Implantable Medical Device
IoT	Internet of Things
IP	Internet Protocol

IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6
JSON	JavaScript Object Notation
JWT	JSON Web Token
LAN	Local Area Network
LTE	Long Term Evolution
MANET	Mobile Ad-hoc Network
MFA	Multi-Factor Authentication
MIT	Massachusetts Insititute of Technology
NFC	Near Field Communication
NMT	Nordic Mobile Telephony
OASIS	Organization for the Advancement of Structured Information Standards
OATH	Open Authentication
ObC	On-board Credentials
OP	OpenID Provider
OSI	Open System Interconnection
OTP	One-Time Password
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
REST	Representational State Transfer
RFID	Radio-Frequency Identification
RP	Relying Party
SAML	Security Assertion Markup Language
SDK	Service Develoopment Kit
SIM	Subscriber Identity Module
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SP	Service Provider
SPKI	Simple Public Key Infrastructure
SSO	Single Sign-On
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
U2F	Universal 2nd Factor
UAF	Universal Authentication Framework

UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USIM	Universal Subscriber Identity Module
VANET	Vehicular Ad-hoc Network
WAVE	Wireless Access in Vehicular Environment
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WWW	World Wide Web
XML	Extensible Markup Language
XRI	Extensible Resource Identifier

1. Introduction

From the 1980s, people have had personal computers at their homes for word processing, games, and such activities. Since the World Wide Web became popular in the middle of the 1990s, the home users started to have Internet connections to their home. The same kind of developments happened in the workplace. At the same time, various services started to move to the Internet. This marked the first time when the majority of computer users had no training for it, and the majority of computers were not professionally administered. Soon, mobile networks and devices with Internet connections started to develop and found their way into people's pockets and handbags. Phones and computers became commonplace tools for all jobs and not just for specialists. Mobile devices have developed further, and their price has fallen. Nowadays they are capable of running a wide selection of software developed by third parties and have more computing power than early supercomputers. Software architectures have changed so that most new digital services are online, in the cloud. All this means a change in the population that uses digital services from specialized professionals to ordinary consumers and workers who are not familiar with the "inner life" of computers, networks, or online services. Modern service providers do not have any means to educate all of their users. Thus, the services must be such that any ordinary user can use them as is, or only with a short user manual, which the user typically does not read.

As the web-based online services proliferated, each online service provider implemented its own system for registering and authenticating users. Most used simple password authentication, and the creation of an account did not require any verification of the user's real identity. When banks started to offer online banking, more secure means for authenticating users become necessary for the wider audience than, for example,

corporate staff to get remote access. Moreover, users soon began to suffer from the difficulty of remembering the many passwords [37]. This led to insecure practices, such as reusing the same passwords for multiple services. As a result, many different technologies have been developed in order to improve the security and usability of user authentication and for the management of digital identities. In particular, various single sign-on systems have been deployed both for internal use in organizations and for the open web. In this thesis, the author will explain what kind of solutions exist for managing digital identities and present solutions for some of the remaining problems.

1.1 Motivation

Maler [74] said "identity is a key component for ensuring security, access control, personalization, and even regulatory compliance". There is a wide range of solutions for user authentication and for managing digital identities. Companies and coalitions have proposed many solutions with slightly different aims and scope. Nevertheless, the widely deployed authentication methods for online services have remained unchanged until very recently, and many services still rely on password authentication against a user database maintained by the service itself. In the recent years, single sign-on (SSO) systems have finally been deployed more widely. They can reduce the number of passwords and enable the deployment of alternative authentication methods, such as two-factor authentication. However, all the solutions have shortcomings, either for business or technical reasons.

New ideas and improved identity management services are still being proposed. One reason is the endless race between hackers and security solution developers. Another reason is the changing computing environment with new kinds of services and devices. Moreover, there still remains a lot of work to be done in improving the usability and security of digital identity systems. Ideally, user identification online would be as easy and natural as it is in everyday situations when people meet each other.

The motivation for this thesis research is to understand the whole lifecycle of digital identities and how digital identities are used in online services. The lifecycle of digital identities is illustrated in Figure 1.1. Understanding both the technical and non-technical parts of the system helps to identify gaps and opportunities for improvement. This enables us to de-

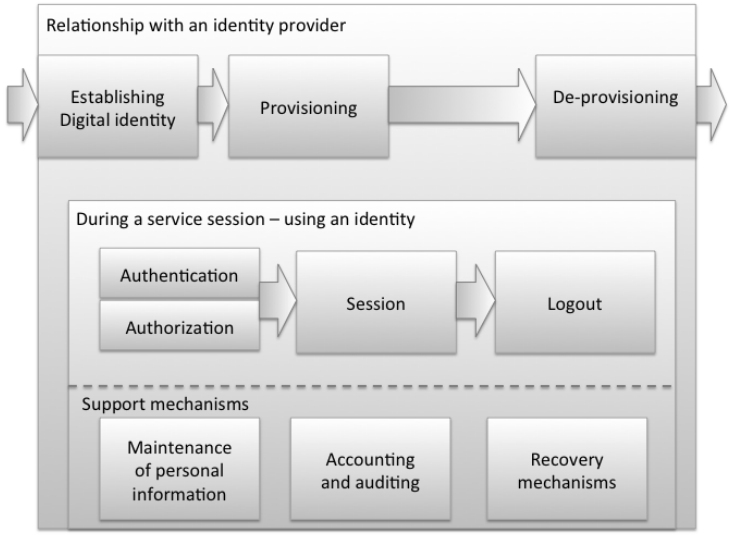

Figure 1.1. Lifecycle of a digital identity

velop technical solutions that make the world of digital identity better for ordinary users. As Matt Bishop has said, understanding the entire process, not just the computer system, helps to concentrate on the essential since not all solutions are technical [18].

1.2 Scope of this Thesis

As mentioned above, understanding the whole lifecycle of digital identity is important: how it is established, managed, used in services, and how it can be deleted. Figure 1.2 gives an overview of the scope of the thesis and describes its research contributions. The top part of the figure illustrates the real world identity that begins from the birth of a child and ends with her decease –the time advances from left to right in the figure. The identity is the same during the whole life of a person, even if she changes her name or gender, but her identifiers can change and she may have several identifiers as will be described in Section 2.2. When the person wants to use a service that is limited to certain people, her identity or her right to use the service will be verified. There is no logout procedure in the end of a real world service session. Publication VI discusses how to establish a digital identity based on a real world identity. Most of the figure illustrates identity in the digital world and online services. There are two ways to create identity in the digital world: either it is based on an offi-

cial identity in the real world or it can be self-established. Either way, an identity provider bootstraps a digital identity that can be used in various online services. This thesis mainly considers identities in federated service environment. Roughly, when a user wants to use an online service, an identity provider first verifies her identity (authentication in the figure). One way to provide strong user authentication for services is described in Publication III. The identity provider may establish an identity session that other services may later use. A service defines what rights (authorization in the figure) the user has in the service and establishes a service session. In Figure 1.2, Service Session D3 refers to the ad-hoc network case discussed in Publication I that describes how users and devices can be authenticated without a connection to online services such as identity providers. The Service Session D2 refers to migrating login sessions between devices described in Publication II. The Identity Session A and the Service Session D1 in the figure describes different logging out possibilities in single sign-on environments. The problems and solutions of logout are discussed in Publications IV and V. Finally in the digital world, the person may want to end her relationship with an identity provider (or service provider), which is done in de-provisioning, but that is out of scope of this thesis.

The focus of the thesis is on single sign-on systems since they reduce the need for service-specific digital identities, thus reducing the work load on users. Moreover, we are primarily interested in strong authentication methods that can link the real world identity of users to the digital world. However, all services do not need such digital identities, and self-established identities and weaker authentication can equally benefit from improvements to single sign-on.

Since mobile devices have become so popular among users, the thesis considers what additions they bring to the management of digital identities. Mobile phones can at least provide a second communication channel that can be used for two-factor authentication, since the mobile phone account is authenticated to the mobile network using a smart card. Also, mobile devices sometimes form ad-hoc networks that have no connection to services on the Internet. This means that online connections to identity providers cannot be used but something else is needed for both authenticating users and defining which device can offer services.

Some relevant topics are not covered in this thesis: role based and attribute based access control, message authentication, trusted hardware,

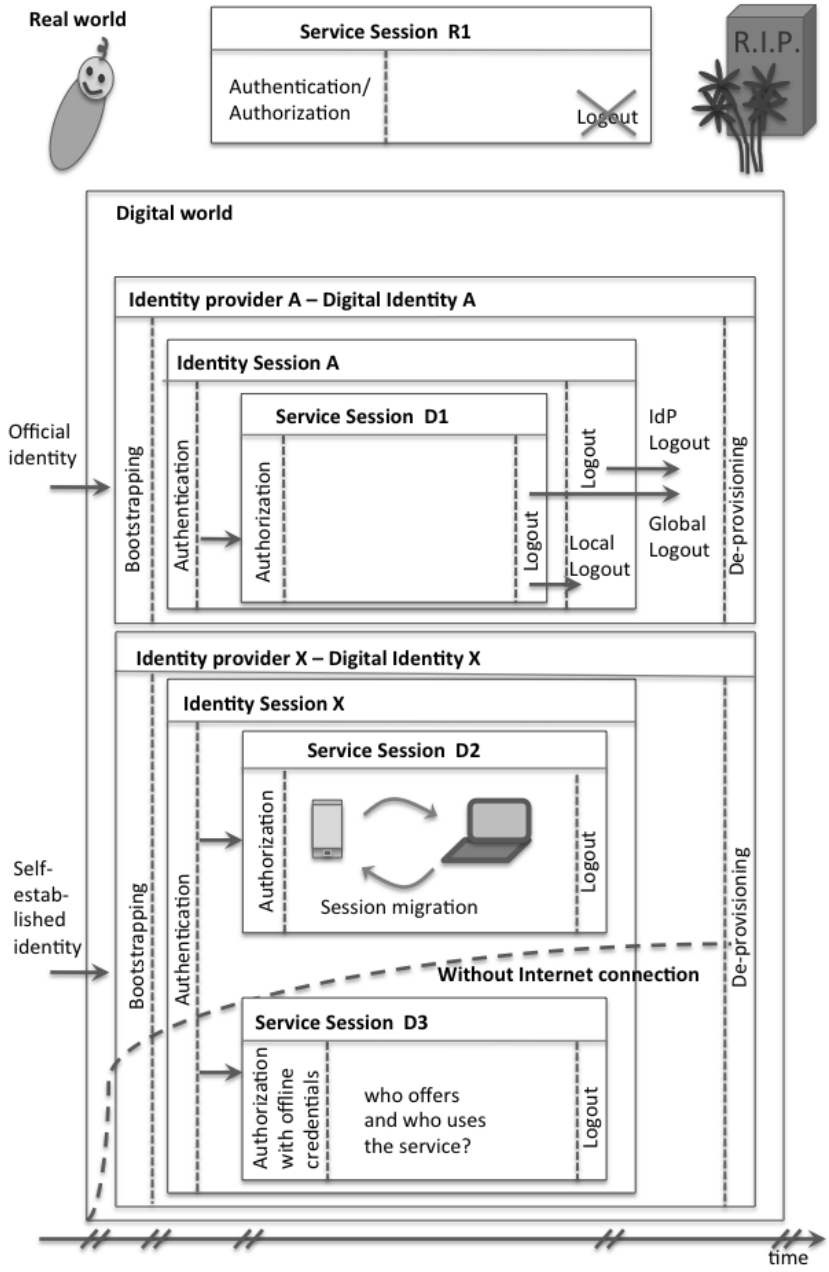

Figure 1.2. Summary of this thesis

and privacy or trust issues of managing digital identities. Furthermore, service, server and device authentication as such is not considered, except in the case of ad-hoc networks where the user may want to define which devices of other users can provide services to her.

1.3 Research Questions

The goal of this thesis is to solve practical problems in digital identity management systems that provide single sign-on service. The work has identified some gaps in currently used systems: what is the origin of a digital identity, when it is established, what new aspects do mobile devices bring to the management of digital identity and user sessions, and how are the end of user sessions handled? These have led to the following research questions:

Research Question 1: How can a real world identity be linked to online world identity in a distributed and even international environment in a strong way?

Research Question 2: Mobile devices provide a handy way to access online services, but what new requirements and opportunities do the mobile devices bring to digital identity management?

Research Question 3: Existing SSO solutions are focused on the initial authentication at the beginning of a identity and service sessions, but what security issues arise later in the session lifetime?

1.4 Research Methodology

In science, research methods form an essential part of the work. The methods should provide reliability and validity to the research. Reliability means that someone else could repeat the research and end up with the same conclusions. Validity means that the conclusions made based on the research are correct. In engineering research, an additional important issue is relevance or applicability of the research. In order to investigate a broad topic such as the lifecycle of digital identity, using multiple research

methods is likely to produce a wider perspective and give more relevant answers to the questions.

Commonly used methods in computer science and software systems research are modeling, simulation, and theoretical and experimental methods. In modeling, a simplified model of a phenomenon is compared to its real world version. Simulation is also based on modeling, but the point is more to change some variables in the model or give a different input for the system, and to see what happens. Theoretical computer science uses logic and mathematics to model phenomena and to prove that, for example, something can be computed, or that a problem is solvable in finite time. Its target is to improve algorithms and data structures or to classify computing problems. Experimental computer science creates experiments or prototypes based on hypotheses and tests how they work. The last mentioned method is used in this thesis because it is suitable for testing new ideas directly in the environment where they would be deployed..

In this thesis project, prototyping and user studies were chosen as suitable research methods for resolving technical questions in managing digital identities. For finding out how identity is managed in the real world, a literature survey of governmental reports and online documentation was conducted. We did not conduct formal or informal security evaluations for the developed prototypes because it would have required more resources than were available. More through security evaluation would be needed before broad deployment of the developed technologies. Next, the research methodology is described in more detail.

1.4.1 Proof-of-Concept Prototyping

Publications II and III use prototyping as the research method. Both were implemented as Master's thesis projects where the author was the advisor. Moreover, in Publication V made use of prototyping in two ways: first, it showed that it is possible to implement a service with two options, local and global logout, and second, the usability test was conducted with the prototype. This method has helped us to answer to Research Questions 2 and 3.

Brooks [38] suggested rapid prototyping in software projects for checking that customer requirements are understood and attained and all necessary interfaces have been taken care of. A prototype simulates the main tasks of the system but it may not be fully functional or work on the target

platform [38]. Brooks emphasised the iterativeness of software projects. A proof-of-concept prototype is a typical way to show that an idea is feasible, and it is used in the early phases of design [115]. Proof-of-concept prototypes can have different levels of functionality from paper prototypes to fully functional software, and they are also often needed in user testing during the design process. The point is not the proof-of-concept prototype itself but demonstrating that it is possible to implement the idea. Later prototypes can show that the production is feasible, production methods are successful and the manufacturing process is efficient [115]. The features of the prototypes can be evaluated various ways; for example, their performance and functionality can be compared to pre-set requirements or similar systems. To conclude, proof-of-concept prototyping is a good way to test whether an idea can be implemented. However, it is far from a working implementation that can be deployed to users as a product. Moreover, it does not show the only way or the best way to implement the system.

1.4.2 Usability Testing

User studies can give much information about how people are using services and systems. In Publication V, we conducted a usability test for logout in an SSO system in order to answer to Research Question 3. Usability test in laboratory settings was chosen instead of an online test because the test users could elaborate their thoughts in an interview conducted after the moderated test.

Historically, security and usability have been seen as orthogonal to each other: a system that is truly secure has low usability, and a system that is usable cannot be secure [5]. Later, user-centered security approach wanted to synthesize usability and security since users' needs were seen as the primary motivator for the designed security features in a system [119]. Moreover, security is also considered to be as strong as is its weakest link, and if this is the user, then the solution must help her to act in a more secure manner [28]. Nowadays, users are taken into account in the design process of secure systems. One way to do this is to ask ordinary users to test a system before it is ready. The main point of usability testing is debugging, i.e. finding problems in the system [86]. Thus, usability testing requires a much smaller sample of users than is needed in behavioral sciences such as psychology that are interested in how a population behaves.

Usability testing requires determining the goals of the test, planning of tasks the user will do in the test, creating scenarios for the usability test, deciding how to recruit participants, and defining how to collect the feedback [13]. The goal of the test should not be too wide. For goal setting, Barnum [13] suggests using the following five criteria: efficient (can user find necessary information), effective (can user do the task), engaging (is the system satisfying or enjoyable), error tolerant (did user counter errors and did she recover), and easy to learn (is help needed). The test can be done in any phase of a product development, for example using pictures drawn on paper or a prototype of the product. The scenario describes what a test participant is trying to do and gives her a role, but it should not reveal the goal of the test. It contains all the tasks of the test. Choosing participants depends on the goals of the task. Background variables such as age, gender, education, and language can affect the results, and thus this information is usually collected and presented together with the data and results [13].

Usability tests can be conducted in a laboratory, meeting room, office, or almost anywhere. More essential than the place is how to record the findings of the tests: the participants can be video or audio recorded, taped, or the moderator of the test can take notes. Usually the moderator asks the participants to think out loud, saying what they are trying to do and what they like or not, or even to ask questions if something is confusing. Information about the participant, tasks and the test are often collected with questionnaires and, for example, semi-structured interviews. After the test, the results are analysed: what positive or negative findings the participants found, and whether something surprising was encountered. The findings are categorized or grouped, or individual tasks can be analysed separately. Often statistical methods are used. Because users are asked to think aloud, even a single user can provide valuable feedback for the usability of the test subject. After the analysis, recommendations for fixing the system can be made [13].

1.4.3 Survey of strong authentication deployments

The research method used in Publication VI was based on technical and online documentation. Usually in a literature review, the sources and databases where the research are targeted are defined first. Then, search words are defined and the search is executed. In an unstructured literature review, the search is expanded opportunistically to promising direc-

tions. All the found articles are then read and analysed, and a synthesis is formed based on the articles.

In the survey conducted in Publication VI, the sources of information were specifications and documentations of governmental organizations, which were publicly available, and reports published by the European Union and OECD. In addition, some academic research was reviewed. The author tried to find solutions that citizens could use either to log in to governmental services or that provided a verifiable real-world identity for third-party online services. The Google search engine with English search terms, such as electronic identification, citizen identity, digital identification, and electronic identity card was used. Furthermore, information in French and Spanish was searched, and, in addition to Google translate service, native speaking coworkers and friends helped to translate interesting webpages from Chinese, Portuguese and Russian. In addition, many improvements for local implementations were suggested in the scientific literature and conferences. These sources provided valuable information about problems that citizen authentication solutions have faced in various countries. This method was chosen to answer to Research Quesion 1 because many countries already have solutions for linking real world identity to online identity, but only some of them seem be succesfully implemented and deployed while others have encountered problems.

The survey based on governmental webpages in multinational environment has some shortcomings. From a reliability point of view, anyone can repeat the survey but because legislation and technical solutions are changing over time, she could end up with different conclusions. Validity can also be questioned since the search may not be complete. Governmental organizations in different countries may have different publication policy, and thus information available online may be scarse and scattered. In different countries, the responsibility for defining and providing digital identity is organized in various ways. Moreover, web pages may have old information that is updated or redefined somewhere else. Thus, the conclusions in Publication VI are somewhat bound to the time, spring 2015, when they were made. However, understanding the wider context of the technical research helps in finding solutions that are not technical. Furthermore, political, cultural and historical factors have had an influence on the technology acceptance, which varies between countries.

1.5 Summary of Contributions

As a university lecturer, the author's research has been conducted together with Master and Bachelor students. In most cases, the author has specified the research problem and worked out the solution ideas with the students, who have then done the technical implementations or experiments with the author's supervision. The final papers were written by the author using text from the student's thesis as a starting point.

In this thesis, the author found ways to improve digital identity management of users in single sign-on systems. Mainly she concentrated on what happens in the beginning, during, and at the end of a service session. In addition, she was interested in how to authenticate users strongly when a digital identity is created or when a user authenticates herself to a service.

Publication VI gives the results of a survey how electronic identification of citizens works in over 20 countries. These solutions can often be used to establish digital identities in private sector services or, in some countries, services can use a governmental authentication service to authenticate their users for every service session.

Nowadays, mobile devices can be used in authenticating users to services. Publication III provides a proof-of-concept prototype that shows that a mobile phone operator is not needed for strong user authentication when two-factor authentication is used. Moreover, the service does not need to know the user's mobile phone number beforehand. Publication I addresses an ad-hoc network scenario where just authenticating users for services is not enough, but a policy for define which service providers are allowed to offer services for the user's device is also needed. Furthermore, a user may want to change devices during a service session. Publication II gives a simple way to migrate an authentication session from one device to another one without reauthentication.

At the end of a service session, the author found out that logout is problematic when a service uses single sign-on for authenticating its users: when the user presses the logout button, should she be logged out from only that service or also from the identity provider, or even from all other services that use the same identity provider? Publication IV describes the problem and Publication V presents a proof-of-concept prototype where users could choose between local logout from a single service or logout from the identity provider. Publication V also conducted a usability test

that shows that users could understand the difference between the two options.

1.6 Organization of the Dissertation

The next chapter describes our heterogeneous network environment, the lifecycle of online identity, and single sign-on and federated identity management as background information. Then, in Chapter 3, the improvements that this work provides are presented and compared to other later solutions. Then, a summary of answers to the research questions is given in Chapter 4, and Chapter 5 concludes the thesis. The published articles, which contain the main research contributions of the thesis, follow the conclusions.

2. Network Environment and Online Identity

Human beings can recognise someone or something familiar in a fraction of second. In the human brain, the neurons of the medial temporal lobe react when pictures of faces or objects are shown. For example, Quian Quiroga et al. measured neural activity of epilepsy patients using single cell measurements and found a cell that reacted only when pictures of actress Jennifer Aniston were shown to one of the patients [94]. Of course, recognition is not always so straightforward in the real world. The real world identity is usually local: even though authorities in most countries can give official identity certificates to the country's citizens, that does not cover all aspects of identity. Also, when introducing new people to someone, usually no evidence of their identity is presented.

In the digital world, identity is more or less the same: someone can claim any identity when, for example, registering with a service. The verification of an identity often requires only a working email address, not any proof of a real-world identity. However, the devices that someone owns and the various connection channels by means of which she can be reached can provide the means to verify her identity. For example, since a mobile phone operator can send a bill to her contact address (email or postal address) and if she pays the bill, the mobile operator may conclude that she is who she claims to be. The development of mobile phone networks and devices that use wireless communication has set users free from being just in one place the ways in which the same user connects to online services has become more diverse. So, too, identification of users and their authentication to online services must be available on a range of networks and devices, and there certainly is no one-to-one mapping between users and devices.

Next, we brefly describe the development of the current network environment. The key concepts of online identity are then defined. Both of these issues are also connected to the articles of this thesis.

2.1 The Heterogeneous Network Environment

Nowadays using the Internet at home and with mobile devices is common. Phone operators have become Internet service providers and use their old landline phone networks to offer Internet connections. Devices at home can be connected to the Internet with broadband connections delivered on the old wired phone networks or the cable television networks or, increasingly, newly laid fiber-optic data connections. In addition, people connect to the Internet using their mobile phones, tablets, laptop computers, and even with smart watches anywhere they are. In Europe, the two most commonly used access methods for the mobile Internet are mobile phone networks and wireless LAN hotspots. Some mobile phone network operators offer flat-rate data connections, and, for example, in some rural areas in Finland, the mobile phone network is the only way to connect to the Internet. Next, a brief history of wireless Internet connectivity is given and the current network environment is described.

The Nordic countries have been forerunners in the use of mobile phone networks. The first fully automatic cellular networks, NMT (Nordisk MobilTelefoni, Nordic Mobile Telephony), was operational in Sweden and Norway from 1981 and Denmark and Finland from 1982. The NMT network also offered data connections, but they were very slow, only 380 bit/s. The first data call in the second-generation GSM (Global System for Mobile communications) network was performed in 1993 [34]. The use of GSM for Internet connections took a big step forward when the General Packet Radio Service (GPRS) added packet-oriented data service for the originally circuit-switched GSM networks. In 2003, the Enhanced Data rates for GSM Evolution (EDGE) technology improved data transmission rates making web browsing usable in practice with mobile phones. In the early 2000s, the mobile operators launched the third generation (3G) Universal Mobile Telecommunications System (UMTS) networks. Since around 2010, the mobile phone operators have been moving to the fourth generation (4G) Long Term Evolution (LTE) networks that are so-called all-IP-networks, running the same protocol stack that is used in the Internet.

At the same time as the mobile phone networks developed, wireless data networks also developed. The Institute of Electrical and Electronics Engineers (IEEE) has standardized two wireless network technologies: the IEEE 802.16 standard, usually called WiMAX (Worldwide Interoperability for Microwave Access), for long range wireless Internet access, and the IEEE 802.11 standard called Wi-Fi (or WLAN, Wireless Local Area Network) for local area networks. Wi-Fi networks provide two kinds of interoperability modes: an infrastructure mode where an access point provides a connection to the Internet, and an ad-hoc mode where devices near each other can connect and provide services to each other. At the turn of the new millennium, Mobile Ad-hoc Networks (MANETs) were a hot topic in research and, for example, dozens of routing protocols were developed for multihop ad-hoc networks. We developed in Publication I a way for users in a MANET to provide services to other users regardless of their location in the network and to define a policy to govern who can use or provide the services. The services could be reached from the MANET or from the Internet.

The mobile phone networks have their own technologies for identifying customers and their devices, and these can sometimes be used when identifying clients to online services. These will be briefly introduced later in Section 2.3.3. Wi-Fi networks usually only use password authentication for the access point, and all client devices often use the same password, so this cannot be used as an authentication method for services. But before going into details of identifying and authenticating clients or users, we will define the key concepts of identity management and the lifecycle of identity.

2.2 Key Concepts of Identity Management

According to the Merriam-Webster's encyclopedia, *identity* is something that distinguishes an entity from other entities [76]. When talking about human beings, according to Dick Hardt, identity is "who you are, what you like, what you say about yourself, and what others say about you" [47]. Who someone is depends on the environment: for example, a person's identity includes her work identity and her home identity. Something about the person is revealed when telling where the person lives, what she does for her living, where she studied and when she was born. What she likes also indicates something about her identity since she can be

identified in an environment as that individual who likes to use Linux, wears black and rides a Harley-Davidson. Moreover, reputation is also part of identity. Thus, identity consists of many distinguishing attributes that can be grouped to form various kinds of sub-identities for a person. In addition to human beings, other entities, for example a mobile phone, a laptop computer or a family pet dog, have an identity, and they can be identified to be just that entity in question; however, such identities are out of the scope of this work.

An attribute that can be used to identify an entity is an *identifier*. According to Camp [21], an identifier is a unique name in a namespace for an entity such as a distinct person, thing, or place. If an attribute is used as an identifier in an online environment, its uniqueness is important since identifiers are used as search keys in databases. Sometimes a combination of attributes is used to identify a person. One entity can have multiple identifiers. The identifier should be difficult or impossible to change. For example, a person can lie about her birthday, but it cannot be changed [21].

The identifier is often mixed with the identity concept that is much broader: Identifiers are attributes that can be used to separate someone or something from others, and an entity can have many identifying attributes. Often, when using a service, a person is identified by a name or some other information, such as username, email address, social security number, client account number, or passport number. A service is usually identified based on its name and location (physical or logical, e.g. universal resource locator, URL) and visual signs such as company logos or web page layout. The identity is more than an identifier. For example, the name of a person, which is an identifier, does not reveal what she does for living and other aspects of her identity. Figure 2.1 depicts some aspects of the author's identity (at home, at work and as a student) as an example and gives some attributes that can be use for identifying her, and other attributes that do not distinguish her from others. Clauss and Köhntopp [26] saw lack of privacy and control of users' own information as a problem. They suggested an identity management system where pseudonyms separate aspects of the user's identity in a way that gives her more control.

Often identifiers have a *local scope* and they may not be unique outside that scope. For example, many people have namesakes but they can be distinguished from each others using other attributes such as occupa-

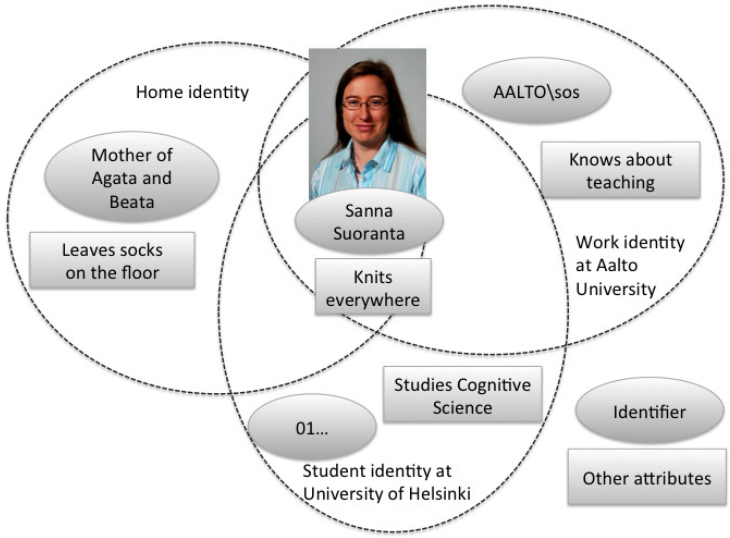

Figure 2.1. Example of an identity, identifier and other attributes.

tion or sound of voice. Linking identifiers together can provide a *global identifier*. For example, Sanna Suoranta who works at the Department of Computer Science at Aalto University is a distinct person. Usually, there is a single person that has a certain identifier but that person may also have other identifiers. The X.509 certificate standard [53] provides a distinguished identifier in which the link between a person and an identifier is supposed to be a one-to-one relation – the person when using the standard would be always identified with the same identifier. Because of privacy concerns and the lack of global directory service, among other reasons, these kind of distinguished identifiers have not been universally adopted.

When encountering a person or other thing, people try to *identify* her or it. As mentioned above, people can usually identify familiar entities fast and automatically because the human brain is specialized to such tasks. For new acquaintances, one can just claim an identity, for example by *introducing* oneself "Hi, I'm Sanna", or someone who knows both parties can act as an *introducer*. For more official situations, for example opening a bank account, the identity is usually *verified* using an official identity document, such as a passport, identity card or driver's license, *issued* by state authorities. These documents provide *proofs* of an identity and they can be used to *verify* it.

When discussing with other people over communications networks, introducing new participants or recognizing old ones has to be done differently since the automatic recognition methods of the human brain do not work. Of course, if the video or voice quality is excellent, one can recognize a familiar face or voice, but that does not work for text-based communication, web services or with a poor quality communication channel. Moreover, the user identification for a service offered online often includes passing an *access control* where the entity is recognized. This can be done with a method called *authentication*, namely checking that the identity of an entity is as claimed. Usually authentication is based on something known like a password, something possessed such as a smart card, or something biometrically unique (or almost unique) like fingerprints. An authentication method that combines two of these is called *two-factor authentication* and, if a method combines several of them, it is called *multi-factor authentication (MFA)*. *Strong authentication* requires that a user's real world identity is verified before giving her credentials for electronic authentication and that two-factor authentication is used. This corresponds the *substantial assurance level* for electronic identification defined in the European Commission Implementing Regulation [108] that specifies technical requirements for the electronic identification and trust services for electronic transactions in the internal market of the European Union (eIDAS regulation) [109] .

Another way to check that the user has the right to use a service is *authorization*. Authorization can allow anonymous access if the right to use the service is not linked to verifying the identity but just checking that the entity requesting access has the necessary credentials. For example, when entering a movie theater, a ticket is shown to the doorman, and if it is valid, access is allowed. To go into a bar, the doorman can ask for identification and can check from an identity document that the person is old enough to legally drink alcohol and that she looks the same as the picture in the document – the name of the person is irrelevant even though it is given in the identity document.

Access control of a digital service matches the attributes given in the authentication or authorization process to those stored in a user database. The information that is stored in the database forms the *digital identity* that can be used to identify the user within the service. Sullivan [106] calls all this information the "database identity" and the information used in the authentication step the "token identity". If the information is stored

in several databases, the digital identity of an entity is such that no single party knows all its attributes, and an entity can have many unlinkable digital identities. For example, a university student who works in a company has identifying attributes at least in the databases of the university and the company, not to mention all the other services she is using online. In the university database, she may have an attribute that reveals her role to be a student, and she can have different email address than in the company's employee database. She can change her name when she marries and have new namesakes that study in the same place. She may forget to provide information about the name change to all the places where she has records; she may not even be aware of all of them. Nevertheless, she is the same person. Because many of the attributes stored in the databases may change during the life of a person, Bohm et al. see identity as a relationship, not as a collection of attributes [19].

According to Camp [21], many problems of digital identity originate from the paper identity documents that have to be self-proving and long-lived. In the digital world, these properties can cause a lot of damage in the form of privacy violations and identity thefts. Sullivan [106] suggests that authentication is different in the real world where a passport merely supports the claimed identity and decision making, and in the online world where the provided and stored information is compared and, if they match, the authentication decision is made automatically.

2.3 Lifecycle of a Digital Identity

Identity management means managing the digital accounts of users. It covers the creation of digital identities, verification of the user's identity in the real world (if needed), authorization and issuing of credentials, recovery of lost credentials, session management in a service, and finally cleaning of the databases when an identity is not needed any more. Many security companies have developed Enterprise Identity Management (IdM) systems or Identity and Access Management (IAM) solutions that provide identity management for organizations to manage, for example, employees' access rights. For customers of a service, the same lifecycle of digital identity applies.

Federated identity management (FIM) systems address situations where several providers offer services by linking accounts in different services so that, for example, one service accepts verification of identity from another

service. If a FIM system provides access to several services with one authentication, it can be called a *single sign-on* system. Such systems help users since the same authentication credentials work for several related services. Pashalidis and Mitchell [91] classified SSO systems into pseudo-SSO and true-SSO systems. The first involves a script that executes the required authentication mechanism where each service has separate credentials. The latter is a union of service providers that accept a user authentication provided by a common authentication service provider. Another aspect they use for classification is the location of the authentication service. For example, a password manager is a local pseudo-SSO system since it is local to a user's device. If the password manager is located in an external server in the Internet, the system is categorized as proxy-based pseudo-SSO system.

Both in FIM and SSO systems, an *identity provider (IdP)* or *asserting party* authenticates users on behalf of a service, called a *service provider (SP)* or *relying party (RP)* depending on the technology. A service might be able to use several IdPs, and a single IdP can provide authentication for several services. Next, the parts of the lifecycle of a digital identity in general are presented.

2.3.1 From Real World to Online Identity

On a global scale, the source of a person's identity is the state where she was born. Vital events are stored in the civil registration system of the state, and the primary purpose of the civil registration is establishing the legal documents provided by law [112]. A birth certificate is a document of a vital record. The United Nations' Convention on the Right of the Child [111] states that a born child should be registered immediately, and that the child has the right "to preserve his or her identity, including nationality, name and family relations". All members of the United Nations have signed the document but the United States has not ratified it. Registering the birth or the birth certificate gives the right to obtain education, health care, voting, and a passport. It also proves the age of a child. According to UNICEF [110], approximately 65% of children under five have been registered worldwide but nearly 230 million children are unregistered. The lowest registration rates are in South Asia and in sub-Saharan Africa where 39% and 44%, respectively, of the children (in Somalia only 3%) have been registered. Low level of maternal education,

living in a rural area, and ethnicity or religion in some countries all affect the likelihood of birth registration.

When applying for a first passport or identity document, the officers can ask for a birth certificate. However, the birth certificate may not contain anything that actually links it to its rightful owner [19]. Another way of authenticating the applicant is to rely on someone whose identity and reputation is verified to introduce the applicant of a passport, for example the parents of a child. Even after one has obtained an identity document with a photograph, comparing the picture in an identity document to a perceived face is error-prone. Kemp et al. [59] organized an experiment where test persons went shopping with credit cards that had one of their own picture, a slightly modified picture, a picture of someone who looked like the test person, or a picture of someone that did not look like the test person: the rates of acceptance of false cards and rejection of valid cards were both high – in total only 67% of the decisions were correct. Officers issuing passports also have a third way to verify applicant's identity. For example in Finland, they can ask questions such as "what was your previous home address" and "what is your grandmother's maiden name" and compare the knowledge of the applicant to the information stored on databases about her, and base the verification of the identity on that. However, this method has its problems nowadays because many questions are easy to solve with efficient search engines [21].

After getting the first official identity document, it can be used when renewing the document later or when applying for another type of official document. Nowadays many states have an authentication service or offer electronic identification documents that can also be used in the online world either in governmental or private sector services. Most of these are considered to provide strong authentication since they, for example, combine a PIN code with a physical token, i.e. they provide two-factor authentication.

The above approach describes how a global identity is created and attested to by a state. However, much of our communication occurs at a local scale, between people who have never had their identities verified by any official source. Usually, someone just claims an identity or someone else acts as an introducer. The distance between people through common acquaintances are surprisingly short: Backstrom et al. [11] calculated that the average distance between active Facebook users (about 721 million users and about 69 billion friendship links) to be 4.74 for the

shortest path in the social network graph, and that is without links provided by non-Facebook members. An online identity can be anchored to a real world identity through, for example, a relationship with a friend or institutional email account. In the online world, an identity can also be local in a service. Additionally, services such as LinkedIn and Facebook can provide linking through a common acquaintance. Claiming an identity and investing in it works similarly in both the real and online worlds. Even if a person has initially lied about her name, if she has subsequently used it for a long time in various connections and accomplished, for example, a doctoral degree with that name, she will probably want to be known with that name later on, too. Moreover, in the online world, people usually focus on the positive sides of their identity and give a polished picture of themselves [118]. In England, someone trustworthy, for example a college professor, can introduce people that do not have a birth certificate but have been known for long time with a certain name to governmental officers. In the online world, such an identity is not generally considered strong, even though this might be the ambition of some social media services.

Publication VI describes what kinds of citizen authentication methods for online use are offered around the world. Many states offer electronic identification cards that can be used to prove identity in online actions. In addition to the smart card based solutions, some states offer identity provider services for governmental and third-party services using some other means of authentication. As interesting as this topic would be, using local online identities and human-to-human authentication are outside the scope of this thesis.

2.3.2 Provisioning and Managing an Online Identity

Online services often require registration before the user can access the service. This does not necessarily mean that the real world identity of the user is verified in the registration, but information is stored in the database of the service provider in order to recognize the user when she returns later. Registration can be required for several reasons: the service may be subject to a charge, the user may personalize the service to gain a better user experience, or registration can be required by law, for example showing that the user is of age. In many countries, legislation requires that only necessary information should be collected, but it is hard to define what is necessary.

For more formal relationships, for example creating an online account for a new university student or a new employee, the user's real world identity is often verified. This can be done either in a face-to-face communication with an officer of the organization, or by using other online identities, for example those offered by a state, to bootstrap the local identity. Moreover, the user's role is often defined in the provisioning. For example, the role of student or staff can be assigned to a new university account, and this can determine which services of the university can be accessed and what the user's entitlements in these services are.

During a customer relationship, information about the user can change. She may change her name, email address, or phone number, she may gain or lose rights, and she can lose her credentials. Often services require changes, too, for example changing passwords every half a year. Identity management must handle all these situations.

2.3.3 Online Authentication and Authorization Methods

As mentioned above, authentication is usually based on something known, something possessed or on a biometric identifier. Typically, web services use *passwords* to protect user accounts even though they are often not considered to provide good protection because they are not user-friendly. Good passwords are hard to remember, and users circumvent security policies in order to manage their passwords and because they do not understand how passwords can be cracked [3]. In 2006, according to a study that had 500 000 Windows Live Toolbar users as participants, the average user had about 25 accounts with 6.5 different passwords, and she typed on average 8 passwords per day to different services [37]. Single sign-on systems may have since then reduced the number of service-specific passwords. However, if computer screensaver locking is used to protect access to services, the user may need to type the screensaver password over 300 times a day [52], which may be irritating. More information about SSO systems will be provided in Section 2.4; authentication methods are described next.

Password authentication is the simplest form of *challenge–response* authentication. Typically, the authenticating server will retain a hash of the password rather than a cleartext version. In cryptographic challenge–response authentication, the challenge is a random value and only legitimate partners can generate the correct response from the password and the callenge. Some challenge–response authentication protocols also

provide mutual authentication where both parties can verify each other's identity. For example, the Kerberos protocol provides mutual authentication over an untrusted network with the help of a trusted third party [85]. The Kerberos protocol uses secret-key cryptography and hence requires all clients and services to share secret keys with the authentication server; it is based on the pioneering work of Needham and Schroeder [83]. Kerberos will be described in more detail in Section 2.4.

One-time-passwords (OTPs) are one way of making authentication stronger. As the name indicates, an OTP password is valid for only one login, thus preventing replay attacks. There are several ways to distribute these passwords, and in practice many are based on proprietary solutions. The simplest is a list of OTP passwords on a piece of paper, which is still used for example in online banking. Another sequence-based OTP is S/KEY [44] used in Linux or BSD where, to put it simply, a password is a hash of a previous password that is a hash of a previous password, etc [65].

OTPs can also be based on a separate *hardware token*. For example, RSA SecurID [100] is a small device that generates a password based on a clock that is synchronized with the authentication server. The RSA SecurID token has a small display that shows a numeric code, and the user types in the code when authenticating to a service. However, a display is not necessary for an OTP token. For example, YubiKey is a small USB token, and when an OTP password is requested, the user just presses the button on the YubiKey token [116]. There are also open solutions, including one developed by the Iniative for Open Authentication (OATH) known as the HMAC-Based One-Time Password Algorithm (HOTP) [82]. This scheme offers a challenge-based algorithm that anyone can implement in hardware or software. Moreover, widespread use of mobile phones has opened the possibility to use them as a token or delivery channel for OTPs. For example, mobile phones have trusted hardware that can be used to manage OTPs [81], or a service may require the user to type in an additional code sent to her as a short-message-service (SMS) message. OTP solutions provide two-factor authentication that is generally considered to be stronger than, for example, a simple password. Publication III presents one solution that implements two-factor authentication for the Shibboleth SSO system using a mobile device as the token.

In addition to paper tokens such as OTP lists, other physical devices can provide cryptographic credentials for authentication. As mobile phones

have become widely used all around the world, technology that is used to identify the phone to the network operator has been seen as one way to authenticate users. The mobile phone network identifies the mobile phone through a smart card called the Subscriber Identity Module (SIM) for GSM or the Universal Subscriber Identity Module (USIM) for 3G. (Later in this thesis, we will call them both SIM cards for better readability.) When someone opens a new subscription with a mobile phone operator, her identity and contact information is typically checked from an official identity document because legislation in many countries requires phone companies to keep track of who called whom and when. However, prepaid subscriptions also exist, for which the identity of the user may not be checked, and these obviously cannot be used for authentication based on the subscription.

A SIM card contains keys for authenticating the subscription and encrypting the communication over the air interface between the mobile phone and the base stations. The user can choose a PIN code that gives access to the card and the services of the mobile phone network, including the network connection. The mobile phone can be considered as a combination of something known (the PIN code) and something possessed (the SIM card), and thus it becomes a tool for two-factor authentication. This has made the mobile phone attractive from the application-level service point of view, and the mobile broadband standardization organization, 3GPP, has responded. It has standardized the Generic Bootstrapping Architecture (GBA) [1] that allows third-party services to use the mobile network infrastructure for authenticating users. However, the standard has not been widely deployed. The SIM card is successfully used to identify the device in the lower levels of the communication protocol stack for Internet services that were not originally available in the mobile phone network. Moreover, the mobile phone itself can have a Trusted Execution Environment (TEE) to store sensitive information and provide a safe execution environment for security software and credential storage [42].

The third category of authentication methods is based on *biometric information*. Many human characteristics are considered to be unique enough to identify one individual. These charasteristics need to be universal in the sense that everyone has the characteristic, permanent so that they do not change or cannot be altered, and capable of being collected and quantified [54]. Biometric authentication can be based on physiological or behavioral characteristics. For example, facial image (optical or infrared),

hand and finger geometry, iris and retina of the eye, signature, voice, vein geometry, keystroke patterns, gait, and finger- and palm-print images are used or under investigation to be used in biometric authentication. In the enrollment phase, the biometric characteristic is scanned, its essential features are extracted and a template is stored in a database. When the user wants to authenticate, a fresh scan of the characteristic is compared to that stored in the database. The system must have good performance, that is, it must be accurate, fast and robust; it must be acceptable so that people are willing to use the biometric identifier; and it must be hard to circumvent.

Biometric authentication has long been discussed but historically the scanning devices have been expensive. Finally, in 2004, IBM introduced a laptop that had a built in fingerprint reader [41], and in 2011 Motorola [43] and in 2013 Apple [8] released mobile phones with fingerprint readers. However, biometric authentication has not proven to be as secure as once hoped [89]. Face and voice are not secret, fingerprints can be found everywhere, and lighting may be too dim for visual authentication or hands may be too cold for scanning. So far, biometric authentication is mainly used locally, to authenticate a user to a device, but not for online services. In local authentication, the device can have its own database for comparing with the sample when the user want to log in. Online services would need their own databases or a common database or they have to trust the device.

The above-mentioned authentication methods are used in access control when a user wants to access a service that requires authentication. In addition to authentication, services usually restrict what the user can do in the service. For example, service administrators have more rights than common users. Authorization is often based on the authentication, namely binding the rights to an identifier such as a name. Some access control systems issue roles to users and bind the rights to the roles. Authorization can also be done without authentication by issuing authorization credentials that give rights to do something in a service.

2.3.4 Sessions in a Service

The creation of an identity is usually done once, at the beginning of the relationship between a service provider or an identity provider and the user, and the creation may occur offline. When the registration is done, the user can access the service and prove who she is using an authentica-

tion method. The service can decide what rights the user has based on the authentication. Furthermore, the service can log usage, for example, for billing or trend analysis. These tasks are often referred to as Authentication, Authorization and Accounting (AAA), and are parts of the session management in services. A session is a shared state between communicating parties, for example client and server software. Protocols define interactions that the parties exchange at the beginning of a session, during it, and for tearing down the session. Communication networks can have sessions in the transport, session and application layers of the OSI (Open Systems Interconnection) reference model, but the network or data link layer access may also require authentication.

In this work, the author concentrates on sessions in the application layer of the Internet, mainly services that are implemented on top of the world wide web (WWW) and hypertext transfer protocol (HTTP), and authentication of human users through physical devices such as mobile phones and computers. The first version of HTTP was stateless because a server just replies to a request of a client, typically a web browser [16]. HTTP works on top of the Transmission Control Protocol (TCP), using it mainly for reliable transport, not for long-lived sessions. Later, HTTP cookies were defined to enable servers to store a state for sessions [15]. When the server wants to use stateful communication, it replies to a query of the client with a message that has the Set-Cookie header field. It contains a name–value pair and associated metadata. The client sends the cookie back when the client makes a new requests to the server. As such, cookies are not secure documents, and there are many security and privacy issues associated to them, but they can be used for information storage for sessions. Moreover, for applications that require any level of security, HTTP must be run over the Transport Layer Security (TLS) [29] protocol instead of plain TCP. TLS provides integrity and data encryption for the connection, and the server is usually authenticated using X.509 certificates at the beginning of the session. TLS also supports authentication of the user with an X.509 certificate, but users typically do not have such certificates. Thus, user authentication is done with other means at the application layer, on top of a connection secured by TLS. Methods for user authentications were discussed in Section 2.3.3.

In a service that uses federated identity management for user authentication, the client side has two sessions: one with the service provider and another with an identity provider. Depending on the system, either

the service or the identity provider starts the first session. Some identity providers do not keep sessions for users, in which case the user needs to reauthenticate if she wants to start using another service. If the identity provider has its own login session, the system can provide single sign-on since the IdP already knows the user, when there is another request for her authentication. FIM and SSO systems will be discussed in detail in Section 2.4.

This thesis mainly discusses authentication methods which generate statements to the effect that a user gave valid authentication data and was present at a point in the past, at the beginning of a session. During a live session, some situations may require checking that the legitimate user is still present. For example, when a user wants to change her role in a system from a normal user to a privileged user, she may need to reauthenticate. A user may also want to change the device she is using. In the end, a device is just a tool that someone is using, and the services aim to authenticate the user, not her device. Publication II describes how an identity session can be migrated from one device to another without reauthentication. The solution is based on extracting cookies for the identity session, moving them to the other device, and inserting them into the web browser there. This allows the user to continue the service session without reauthentication.

Finally, the end of a session needs to be handled in a controlled manner. When a user does not want to use a service any more, she either logs out, closes the service, or just does not use the service for a long time. The server usually defines for how long a time the service can be left idle. Idle sessions are closed because they consume resources and may pose security threats. If the user returns to the service after the timeout has occurred, she usually has to reauthenticate. If the user logs out from the service, the server knows for sure that she is ending the session, and the session can be ended in a mutual process. However, federated identity management systems make logout more complicated. When the user logs out from one service, does it mean that she wants to end all her other service sessions in the same federation or just in that one service? Publications IV and V ponder these problems.

2.3.5 Accounting and De-provisioning

Service providers often monitor the use of identities, for example recording when someone has logged into a service and how long she has used it.

There are various reasons for this. The service may charge its users based on how many authentications they have performed in a month, as is done in Finnish mobile signatures. The service may also collect information about the user and what she is doing in the service, and use that information for showing her advertisements that should be in her interest.

At the end of a customer relationship, permissions should be revoked and information about the customer should be destroyed. For example the Finnish Personal Data Act [66] requires that personal information is stored only if there is a justified need due to the operations of the service and that they must be destroyed if they are no longer needed.

Accounting and de-provisioning are outside the scope of this work, but some of these aspects are considered in a special case: what can happen during a service session and what happens at the end of a service session, but not at the end of a customer relationship.

2.4 Single Sign-on and Federated Identity Management

This section describes the historical development of SSO and FIM systems. *Kerberos*, developed at the Massachusetts Institute of Technology (MIT) in the 1980s, is one of the oldest authentication services designed for networked services on Unix [85]. It provides centralized user management with one password, and it has later been extended to support federations. The current, fifth version is standardized by IETF [84]. Figure 2.2 depicts the Kerberos authentication protocol, which has the single sign-on property that allows a user to authenticate herself to several services with one identity verification. An authentication server grants tickets to users: one for getting tickets and others for gaining access to services. These tickets guarantee the identity of the user to a service. In addition to authentication, Kerberos provides encryption keys for sessions.

Kerberos also provides cross-organizational authentication, which is typically used between sections of the same large organization [85]. A *realm* is formed around one authentication server that shares keys with users and servers in the realm. In *cross-realm* authentication, two authentication services share a cross-realm key. The ticket granting service of the user issues a ticket-granting ticket for the other realm's server, and that ticket is used to get a service ticket for the service of that realm from its ticket granting service. In multi-hop cross-realm authentication, the au-

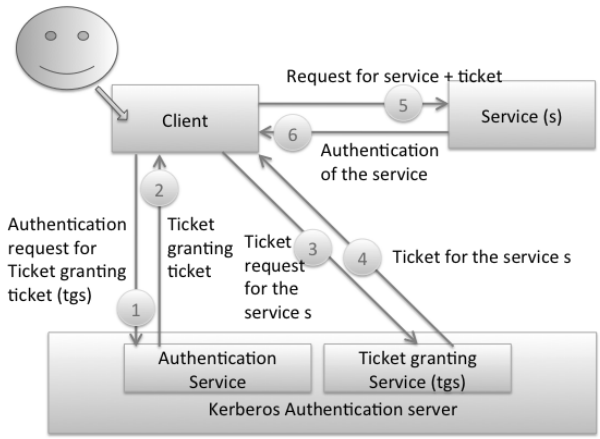

Figure 2.2. Kerberos authentication protocol [85].

thentication servers form a hierarchy and keys are shared between parent and child servers in the hierarchy.

More recently, the Security Assertion Markup Language [95] standard has provided an SSO technology for closed or federated systems. One of its implementation is Shibboleth [103], which has been deployed widely for SSO to web-based services at universities. As web services became more popular, web-based open SSO solutions were developed. Microsoft Passport was the first attempt to provide SSO for services and a wallet for online commerce [77]. The Liberty Alliance Project [104] and OpenID were competing solutions that have a somewhat similar technical structure but different trusted parties. None of these were particularly successful until Facebook introduces an SSO service based on OAuth. Subsequently, Google and Microsoft have also gained users for their SSO services, in Google's case initially based on OpenID and more recently on OpenID Connect. Recently, Open ID Connect has become a common underlying technology for real world SSO systems, notably, as mentioned above, for Google's system. Next, the above-mentioned solutions for web services are each described in more details.

Microsoft Passport (MS Passport) was a centralized SSO system in which a customer had an account witch held a range of personal information, for example the name and address, and a wallet containing a credit card number, which was supposed to enable easy payment in online shops. The

system used web cookies to store the session information. MS Passport was used, for example, in Hotmail that was a popular free email service. However, the possibility of collecting shopping habit information was seen as a threat to privacy [6].

After the failure of Passport, Microsoft released a system called *CardSpace* (InfoCard) [25, 27] which was part of the Windows system. Unlike Passport, CardSpace did not involve Microsoft providing identity services, but instead allowed any party to take that role. Any service that supports WS-* protocols would have been able to use it for user authentication. Windows CardSpace also allowed a user to manage her own identity information. When a user wanted to log in to a service, she could provide a card that fulfilled the requirements of that service. The cards were stored in encrypted form and protected by a PIN or a password. In 2011, Microsoft announced that it would not develop CardSpace further [80].

Currently, Microsoft provides an SSO system called *Microsoft account* [78] (previously known as Windows Live ID) that can be used to sign in to Microsoft's services such as outlook.com, Hotmail, Skype, and Xbox Live, but also to devices such as a Windows phone. Anyone can create a Microsoft account either with an existing email address or a new one. The user's identity is not verified but, if an existing email address is used, the user has to prove that she can read messages sent to that address. In 2008, Microsoft published a service development kit (SDK) so that other web services could use the Microsoft account for authentication [79].

The *Liberty Alliance Project*, started in 2001, was an effort to create an open standard for federated network identity for the Internet [104]. More than 150 companies and organizations participated in the development work. In Liberty, identity and service management were separated. Services providers offer web-based services for users that are identified by an identity provider [23]. They form *circles of trust* where the service providers define which identity providers they accept as provers of the users' identity. Figure 2.3 presents an example of two circles of trust. The user can choose any identity provider that a service provider trusts. Each service provider has its own identifier for the user, which can be different from the user identifier embloyed by identity provider. Even though the IdP links the identifiers, it does not track to which services the user has logged into. These two features protect the user's privacy. Some of Liberty's ideas have been adopted in the SAML and the Web Service standards [70].

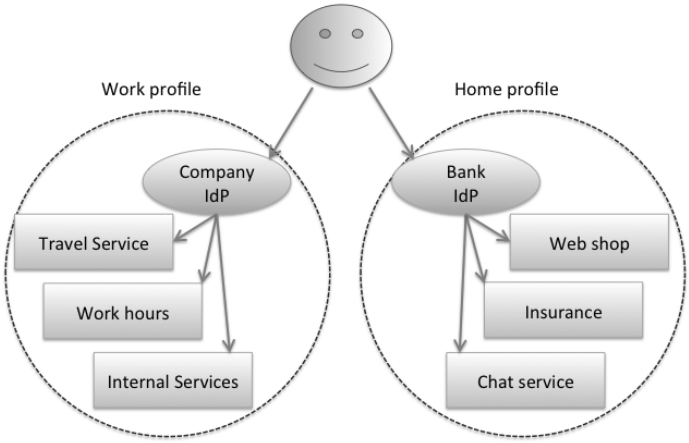

Figure 2.3. Federated network identity and circles of trust [23].

Shibboleth implements both identity provider and service provider software that can be installed into web servers in order to create a working single sign-on environment. The Shibboleth project started in 2000, and published the first implementation based on their own technology in 2003 as open-source software [103]. Shibboleth 2.0 published in 2008 is based on the SAML 2.0 standard, described later. Shibboleth was adopted by higher education organizations. For example, all universities in Finland use Shibboleth-based identity federation that has 44 registered IdP servers and 217 services [64]. In addition to SP and IdP software, Shibboleth may have an Identity Provider Discovery service that allows SPs to use multiple IdPs. Moreover, Shibboleth supports user attributes that are delivered from the IdP to the service provider together with the identity information [103]. With this, for example universities can assign roles to their users and provide different privileges for students and teachers in a service. For Finnish universities, a separate company called CSC – IT Center for Science Ltd manages the central discovery service, metadata about the services and identity providers, and a SAML profile for the user attributes [64].

The Organization for the Advancement of Structured Information Standards (OASIS) has standardized the *Security Assertion Markup Language 2.0* [95]. A previous version was adopted by Liberty Alliance and Shibboleth, and their developments and experiences have had an impact on

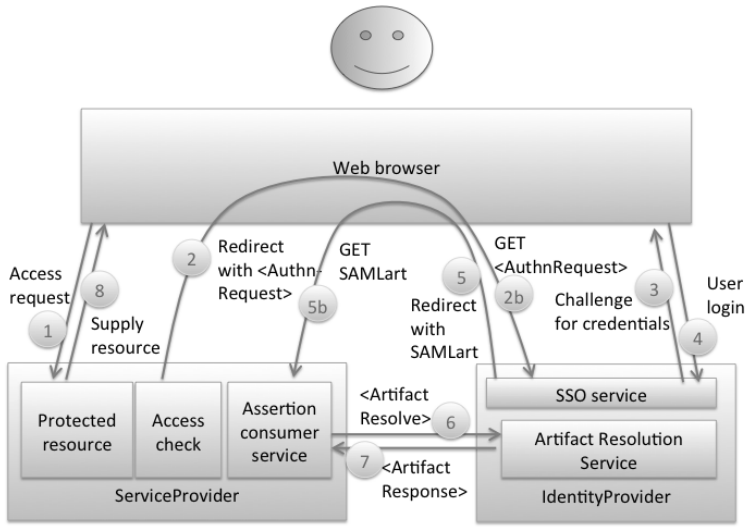

Figure 2.4. Service provider initiated communication for SSO Authentication [95].

the second version of SAML [74]. SAML is a framework that defines exchanges of security information with XML-based descriptions [95]. Its purpose is the same as in Liberty and Shibboleth: exchanging information between a service provider, called relying party in SAML, and an identity provider, called asserting party in SAML, in a way that allows multi-domain single sign-on. Identity, authentication, attribute, and authorization information is wrapped as SAML assertions that state something about a user. Messages are exchanged using the SAML protocol that works on top of the HTTP or SOAP protocols. Identifiers in SAML can be agreed between the parties dynamically. Even though one party is an identity provider, the user often has a local account with the service provider. When an identity provider is used to authenticate the user, the local account has to be associated with the federated identity in an account-linking procedure. Figure 2.4 depicts one version of message exchange between parties when a user tries to access a protected resource, but there are also other variations. Many working solutions for SSO and FIM are build on top of SAML, and for example Web Services Security (WS-Security) can use SAML assertions as security tokens in its message exchanges [95]. Since SAML offers so many variations, interoperability between different implementations is hard to achieve.

The above-mentioned systems were developed for authenticating users to a web service. Today, many web services are actually composed of ap-

plications provided by several different providers, some of which act as a proxy or aggregator for other services. Traditionally, such front-end applications all needed the same access rights to the back-end services as the resource owner, i.e. the end user. *OAuth* was developed for access-right delegation for third-party applications such as widgets that are embedded in an application [46]. OAuth separates the authentication and authorization. The whole idea is upside down compared to the traditional authentication model: a web application asks for access rights from a user who owns a resource in order to access the resource with a limited subset of the owner's rights. For example, a user owns photo files that are stored on a photo-sharing service. She has an account on the service, and her access rights are verified when she authenticates. The service can be linked to a printing service that is provided by a third party. If the user wants to print a photo, the printing service needs access rights to that photo. With OAuth, the photo-sharing service delegates some of the user's access rights, for example the right to read the photo file, to the printing service by issuing an access token. Namely, the client software (printing application) asks for authorization from the resource owner (the user) who instructs the authorization service in the resource server to issue an access token with a limited set of her rights; the client software can then use the access token to get resource from the resource server. Thus, the printing service does not get the user's full login credentials. OAuth was also used to provide user authentication for a service using third party accounts, such as Microsoft, Google, Twitter or Facebook, but that is not its primary purpose. Later, OpenID Connect was built on top of OAuth 2.0 for user authentication.

OpenID started in 2005 as a number of projects implementing identity management solutions, and in 2007, the OpenID Foundation was established to develop it. OpenID is a decentralized SSO system for web services, and it does not require pre-established trust relationships between the services, called relying parties, and the identity providers, called OpenID providers (OPs). Users can freely choose an OpenID provider. The second version of the OpenID Authentication protocol was published in 2007 [90]. OpenID uses an HTTP or HTTPS uniform resource identifier (URI) or an extensible resource identifier (XRI) for the users, and handles them differently to other FIM systems. The identifier is a resource that the user controls, for example a URL for a blog of the user. When the user logs into a service offered by a relying party, the RP has to discover

the OpenID provider for the identifier that the user has typed in. URL identifiers have the advantage that the URL itself can lead to the OP. The problem with URL identifiers is that they may not be persistent. On the other hand, XRI identifiers have two parts, *i-name* and *i-number*, where the first can be reassigned but the latter is persistent, and this makes the discovery of the correct identity easier [98].

The OpenID authentication protocol [90] is depicted in Figure 2.5. As a protocol, the message exchange looks quite similar to that of SAML or Liberty. However, the identifiers and their handling are different. The OpenID provider does not need to keep a state for the identity. Thus, OpenID does not require the use of cookies but only HTTP redirection. If the user wants to log in to another RP, the OpenID provider authenticates her again. When used in this way, OpenID 2.0 is not a pure single sign-on system, but it reduces the number of required identifiers. The user can choose which OpenID provider she uses. The OpenID provider can decide which authentication method it uses to verify the identity of the user. However, a separate policy extension defines mechanisms for a RP to request a certain authentication method or an OpenID provider to inform the RP about the authentication policies [97]. When the RP requests the OP to authenticate the user, it can add descriptions of its preferences for the authentication policy. The OP can also add information about the policy even if the RP did not request it. The supported policies are phishing-resistant, multi-factor, and physical multi-factor authentication.

Companies, among others PayPal, Lenovo, and Google, have noticed that mobile phones can provide strong user authentication for services. They established the *FIDO Alliance* [36] that has defined industry standards for authentication to complement OpenID and SAML specifications which do not specify how an IdP should authenticate its users. In FIDO, a user first registers her mobile device to a FIDO server and gets a unique key pair for the device, online service and her user account. The Universal Authentication Framework (UAF) [73] specifies an authentication procedure in which user's biometric information or a PIN code is verified locally in her mobile phone. Another possibility is to use FIDO's Universal 2nd Factor (U2F) protocol [105] that adds a physical token, e.g. a USB device, to normal password-based authentication.

OpenID Connect authentication, published in 2014 [101], is built on top of the OAuth 2.0 authorization protocol described above. It supports native and mobile client applications in addition to web applications. The

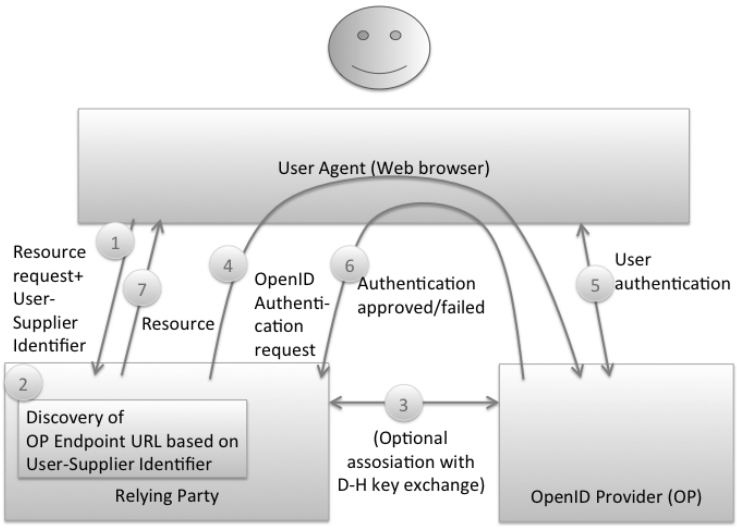

Figure 2.5. OpenID protocol overview [90].

OpenID Connect authentication has a REST architecture and it uses JavaScript Object Notation (JSON) [20] which is, despite the name, a language-independent data format. In the process, an identity provider returns an ID token to a relying party. The ID token follows the standard format of a JSON Web Token (JWT) [57] and contains an issuer URL, a unique subject identifier, an identifier of the relying party for whom the ID token is intended, and the expiration time [101]. The ID token is at least signed using a JSON web signature [56] and it may be also encrypted with JSON web encryption [58]. For example, the current version of Google+ Sign-In uses OpenID Connect, and Microsoft, Ping Identity, and Yahoo! also provide OpenID Connect authentication for their users. Unlike in the orginal OpenID, the identity provider is bound to certain relying parties and users cannot choose freely which identity provider they want to use for a service.

This Chapter described authentication technologies and their history. Some of them are available as open source, and we have used their available open source versions as building blocks in our solutions presented in the articles. Moreover, we surveyed single sign-on solutions available for online services. Our solutions are based on Shibboleth since it is widely deployed in the Finnish higher education institutes. It is also available as

open source, and we were able to use the identity provider of our university for the experiments.

3. Improvements to User Authentication and Single Sign-on

This chapter presents the contributions of this thesis. We will also describe other other similar solutions that have been proposed since our articles have been published.

3.1 Establishing Online Identity

Online communication and commerce work on a global scale, and crossing the borders of counties can form obstacles for identification. Service providers follow the national-level legislation that applies where they are operating, but their clients are often in other continents. The Parliament of the European Union adopted a regulation [109] that is intended to to ease electronic commerce in the internal market by mutually recognizing electronic identities issued by other European countries but it does not say anything about the technical solutions. For example, Sánchez García et al. [40] present several technical interoperability solutions, such as a network of proxies that allows services within one country to use an identity provider of another country in Europe. However, real world implementations do not yet exist.

Publication VI surveys the electronic citizen identities and deployed strong authentication systems in different countries and investigates how the countries issue digital identifiers for their citizens. Our initial goal was to understand the technical solutions and open problems, but one conclusion of the survey was that the deployment and interoperability issues arise mainly from non-technical causes.

Technical innovations have improved identity verification in the real world by adding biometric information such as a facial image and fingerprints to a micro-chip in passports, also making them harder to forge.

The machine-readable chips in principle could provide a means of authenticating citizens to online services, but reading the passport chip requires special secure terminal equipment and, in practice, they cannot be used online. Many countries provide solutions of their own for official online identity verification, e.g. using an identity card, or some other physical token such as a USB stick, or a password. In the OECD countries, every second citizen has used governmental online services and the usage has been highest in the European countries [87]. Another source of identity is the social and business relationships that a person forms with other people or organizations without the help of authorities. The relationship might start from, for example, a shared friend or initial contact a person via a phone number or home address. In the digital world, the most widely used source of identity is an email address via which the person can receive messages. Based on such an address, she can create an account in, for example, social media services, which may then act as trusted third parties for other services that require authentication. Stronger identity can then be established gradually, accumulating information and reputation with direct contact and via various social media services such as photo feeds, blogs, etc.

Local history and traditions of governance seem to strongly affect the kind of solution of strong authentication that are successful in each country. Many countries provide electronic identity cards but they are seldom used in an online context. The Nordic countries have been relatively successful in the deployment of online verification because 70% of Nordic citizens have used the Internet to interact with public authorities [87]. For example in Estonia, the national electronic identity card is used in a number of services from bus tickets to registering a new company. In Finland, there are several possibilities for strong citizen authentication, and instead of electronic identification cards, online bank credentials are more commonly used in authentication. In spite of the attempts of the European Union to create working online authentication in all its member countries, some countries have failed to develop national online authentication. For example, France has postponed publishing their electronic identification card, and the United Kingdom even cancelled their part-deployed electronic identity card system. The main concerns have been the security of the database in which all information is collected for issuing the cards, and that the identity provider may track all the services that the person is using based on the authentication requests.

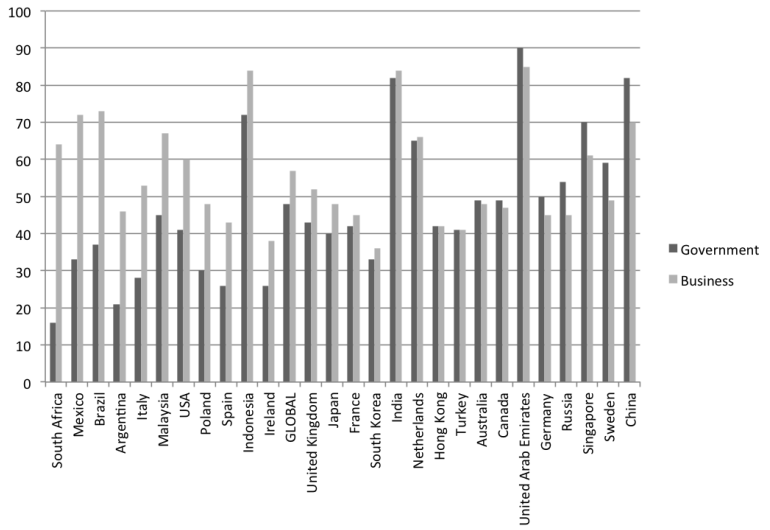

Figure 3.1. Trust in Government and Business in 27 countries [32].

Another approach to citizen authentication is to outsource it to commercial service providers, which can then be used for both governmental services and private online services. In many countries, banks, the postal service or mobile phone operators provide this kind of authentication. The reasons for this may be historical. For example in Finland, the Merita bank (currently the Nordea bank) decided to transfer their online banking service to the Internet in 1995, and in 1997 they were amongst the first in the world to launch an online bank [4]. The online banking scheme required reliable authentication of the clients, and the bank had to develop their own solution for that. Their solution was available before the corresponding governmental service, which only started to provide electronic identity cards in 1999 [99]. Another benefit was that authentication was based on one-time-passwords delivered on printed paper, and did not require any hardware device such as a smart card reader for the ID card. Later, the Federation of Finnish Financial Services specified the TUPAS Identification Service [35], a standardized version of online authentication for banks and also for other service providers.

Another reason for outsourcing authentication to the private sector may have its origin in the fact that citizens in many countries have more trust in companies than in governmental bodies. In 2015, the research organization Edelman interviewed 33000 people in 27 countries about their trust in the government and in media and companies in general [32]. According to the study, only in eight countries out of 27 did more than 50%

trust their government, and in six countries less than one third of the people trusted the government. For example, only 16% of South Africans trusted their government. In general, people had more trust in private businesses, in which the trust level was the lowest among South Koreans (36%). These results are depicted in Figure 3.1. In the left part of the diagram, the difference between trust in government and businesses is the largest in favour of businesses. These countries include, for example, South Africa, Brazil, and USA. In the right part of the diagram, people have more trust in government than in businesses, for example in China and Sweden. If we compare these countries to the G20 countries studied in Publication VI, it seems that trust in government must be strong in order for electronic authentication based on government solutions to succeed. Countries that have tried but failed to develop such solutions, notably the United Kingdom and France, seem to lack trust in the government. In countries where people trust businesses more, a solution where the government outsources authentication to companies, as is done in the USA, may work better. However, the roots of trust are complex and, for example, economic problems in European countries may have affected trust in governments during the study period. Further analysis concerning reasons why governments are trusted (e.g. in Sweden and in China) is outside the scope of this thesis.

3.2 Strong Authentication

As mentioned at the beginning of Section 3.1, one source of identity is relying on common friends who can, at a personal level, introduce people to each other. Single sign-on systems essentially follow the same pattern, except that the identity provider is the common “friend” of a users and a service providers. The identity provider takes care of the establishment of the digital identity and provides authentication of the users when they want to access the services. In the early days of SSO, identity providers mainly used password authentication. Often SSO protocols themselves do not specify the authentication method, allowing identity providers to innovate.

In **Publication III**, we have developed a strong authentication method that uses a mobile phone as the secure token without the involvement of mobile phone operators. We use the phone as the second authentication

method. Such solutions were not widely used at the time of the research, and our solution differs from the currently deployed ones in that the second channel is initiated from the mobile phone.

Our design for strong authentication in SSO is modular, allowing the use of any SSO protocol and any tamper-resistant security module available on a mobile phone. In our prototype implementation, we used the Shibboleth SSO system and a Nokia N900 phone with the On-board Credentials (ObC) trusted hardware emulator. Details of the system are presented in Publication III, and Andrade [7] gives implementation details. All of the components of our design are open and free to use. The main difference between our system and other two-factor authentication methods that rely on two different communication paths is that the user starts both the browser session on her computer and the authentication client on her mobile phone. These two devices do not communicate directly with each other, but the user acts as a communication link by checking that both the service session and the authentication session belong together. This means that any mobile phone that has a tamper-resistant module may be used as a token, even if the phone is not capable of multitasking or has no event-based notification system. The user does not need to set up a communication link between the devices, a task that may be cumbersome. The user does not need to register her phone number, and the system also works with prepaid SIM cards and with foreign SIM cards since it is independent of mobile phone operators. However, the user has to register her public key when enrolling with an identity provider. This can be done as part of the process in which her identity is verified and online identity is established. The system can be deployed incrementally becausemodifications are only needed at the IdP and because service providers can independently decide when to start requesting strong authentication of users.

Other researchers have also noted that SSO systems need stronger authentication methods and that mobile devices can help provide them. Recent solutions assume more from the mobile device, for example a camera for scanning QR codes, a Trusted Platform Module (TPM), or support for mobile signatures in the SIM card. These differences are briefly summarised next.

Mobile phones are at present used as secure tokens that provide a second communication channel for users. One solution for checking that a

user of a web service has a certain mobile phone is to show a QR-code on the login page of the service, which the user scans and signs digitally. The signing can be implemented with a software application, a trusted execution environment, or a SIM card. Such solutions require modifications to user devices and identity providers but not in the services themselves. For example, Binu et al. [17] have developed a mobile-phone-based two-factor authentication for SAML-based SSO. Their solution is similar to ours since it requires the mobile phone to initiate the authentication and does not require the IdP or service provider to store the mobile phone number, meaning that the mobile network operator is not involved as a trusted party. However, their QR-code based solution uses software functions to store the mobile token securely, protecting it only with a password, whereas our system uses a tamperproof module available on the mobile device. Another similar example of the use of QR-codes is described in Dodson et al. [30], but they do not describe how they protect the shared keys delivered in the QR-code messages. QR-code based challenges can also be used in other ways. For example, Carullo et al. [24] suggest that a QR-code is sent to the mobile phone of the user, whose contact phone number is stored within the identity provider, and the QR-code is shown to a web camera on the computer.

The SIM card can also be employed as a tamperproof token. The SIM card is used to identify the mobile subscriber, and it stores secret keys for encrypting the air-interface traffic between the mobile phone and the base station as well as for authentication. For application-layer services, the SIM card can be used with the Extensible Authentication Protocol (EAP) that was originally designed for authenticating link level access [10]. The EAP protocol has extensions for using both GSM SIM cards [49] and 3G USIM cards [9] to provide authentication for applications. Moreover, the General Authentication Architecture (GAA) [2] is an architecture for peer authentication that can use either the SIM card or a public key infrastructure. Furthermore, mobile phone operators can also offer strong authentication with mobile signature, which are created on the SIM card [88]. For example in Finland, this is one of the strong authentication methods accepted by government online services and other web services. The service providers need an agreement with only one Finnish mobile operator to authenticate all users since the system is federated [60].

Another way to use mobile phones as a secure token takes advantage of their secure hardware environment. This environment was originally

intended for checking intellectual property rights and provides a secure storage and execution environment for security-critical functions. We have described a way of using it for storing credentials for authentication and calculating responses for authentication challenges. Other authors, for example, Leicher et al. [68] have developed a local OpenID provider that is based on the Trusted Platform Module. When a service requires authentication, the connection is redirected by a local DNS lookup or a browser plugin to the local identity provider that authenticates the user with a two-factor authentication scheme. They described also another scheme that uses the SIM card of the user's mobile device for storing credentials and creating signatures [67].

3.3 Heterogeneous Environment and Ad-hoc Networks

At the turn of the millennium, mobile devices were less capable and had smaller screens than those available today, but the Internet was nevertheless available using mobile phones. These and other mobile devices could also form wireless connections either to the Internet through an access point or with each others without connection to the Internet. The latter mode is called a wireless ad-hoc network or mobile ad-hoc network. Many aspects of ad-hoc networks, such as routing, were a hot topic in research at that time. The initial main application area was military networks, where fast setup and takedown were needed. For example, Tang and Chang [107] reviewed strong authentication mechanisms for tactical mobile and ad-hoc networks.

At Helsinki University of Technology, we engaged in a joint project on this topic together with University of Helsinki and Tampere University of Technology. The objective was to investigate seamless service interworking in heterogeneous mobile and ad-hoc networks. Our goal was to create means for users in an ad-hoc network to find services, such as another device that could offer Internet connectivity, and create sessions with these services. We noticed that one peculiar characteristic distinguishes access control in ad-hoc networks from other networks: someone could want to limit which service providers are allowed offer services to their devices. The services are usualy authenticated with X.509 certificates but there is no separate access control defining which services a device can contact in the first place. Moreover, X.509 certificates normally require trusted third parties. In our system, we implemented a kind of secure wallet

where credentials and certificates could be stored and exchanged between devices [62, 72, 113].

Publication I describes the architecture for finding and using services in ad-hoc networks, and we at Helsinki University of Technology were especially responsible for the security of the design. Our main research contribution was two-directional authorization between the user device and the local and online services. This publication is significantly earlier than the other publications in this thesis, and it motivated our later work on identity management with ubiquitous Internet connectivity.

Ad-hoc networks are no longer so extensively studied, expect in one or two areas. Kärkkäinen et al. [63] list practical and principled reasons why ad-hoc network technology is not really deployed: for example, mobile device vendors do not seem wish to support it, and altruistic co-operation between users lacks incentives. Also, during the last 10 years, the network environment has changed significantly. Mobile network access is available almost everywhere either through WiFi hotspots in cities or via the mobile phone networks. On the service side, cloud computing has changed a great deal, offering a scalable server and service environment for service providers. At present, investigation of ad-hoc network technologies has focused on vehicular networks and and the Internet of Things (IoT). Next, we will briefly overview the problems identified in other research litterature for authentication and identity management in ad hoc networks.

A number of car manufacturers are developing self-driving cars. Vehicles close to each other can form Vehicular Ad-hoc Networks (VANETs), warn one another about the danger of collision and communicate with road infrastructure devices about road conditions [48]. The same technology can be used, for example, to collect road taxes and to monitor traffic, something that troubles those who care about their privacy. Already, vehicular communication has its own dedicated frequency, 5.9 GHZ, and IEEE has standardized a link layer protocol called Wireless Access in Vehicular Environments (WAVE) and considered the associated security issues [51]. Authentication of vehicles is based on certificates that can be changed from time to time to protect the privacy of the vehicle driver or owner. However, Förster et al. [39] claim that changing of certificates is not defined clearly in the standards. They have investigated how it can be done in such a way that the linking of pseudonyms is not possible for unauthorized parties. Horng and Tzeng [50] have developed a secure and

privacy-preserving value-added service scheme for VANETs. Using blind signatures, vehicles could request services without revealing their real identities and the services could authorize the vehicles.

Technologies such as radio-frequency identification (RFID), ad-hoc networks, near field communication (NFC) and Internet Protocol version 6 (IPv6) all help to realise the network for Internet of Things. The application areas for IoT are wide, for example covering healthcare and building maintenance. Security and privacy are key issues, because these networks can contain a great deal of sensitive information. For example, unauthorized access to a pacemaker or other implantable medical devices (IMDs) may be life-threatening. Halperin et al. [45] have suggested criteria for the security and privacy of IMDs. For example, there may exist different access levels: the patient and her primary care physician might have access based on their identities, and emergency personnel might get access via role-based authorization. Furthermore, outsiders should not even know that a patient has an IMD. One challenge of embedded devices is that they often have low computing and battery power, which makes it difficult to use public-key cryptography. For example, Li et al. [69] consider energy efficiency from a computation and communication points of view for user-aided group device pairing for the body area network (BAN). Yang et al. [114] have proposed a RFID-based solution for authenticating devices with the help of a centralized database.

When the Internet of Things and Cloud computing are combined as the IoT Cloud or as IoT as a Service, new security issues arise. For example, Barreto et al. [14] have presented an authentication system for IoT Clouds based on a Trusted Platform Module. Bamasag and Youcef-Toumi [12] have developed a protocol that provides mutual and continuous authentication for IoT devices but they have not yet described an implementation. Markmann et al. [75] have developed identity-based cryptography (IBC) based end-to-end authentication, where the public key of a device is an arbitrary bit string and a gateway acts as a trusted authority. The gateway links the public key to the IPv6 address of the device locally in its subnet, and the gateways form a federation where the authentication of end nodes is provided by their own gateways. Sciancalepore et al. [102] have proposed a solution based on elliptic curve cryptography (ECC) for key management in IoT systems. ECC is less computationally intensive than public-key cryptosystems based on integer factorization or discrete

logarithms over integer rings, and thus appears better suited for IoT networks.

3.4 Session Migration between Devices

Today, users can install software on their mobile phones, have portable tablet computers connected to Internet, and use cloud services almost anywhere since wireless networks are widespread. Today's portable devices have the capability to run almost all the same software as computers, and touch screens have changed the user experience. Even though people may find their mobile phone more personal than their computer, users still have to be authenticated to the services because the devices may easily end up in the wrong hands. Moreover, many tasks still require a reasonable-sized display, and physical keyboards and other input devices are more ergonomic to use for long periods. This means that a mobile device often remains a secondary way to connect to services and is only used when mobility is necessary. For example, when leaving the breakfast table, a user could move her sessions from a tablet computer to a mobile phone for the commute to work, and later again migrate them to a desktop computer in the office. Although nowadays whole services are implemented in the cloud environment, user authentication often requires a part of the session to exist in the user device, and changing the device would require the user to authenticate again. Services often seem to consider authentication only a minor task for the user, while in fact it is an unwanted hurdle for the user who only wants to use the service. There have been only a few research papers on session migration without reauthentication, but session migration in general and moving services between services in the cloud environment have attracted the interest of a number of researchers. Much of the published research concerns network layer sessions, but we are interested in application layer sessions.

Publication II describes a mechanism for moving the authenticated user session from one device or web browser to another without reauthentication. In stateless web applications, it is often sufficient to migrate the session cookies. We implemented the session migration on a button click directly between two user devices that have been paired earlier. While modern browsers synchronize various settings between devices, they do it

through a cloud service and, so far, we have not seen any of them migrating authentication sessions.

Basically, there are three ways to migrate session information between devices: directly between clients, using a proxy, or storing information on the server [22]. The benefits of client-based systems include access to all the relevant information on the client, but the clients can be heterogeneous and require different ways accessing the information. Our solution moves authentication sessions directly between client devices when a user initiates the migration, but we did not consider where the other session-related information is stored. In order for a session to continue seamlessly, this information must be held by the server. When implementing the solution, we noticed that different web browsers handle cookies in different ways, which means that every browser would require its own implementation. A few others have also implemented solutions for client-side session migration without reauthentication. For example, Zhang et al. [117] suggest a system where an application consisting of web apps can be migrated between the device and the cloud by moving its saved state and relaunching it. The device has a manager that takes care of the coordination of web app components, and the cloud has another manager that is responsible for the cloud resources. Authentication is based either on a pair of application session keys or the system can use OAuth-like authentication, but the details of the system are not described. On the other hand, Pippal et al. [92] propose smart-card based authentication for session migration between user's registered devices and give only cryptographic details of how devices delegate a user's authentication when the session is moved.

Another way of migrating a session is to use a proxy that stores all the session information for the client and server. The benefit of such an approach is that it requires little modification to clients or servers [22]. If the communication between the client and the server is protected, this approach does not work.

The third solution is to store session information at the server [22]. This corresponds to the typical current situation where client-side programs are often so-called thin clients, all the service logic executes in the cloud and information is also stored there. If there are only a single client and a single server, this should be easy to admister, but if the session is actually composed of several components running on different servers, session migration may be difficult. Although Publication II did not directly con-

sider cloud computing, the cloud has made migration more easy to achieve since only the authentication session would exist on the client device and moving this would be enough. However, even this migration depends on how the single sign-on mechanism stores its credentials, the specific web browser the client is using, and how the device is used in two-factor authentication.

Moreover, some mobile devices nowadays have docking stations that enable the device to provide all the normal desktop PC functionality when connecting to a keyboard and full-sized screen, thus offering a simple alternative to session migration.

3.5 Logout

When a user is logging out from a service, the service can release resources that were reserved and close the network connections. This requires that the service session to be ended in a controlled manner. If the user just closes the web browser window, the server does not know that the session has be closed. The situation appears similar to when a temporary network failure prevents connections from the client. A single sign-on environment makes this even harder, since the user can have active sessions with several services and identity providers. It is often assumed that, if a user presses the logout button in a service that uses SSO, she would like to log out from all the services under the same identity provider. This assumption is consistent with the findings of a usability study by Linden and Vilpola in 2005 [71]. Kormann and Rubin [61] investigated Hotmail when it was using MS Passport for logging in. They noticed that it offered signout for Passport and logout from Hotmail, and they feared that this may confuse users. Moreover, they noted that the logout did not really work with the Netscape web browser. Nowadays, a user may be surprised when she gets into her Gmail without entering credentials after using a third-party service with her Google account, even if she has later logged out from the former service [96]. Moreover she may be equally suprised when a service has logged her out from the Google account.

Publication IV and **Publication V** investigate logout in SSO systems. The former describes different types of logout that can occur in SSO systems, and how sessions are handled when terminating the service. We

point out various problems in the current implementations of session termination. These issues still remain in typical Shibboleth integrations. The latter publication provides a solution wherein the user can choose between logout from a single service or from all services that use the same identity provider. The solution was implemented for Shibboleth 2 by polling the identity provider from the services.

The solution was tested with 18 users who performed tasks in a usability test followed by a structured interview. All the participants had experience of using SSO systems and all of them worked in either research or support services at the university. The results of the test regarding understandability of the meaning of single logout and local logout could be different if the test participants had no previous experience of SSO systems. Finding out the general level of acceptance of a single logout solution would have required a wider survey. However, from our tests, we found that people understand the concepts of logout in an SSO system differently and that they need more support from the system in order to act securely. The test participants also liked the possibility of choosing where to log out, since they could then continue using other services without reauthentication.

Persistent authentication, in which the user is often authenticated based on her proximity to a user workstation, has recently brought logout into the focus of research. This type of authentication is well-suited to situations in which users move and handle sensitive information and where authentication has to be completed quickly, for example access to patient records at a hospital emergency room. For example, Premarathne et al. [93] discussed global logout management and persistent authentication in SSO systems. Their solution forms groups from the authentication sessions in which is the user is engaged during period of time. If the user logs out from one of the services, the system also ends other service sessions where the same identity was used. Dodson et al. [30] proposed briefly that a mobile phone can be used as a proximity sensor: the service can ask for reauthentication if the mobile phone is moved too far away from the place where it was when the initial authentication occurred. In their solution, the mobile phone is used as an authentication token, and the user can also close all open sessions with the mobile phone. However, they do not give any further details.

4. Discussion

In this chapter we return to the research questions defined in the Introdution, and assess how well they have been answered in this thesis. We also describe possible future work.

4.1 Contributions

Research Question 1: How can a real world identity be linked to online world identity in a distributed and even international environment in a strong way?

As discussed in Section 2.3.1, sources for digital identity can be a state, private organizations, or even one's friends, depending on the context where the identity is used. For strong verification of identity, two-factor authentication is required, which means using at least two authentication methods. A real world identity often works as a basis for a digital identity. Even though passports often include a smart chip that contains a picture of the passport holder, they cannot easily be used in online services since they require trusted readers. Publication VI presents a survey of over 20 countries that offer electronic identification for their citizens. These electronic identification systems can be used at least for government online services, but many countries also provide authentication for third party online services. Moreover, a few countries have outsourced citizen authentication to trustworthy parties such as banks, mobile phone operators and post offices. However, these solutions usually only work at the scale of a country, and not internationally.

There are two ways to use real world identity as a basis for an international digital identity: either national systems enroll non-citizens into the system, or the national identity verification services are federated so that services in other countries can ask for user authentication. Currently,

there are no available federated solutions for citizen identities but the eIDAS regulation [109] of the European Union requires that EU countries will in the future recognize electronic identities and signatures of other member states. Some countries provide identity cards to non-citizens that have a permanent residential address in that country. Only Estonia provides electronic identification cards for non-resident foreigners, called e-Residency [31]. This smart card is similar to the electronic identity card of Estonian citizens. It can be used to digitally sign documents and contracts, for example to establish a company in Estonia, even without a physical office in Estonia. In order to get the card, an application is filled online, and the card can be collected from Estonian consulates or Estonian Police service points where the applicant's identity is verified using identity documents such as a passport. Physically verifying the client's identity from an official identity documentation at a service point by someone who then activates an online account for the client is still the most widely used way to link a real world identity to an online identity.

We did not investigate bootstrapping of identities based on private arrangements, on introductions by friends or on building reputation-based digital identities in online services. Publication I touched on the subject because ad-hoc networks may not have connections to identity providers or trusted third parties that issue credentials. In such environments, friends may offer services to each other, and it is natural that an identifier is linked to a digital identity based on direct contact between the users, or by relying on a common friend to verify it. We will return to ad-hoc networks below under the next question.

However, even if citizens have electronic identity cards, they seldom use them in online services. The problem seems not to be technical but rather a result of the fear of losing privacy as well as attitudes towards the identity provider. In the end, it seems that many services do not actually need the link between online identity and real world identity. The services can, for example, outsource their billing to other services such as PayPal or credit card companies that either have implemented strong authentication methods that link the customer identity to her real world identity or base their trust on gradually established reputation and financial risk management.

Research Question 2: Mobile devices provide a handy way to access online services, but what new requirements and opportunities do the mobile devices bring to digital identity management?

The new requirements arise from the mobility of the devices and the possibility to offer services to other devices. Use of mobile devices is pervasive today. Almost everything that could be done with computers a few years ago can now be done with mobile devices, and Internet connectivity with WiFi or mobile phone networks is available everywhere. The mobile devices can also form networks with other devices in close proximity, without a connection to the Internet, and they could offer services to each other in an ad-hoc manner. Mobility as such is not the focus of this thesis, but opportunities that the mobile devices bring to authentication are taken into account. For example, many mobile devices now have a trusted execution environment that can be used for secure credential storage and also for performing cryptographic algorithms. Furthermore, a user can move with her mobile device, but since it has a smaller display and cumbersome input methods such as a touch screen, she may want to change devices when a better user interface is available. This possibility is considered under Research Question 3.

As mentioned above ad-hoc networks have particular properties since they are formed of devices that happen to be in the same location. In multihop ad-hoc networks, devices are assumed to be altruistic, meaning that they deliver packets to devices that they themselves do not have anything to transmit to. Packet delivery can be seen as one service in the ad-hoc network, and a device can even offer to be a gateway to the Internet for other devices. In such an environment, it is not sufficient to just define who can use a service but also a policy for who can offer services to whom. Nowadays, the only way for a user to influence this is to decide whether or not to use a service. Publication I describes a two-way access control list in which such policy definitions can be defined. Our system supports all kinds of credentials: a trusted third party can issue certificates, or they can be self-signed. The credentials are linked together through a so-called base certificate that represents the digital identity of the device holder. Other credentials describe the two kind of access rights: for services that the user has the right to access, and rights of her device to offer services to other users. The task of the user is to define which other users are permitted to offer services, such as providing connection to Internet, but this may be hard for most users. Even though ad-hoc networks have not become as popular as expected at the time this research was carried out, the same kind of issues have arisen, for example, in vehicular networks as described in Section 3.3.

Many SSO systems still use password-based authentication. The easiest way to increase the security of password authentication is to add a physical token that only an authorized user has access to. Mobile phones are considered to be quite personal, and physical access to their data can be protected by a PIN code. Thus, they can act as hardware tokens that provide two-factor authentication. Publication III provides strong authentication for single sign-on systems without linking to a real world identity, but such a link could be created by verifying the user identities before issuing the credentials. In our prototype implementation, the identity service credentials are stored securely using the TEE of the mobile device, without requiring the involvement of the mobile phone operator or use of SIM cards. When a user connects to a web service with her computer, the redirected connection to the identity provider stops and waits for an authentication message from her mobile device. Our system does not require much technical knowledge from the user since she acts as a link between the authentication session on the phone and the service session on the computer. The phone and computer do not communicate directly. A user can access a service either with a separate computer or using the same phone. Similar systems are now under development for national use, but at the time of the publication our system was state of the art.

Research Question 3: Existing SSO solutions are focused on the initial authentication at the beginning of a identity and service sessions, but what security issues arise later in the session lifetime?

Compared to the real world where people recognize familiar faces automatically, authentication in the digital world requires a separate process. Most of the effort in developing digital identity management has been devoted to the beginning of the relationship, either in verification of an identity before issuing credentials for the digital identity, or authenticating the identity at the beginning of a session. This thesis also addresses security issues later in the session lifetime, such as whether the user is still the same as at the beginning of the session when she tries to initiate some critical action, whether she can log out from services, and what logout actually means in the single sign-on environment.

Nowadays, cloud computing offers the possibility of implementing services in such a way that only the authentication session has to be stored on the client device and the applications run statelessly in the web browser. Thanks to mobile devices and ubiguitous network connectivity, the user can be independent of any physical location while using an online ser-

vice. However, mobile device screens are small and their keyboards are not very ergonomic, and people may still want to use a tablet, laptop or desktop computer when one is available. Publication II shows how an authentication session of an SSO service can be migrated from one device to another simply by moving its HTTP cookies. Our system does not require reauthentication when the user switches devices – the digital identity belongs to a person, not to the device she is using.

After our publication, the need for session migration has been partly reduced by the dominance of the big application providers, such as Google and Facebook, and the fact that users remain always logged in to them on all their devices. User expectations may also be moving to this direction. Some users in our study preferred to stay continuously logged in to all services on several devices and, in the future, users may not perceive the need for session migration.

In addition to session migration, logout is another critical point in the session lifetime, especially when using shared computers or ubiquitous devices that are not personal. In order to prevent misuse of open sessions in services, the sessions should be closed in a controlled way so that both parties agree that the session is closed. This issue, however, is often neglected in SSO systems. Logout procedures are often defined only vaguely in standards, since the goals of logout are not well defined, and the order in which sessions are terminated can affect the end result. Actually there may be several active sessions in an SSO system: the user may have a session with the identity provider that authenticated her at the beginning of a service session, and she may have used this authentication to create sessions with other services. When the user wants to log out, what sessions does she actually want to terminate?

Publication IV describes the problem of logout in SSO systems, and Publication V provides a solution in which a user can choose between local logout from a single service or global logout from all services that use the same identity provider. Even though the identity provider does not keep track of which services it has authenticated the user to, the services can poll the identity provider to learn if it still has an active session for the user. In this way, the other services can end their sessions after a short while if the user has requested global logout that also terminates the session with the identity provider. Our usability study in Publication V shows that users can understand the differences between these two concepts even though they did not understand the words we used for

them. Moreover, the study confirmed our hypothesis that users often close a browser tab without logging out, but that they do not want to close the whole browser at the end of using a service, which is the solution recommended by many web sites. The service session should be ended even in these cases. Furthermore, the beginning and the end of service sessions in a federated single sign-on system should look the same, in order to be understandable and trust-promoting for common users. Implementations of federation should incorporate carefully designed processes to test services so that they implement logout in a correct way.

4.2 Possible Future Work

Much work remains in putting the research results into practice. Even though we have worked with the university IT services to bring clarity to the logout processes, the implementation of logout varies from service to service. Moreover, the HAKA SSO federation of Finnish higher education institutes has not yet revised its guidelines. It seems that some service providers have just given up and do not implement any way to logout except by closing the web browser.

In addition to session migration and termination, some actions during the SSO service session may require extra assurance. For example in universities, paper applications and their handling processes are changing to online services. An existing SSO session may not be sufficient to guarantee that a user has not changed between the login and an action that requires user approval. Single sign-on is not equivalent to digital signatures. It requires further study to decide whether reauthentication of the user could replace digital signatures in such situations.

Although lawmakers of European Union have defined that national electronic identification should be accepted in other member states in the eIDAS regulation [109], the technical implementation and deployment of federated single sign-on systems in the international environment requires further study. For example, Sánchez García et al. [40] described criteria for a Pan-European identity management system and pointed out challenges such as how can service providers trust identity providers in other countries. They stated that national IdPs should have one reliable source for information and that there should be multiple levels of security, etc. However, many European countries have adopted an approach where companies act as identity providers, which is not compatible with

the first requirement. Furthermore, based on the survey in Publication VI, only a few countries provide multiple levels security using different authentication methods, even though, for example, the eIDAS regulation defines three security levels (namely low, substantial and high). Moreover, further study of the attitudes towards citizen authentication is required since citizen authentication is quite rarely used even in most countries where a technical solution is available.

Even though higher education organizations have managed to agree on federated identity management for secure network access in the Eduroam wireless access service [33], private companies seldom trust someone else's identity providers. In order to find out why federated identity management is not used in private sector companies, Jensen and Jaatun [55] studied a competitive international industry in which subcontractors provide many services and need access to services for others. They envisage one solution being trusted third parties whose primary business is to provide identity verification and keep user information up to date. However, further study on the requirements of private sector actors for federated identity management is needed.

Transparent or persistent authentication is an interesting area that is the focus of current research. Any successful solution of this type must address both migrating sessions between devices that are in close proximity to a user and logging her out when she leaves. Hopefully, the latter research will also address services that use single sign-on.

5. Conclusion

In this thesis, we have examined many aspects of single sign-on systems, which aim to simplify user authentication for online services. We looked both at national and organizational SSO solutions and found that, while SSO systems meet their main goal of reducing the number of passwords that a user needs to memorize, many other aspects can still be improved. Our main research questions have been: (1) how digital user identities are linked to real world identities, (2) what opportunities and challenges mobile devices bring to the SSO systems, and (3) how SSO sessions are managed after the initial authentication.

We surveyed citizen authentication around the world, including methods based on smart cards and other credentials. Most of these offer strong two-factor authentication and APIs for integration to private and commercial systems. However, organizations may want to implement strong authentication by themselves without relying on specific national identity systems. We designed and implemented a system that provides two-factor user authentication using a mobile phone as a secure store for service-issued credentials and which could optionally be linked to the real-world identity of the user.

The use of mobile devices gives rise to questions about session mobility. In modern web applications that are distributed between the browser and the cloud, the login session is often implemented with cookies in the client device. We designed a session migration process that allows the SSO session to be moved from one device to another. This enabled users to switch between devices, for example, from a desktop computer to a mobile device and back, and still continue working without reauthentication. Session migration seems like a viable alternative to staying always logged in to all devices, especially for shared computing appliances. We also considered credential storage and server authorization for ad-hoc computing

environments where mobile devices have no connection to trusted online servers.

Moreover, most SSO systems focus on the user authentication at the beginning of sessions. We observe that the logout process and other ways of terminating sessions are confusing and may lead to security failures. We investigated logout in the existing SSO systems and documented the problems in Shibboleth. As a solution, we suggested separating the concepts of local and global logout.

As the computing environment changes, for example, as applications move to mobile and cloud platforms, there is a need to continuously update authentication technologies. This thesis is a step in this process. We have proposed several incremental improvements to SSO systems and addressed various pain-points from the user's and developer's points of view.

References

[1] 3GPP. Generic authentication architecture (GAA); generic bootstrapping architecture (GBA). Technical Report 3GPP TS 33.220, 3GPP, 2014.

[2] 3GPP. Generic authentication architecture (GAA); system description. Technical Report 3GPP TR 33.919 v 13.0.0, 3GPP, 2016.

[3] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, December 1999.

[4] Jussi Ahokas. Nordean henkilöasiakkaiden verkkopankin kehitys Suomessa vuosina 1982-1997 monitasoisen analyysimallin näkökulmasta (Nordea's personal customers' online banking development in Finland in the period 1982-1997 from the point of views of a multi-level perspective on system innovations model). Master's thesis, Aalto University, School of Business, Jun 3 2010. URL: http://epub.lib.aalto.fi/en/ethesis/pdf/12341/hse_ethesis_12341.pdf.

[5] Edward Amoroso. *Fundamentals of Computer Security Technology*. Prentice-Hall, 1994.

[6] Ross Anderson. Why information security is hard – an economic perspective. In *Proceedings 17th Annual Computer Security Applications Conference, ACSAC 2001.* IEEE, December 2001.

[7] André Andrade. Strong mobile authentication in single sign-on systems. Master's thesis, Aalto University, School of Science, May 8 2011.

[8] Apple Inc. Use Touch ID on iPhone and iPad. Webpage, URL http://support.apple.com/kb/HT5883, Oct 2014. Accessed 28 July 2015.

[9] J. Arkko and H. Haverinen. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). Informational RFC 4187, IETF, January 2006.

[10] B.Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible authentication protocol (EAP). Standards Track RFC 3748, IETF, June 2004.

[11] Lars Backstrom, Paolo Boldi, Marco Rosa, Johan Ugander, and Sebastiano Vigna. Four degrees of separation. In *Proceedings of the 4th Annual ACM Web Science Conference WebSci '12*, pages 33–42, 2012.

[12] Omaimah Omar Bamasag and Kamal Youcef-Toumi. Towards continuous authentication in internet of things based on secret sharing scheme. In *WESS'15: Proceedings of the WESS'15: Workshop on Embedded Systems Security*. ACM, October 2015.

[13] Carol M. Barnum. *Usability testing essentials: ready, set - test!* Morgan Kaufmann Publishers, 2011.

[14] Luciano Barreto, Antonio Celesti, Massimo Villari, Maria Fazio, and Antonio Puliafito. An authentication model for IoT clouds. In *ASONAM'15: Proceedings of the 2015 IEEE/ACM International Conference in Social Networks Analysis and Mining*. ACM, August 2015.

[15] A. Barth. HTTP state management mechanism. Standards Track RFC 6265, IETF, April 2011.

[16] T. Berners-Lee, R. Fielding, and H. Frystyk. Hypertext transfer protocol – HTTP/1.0. Informational RFC 1945, IETF, May 1996.

[17] Simitra Binu, Archana Mohan, Deepak K. T., Manohar S, Mohammed Misbahuddin, and Pethuru Raj. A proof of concept implementation of a mobile based authentication scheme without password table for cloud environment. In *2015 IEEE Internation Advance Computing Conference (IACC)*. IEEE, June 2015.

[18] Matt Bishop. Insider threats in e-voting. Presentation in Trespass winter school, January 14 2016.

[19] Nicholas Bohm and Stephen Mason. Identity and its verification. *Computer Law & Security Review*, 26:43–51, 2010.

[20] T. Bray. The JavaScript object notation (JSON) data interchange format. Standards Track RFC 7159, IETF, March 2014.

[21] L. Jean Camp. Digital identity. *IEEE Technology and Society Magazine*, 23(3):34–41, 2004.

[22] G. Canfora, G. Di Santo, G. Venturi, E. Zimeo, and M. V. Zito. Proxy-based hand-off of web sessions for user mobility. In *Proceedings of the Second Annual International Conference on Mobile and Uniquitous systems: Networking and Services (MobiQuitous'05)*. IEEE, 2005.

[23] Scott Cantor, Jeff Hodges, John Kemp, and Peter Thompson. Liberty ID-FF architecture overview. Technical Report Version 1.2 errata v. 1.0, Liberty Alliance Project, 2004-2005. URL: http://www.projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf.

[24] Guiliana Carullo, Filomena Ferrucci, and Federica Sarro. Towards improving usability of authentication systems using smartphones for logical and physical resource access in a single sign-on environment. *Information Systems: Crossroads for Organization, Management, Accounting and Engineering*, pages 145–153, March 2012.

[25] David Chappell. Introducing Windows CardSpace. Microsoft Developer Net, URL: https://msdn.microsoft.com/en-us/library/aa480189.aspx, April 2006. Accessed 30 July 2015.

[26] Sebastian Clauss and Marit Köhntopp. Identity management and its support of multilateral security. *Computer Networks*, 37:205–219, 2001.

[27] Jan De Clercq. Introducing Windows CardSpace. Windows IT Pro, URL: http://windowsitpro.com/security/introducing-windows-cardspace, August 25 2009. Accessed 30 July 2015.

[28] Lorrie Faith Cranor and Simson Garfinkel, editors. *Security and Usability Designing secure system that people can use*, chapter Usable Security Why do we need it? How do we get it? by M. Angela Sasse and Ivan Flechais. O'Reilly, 2005.

[29] T. Dierks and E. Rescorla. The transport layer security (TLS) protocol, version 1.2. Standards Track RFC 5246, IETF, August 2008.

[30] Ben Dodson, Debangsu Sengupta, Dan Boneh, and Monica S. Lam. Secure, comsumer-friendly web authentication and payment with a phone. In *MOBICASE*, volume 76 of *LNICST 76*, pages 17–38. Springer, 2012.

[31] e-Estonia. Estonian e-Resicency. https://e-estonia.com/e-residents/about/. Accessed 20 May 2016.

[32] Edelman Berland. 2015 Edelman trust barometer. URL: http://www.edelman.com/insights/intellectual-property/2015-edelman-trust-barometer/, Jan 15 2015. Accessed 23 December 2015.

[33] Eduroam. Happy 1,000,000,000th! Eduroam celebrates one billion roaming authentications – helping create a global village for research and education. URL https://www.eduroam.org/happy-1000000000th/. Accessed 30 May 2016.

[34] Elisa. History. URL http://corporate.elisa.com/on-elisa/history/, 2015. Accessed 28 September 2015.

[35] Federation of Finnish Financial Services. TUPAS identification service. URL: https://www.fkl.fi/en/themes/e-services/tupas/Pages/default.aspx, May 7 2015. Accessed 28 December 2015.

[36] FIDO Alliance. FIDO alliance – simpler stronger authentication. URL: https://fidoalliance.org/. Accessed 22 August 2016.

[37] Dinei Florêncio and Cormac Herley. A large-scale study of web password habits. In *Proceedings of the Sixteenth International World Wide Web Conference (WWW2007)*, pages 657–666, May 2007.

[38] Jr. Frederick P. Brooks. No silver bullet – essence and accidents in software engineering. In *Proceedings of the IFIP Tenth World Computing Conference*, pages 1067–76, 1986.

[39] David Förster, Frank Kargl, and Hans Löhr. Short: A framework for evaluationg pseydonym strategies in vehicular ad-hoc networks. In *WiSec'15, 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Jun 22-26 2015.

[40] Sergio Sánchez García, Ana Gómez Oliva, and Emilia Pérez-Belleboni. Is Europe ready for a pan-European identity management? *IEEE Security & Privacy*, 10(4):44–49, July/August 2012.

[41] Jack M. Germain. IBM introducing fingerprint reader into laptop. TechNewsWorld, http://www.technewsworld.com/story/37017.html, 2004. Accessed 3 February 2015.

[42] GlobalPlatform. GlobalPlatform made simple guide: Trusted execution environment (TEE) guide. Whitepaper. URL: http://www.globalplatform.org/mediaguidetee.asp, 2016. Accessed 18 May 2016.

[43] GSM Arena. Motorola ATRIX 4G. http://www.gsmarena.com/motorola_atrix_4g-3708.php, 2015. Accessed 3 February 2015.

[44] N Haller. The S/KEY one-time password system. Informational RFC 1760, IETF, February 1995.

[45] Daniel Halperin, Tadayoshi Kohno, Thomas S. Heydt-Benjamin, Kevin Fu, and William H. Maiser. Security and privacy for implantable medical devices. *IEEE Pervasive computing*, 7(1):30–39, 2008.

[46] D. Hardt. The OAuth 2.0 authorization framework. Standards Track RFC 6749, IETF, October 2012.

[47] Dick Hardt. OSCON 2005 keynote speach – Identity 2.0. Video, 2005. URL: https://www.youtube.com/watch?v=RrpajcAgR1E, Accessed 24 June 2015.

[48] Hannes Hartenstein and Kenneth P. Laberteaux. A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, 2008.

[49] H. J. Haverinen and J. Salowey. Extensible authentication protocol method for global system for mobile communications (GSM) subscriber identity modules (EAP-SIM). Informational RFC 4186, IETF, January 2006.

[50] Shi-Jinn Horng and Shiang-Feng Tzeng. VANET-based secure value-added services. In *SocialCom'14 Proceedings of the 2014 International Conference on Social Computing*. ACM, 2014.

[51] IEEE. IEEE standard for wireless access in vehicular environments – security services for applications and management messages. Technical Report IEEE standard number 1609.2-2016, The Institute of Electrical and Electronics Engineers (IEEE), 2016.

[52] Philip G. Inglesant and M. Angela Sasse. The true cost of unusable password policies: password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*, pages 383–392. ACM, April 2010.

[53] Telecommunication Standardization Sector International Telecommunication Union. X.509 series X: Data networks and open system communications, directory, information technology – open systems interconnection – the directory: Authentication framework. Technical report, International Telecommunication Union, Telecommunication Standardization Sector, August 1997.

[54] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Communications of the ACM*, 43(2), February 2000.

[55] Jostein Jensen and Martin Gilje Jaatun. Federated identity management - we built it; why won't they come? *IEEE Security & Privacy*, 11(2):34–41, March/April 2013.

[56] M. Jones, J. Bradley, and N. Sakimura. JSON web signature (JWS). Standards Track RFC 7515, IETF, May 2015.

[57] M. Jones, J. Bradley, and N. Sakimura. JSON web token (JWT). Standards Track RFC 7519, IETF, May 2015.

[58] M. Jones and J. Hildebrand. JSON web encryption (JWE). Standards Track RFC 7516, IETF, May 2015.

[59] Richard Kemp, Nicola Towell, and Graham Pike. When seeing should not be believing: Photographs, credit cards and fraud. *Applied Cognitive Psychology*, 11(3):211–222, June 1997.

[60] Esa Kerttula. A novel federated strong mobile signature service – the Finnish case. *Journal of Network and Computer Applications*, 56, October 2015.

[61] David P. Kormann and Aviel D Rubin. Risks of the Passport single signon protocol. *Computer Networks*, 33(1-6):51–58, 2000.

[62] Jimmy Kurian. Design and implementation of an authentication and authorization module for service access in ad hoc networks. Master's thesis, Helsinki University of Technology, 2005.

[63] Teemu Kärkkäinen, Mikko Pitkänen, and Jörg Ott. Enabling ad-hoc-style communication in public WLAN hot-spots. *ACM SIGMOBILE Mobile Computing and Communications Review*, 17(1):4–13, 2013.

[64] Kari Laalo. HAKA - technical documentation. URL: https://confluence.csc.fi/display/HAKA/In+English, 2013. Accessed 10 July 2015.

[65] Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, November 1981.

[66] Finnish legislation. 22.4.1999/523 Henkilötietolaki (personal data act). FINLEX. URL: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523#L7P34, 1999. Accessed 18 May 2016.

[67] Andreas Leicher, Andreas U. Schmidt, and Yogendra Shah. Smart OpenID: A smart card based OpenID protocol. In *Information Security and Privacy Research, 27th IFIP TC 11 Information Security and Privacy Conference, SEC 2012, Heraklion, Crete, Greece, June 4-6, 2012*, pages 75–86. Springer, 2012.

[68] Andreas Leicher, Andreas U. Schmidt, Yogendra Shah, and Inhyok Cha. Trusted computing enhanced OpenID. In *2010 International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, 2010.

[69] Ming Li, Shucheng Yu, Joshua D. Guttman, Wenjing Lou, and Kui Ren. Secure ad hoc trust initialization and key management in wireless body area networks. *ACM Transactions on Sensor Networks*, 9(2), 2013.

[70] Liberty Alliance Project. Now more than one billion Liberty-enabled devices and identities. URL: http://www.projectliberty.org/liberty/adoption/?f=liberty/adoption, 2008. Accessed 10 July 2015.

[71] Mikael Linden and Inka Vilpola. An empirical study on the usability of logout in single sign-on system. In *Proceedings of the 1st International Conference in Information Security Practice and Experience*, LNCS 3439, pages 243–254. Springer, 2005.

[72] Juri Lumenko. A solution for certificate distribution in mobile ad-hoc networks. Master's thesis, Helsinki University of Technology, 2007.

[73] Salah Machani, Rob Philpott, Sampath Srinivas, John Kemp, and Jeff Hodges. FIDO UAF architectural overview. FIDO alliance proposed standard, FIDO Alliance, December, 08 2014. URL: https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-overview-v1.0-ps-20141208.html.

[74] Eve Maler. Federated identity management, an overview of concepts and standards. In *XML 2005*, November 2005.

[75] Tobias Markmann, Thomas C. Schmidt, and Matthias Wählisch. Federated end-to-end authentication for the constrained Internet of Things using IBC and ECC. In *SIGCOMM'15: Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, 2015. Also published in: September 2015 ACM SIGCOMM Computer Communication Review - SIGCOMM'15: Volume 45 Issue 4, October 2015.

[76] Merriam-Webster. Dictionary. url: http://www.merriam-webster.com/. Accessed 24 June 2015.

[77] Microsoft. Microsoft Passport FAQ. Web page, URL: https://support.microsoft.com/en-us/kb/277759. Accessed 13 July 2015.

[78] Microsoft. One account for all things Microsoft. Web page: URL: https://www.microsoft.com/en-us/account/default.aspx, 2015. Accessed 30 July 2015.

[79] Microsoft Download Center. Windows Live ID web authentication SDK 1.2. Web page, URL: http://www.microsoft.com/en-us/download/details.aspx?id=7843, November 2008. Accessed 30 July 2015.

[80] Microsoft Identity and Access Team. Beyond Windows CardSpace. MSDN Blogs, Claim-Based Identity Blog, URL: http://blogs.msdn.com/b/card/archive/2011/02/15/beyond-windows-cardspace.aspx, February 15 2011. Accessed 30 July 2015.

[81] Laura Marcia Villalba Monné. One-time passwords and remote credential management using On-Board Credentials. Master's thesis, Aalto University, 2011.

[82] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen. HOTP: An HMAC-based one-time password algorithm. Informational RFC 4226, IETF, December 2005.

[83] Roger M. Needham and Michael D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, December 1978.

[84] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. The Kerberos network authentication service (V5). Standards Track RFC 4120, IETF, July 2005.

[85] Clifford Neuman and Theodore Ts'o. Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38, September 1994.

[86] Jacob Nielsen. *Usability Engineering*. AP Professional, 1993.

[87] OECD. Government at a glance 2013. OECD Publishing, 2013. URL http://dx.doi.org/10.1787/gov_glance-2013-en, Accessed 23 December 2015.

[88] Ministry of Transport and Communications. Mobiilivarmenne - mobil id: What? URL: http://www.mobiilivarmenne.fi/en/, 2016. Accessed 27 May 2016.

[89] Lawrence O'Gorman. Comparing passwords, tokens and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[90] OpenID. OpenID authentication 2.0 – final. Technical report, Openid.net, December 5 2007. URL: http://openid.net/specs/openid-authentication-2_0.html, Accessed 10 August 2015.

[91] A. Pashalidis and C. J. Mitchell. A taxonomy of single sign-on systems. In *Information Security and Privacy - 8th Australasian Conference, ACISP 2003, Wollongong, Australia*, LNCS 2727, pages 249–264. Springer, July 2003.

[92] Ravi Singh Pippal, C.D. Jaidhar, and Shishikala Tapaswi. A novel smart card mutual authentication scheme for session transfer among registered devices. In *2013 IEEE 3rd International Advance Computing Conference*, 2013.

[93] Uthpala Subodhani Premarathne and Ibrahim Khalil. Multiplicative attribute graph approach for persistent authentication in single-sign-on mobile systems. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2014.

[94] R. Quian Quiroga, L. Reddy, G. Kreiman, C. Koch, and I. Fried. Invariant visual representation by single neurons in the human brain. *Nature*, 435(7045):1102–1107, June 23 2005.

[95] Nick Ragouzis, John Hughes, Rob Phillpot, Eve Maler, Paul Madsen, and Tom Scavo. Security assertion markup language (SAML) v2.0 technical overview. Technical report, OASIS, March 2008. URL: https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf.

[96] Vaibhav Rastogi and Ankit Agrawal. All your Google and Facebook logins are belong to us: A case for single sign-off. In *Eighth International Conference on Contemporary Computing (IC3)*. IEEE, 2015.

[97] D. Recordon, M. Jones, J. Bufu, J. Daugherty, and N. Sakimura. OpenID provider authentication policy extension 1.0. Technical report, Openid.net, December 30 2008. URL: http://openid.net/specs/openid-provider-authentication-policy-extension-1_0.html, Accessed 14 August 2015.

[98] Drummond Reed, Les Chasen, and William Tan. OpenID identity discovery with XRI and XRDS. In *Proceedings of the 7th symposium on Identity and trust on the Internet (IDtrust'08)*, pages 19–25. ACM, 2008.

[99] Teemu Rissanen. Electronic identity in finland: Id cards vs. bank ids. *Identity in the Information Society*, 3(1):175–194, March 6 2010.

[100] RSA. RSA SecurID. Webpage URL: https://www.rsa.com/en-us/products-services/identity-access-management/securid, 2016. Accessed 18 May 2016.

[101] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, and C. Mortimore. OpenID Connect core 1.0 incorporating errata set 1. Technical report, Openid.net, November 8 2014. URL: http://openid.net/specs/openid-connect-core-1_0.html, Accessed 14 August 2015.

[102] Savio Sciancalepore, Angelo Capossele, Giuseppe Piro, Gennaro Boggia, and Biuseppe Bianchi. Key management protocol with implicit certificates for IoT systems. In *IoT-Sys'15: Proceedings of the 2015 Workshop on IoT Challenges in Mobile and Indistrial Systems*. ACM, 2015.

[103] Shibboleth Consortium. What's Shibboleth? URL: http://shibboleth.net/about/. Accessed 10 July 2015.

[104] Simon S. Y. Shim, Geetanjali Bhalla, and Vishnu Pendyala. Federated identity management. *IEEE Computer*, 38(12):120–122, December 2005.

[105] Sampath Srinivas, Dirk Balfanz, Eric Tiffany, and Alexei Czeskis. Universal 2nd factor (U2F) overview. FIDO alliance proposed standard, FIDO Alliance, May, 14 2015. URL: https://fidoalliance.org/specs/fido-u2f-v1.0-nfc-bt-amendment-20150514/fido-u2f-overview.html.

[106] Clare Sullivan. Digital identity - the legal person? *Computer Law & Security Review*, 25:227–236, 2009.

[107] Helen Tang, Mazda Salmanian, and Connie Chang. Strong authentication for tactical mobile ad hoc networks. Technical memorandum DRDC Ottawa TM 2007 - 146, Defence Research and Development Canada, July 2007.

[108] The European Commission. Commission implementing regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance level for electronic identification means pursuant to article 8(3) of regulation (eu) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Official Journal of the European Union, L 235/7, Sep 9 2015. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=EN.

[109] The European Parliament and the Council of the European Union. Regulation (EU) no 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/ec. Official Journal of the European Union, L 257/73, Aug 28 2014. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R09100&from=EN.

[110] United Nations Children's Fund (UNICEF). Every child's birth right: Inequities and trends in birth registration. URL: http://www.data.unicef.org/corecode/uploads/document6/uploaded_pdfs/corecode/Birth_Registration_lores_final_24.pdf, December 2013. Accessed 30 June 2015.

[111] United Nations Human Rights. Convention on the rights of the child. URL: http://www.ohchr.org/en/professionalinterest/pages/crc.aspx, November 1989.

[112] United Nations Statistics Division. Civil registration system. URL: http://unstats.un.org/UNSD/demographic/sources/civilreg/default.htm, 2013. Accessed 30 June 2015.

[113] Esa Virtanen. A distributed certificate repository and security module. Master's thesis, Helsinki university of Technology, 2008.

[114] Kun Yang, Domenic Forte, and Mark M. Tehranipoor. Protecting enpoint devices in IoT supply chain. In *ICCAD'15, Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*. IEEE, 2015.

[115] Maria C. Yang and Daniel J. Epstein. A study of prototypes, design activity, and design outcome. *Design Studies*, 26:649–669, 2005.

[116] Yubico. Yubikey standard and Nano. Webpage URL: https://www.yubico.com/products/yubikey-hardware/yubikey-2/, 2015. Accessed 28 July 2015.

[117] Xinwen Zhang, Joshua Schiffman, Simon Gibbs, Anugeetha Kunjithapatham, and Sangoh Jeong. Securing elastic applications on mobile devices for cloud computing. In *CCSW'09: Proceedings of the 2009 ACM workshop on Cloud computing security*, pages 127–134, 2009.

[118] Shanyang Zhao, Sherri Grasmuck, and Jason Martin. Identity construction on facebook: Ditigal empowerment in anchored relationships. *Computers in Human Behavior*, 24:1816–1836, 2008.

[119] Mary Ellen Zurko and Richard T. Simon. User-centered security. In *Proceedings of the 1996 workshop on New security paradigms, NSPW '96*. ACM, 1996.

Aalto-DD 226/2016

ISBN 978-952-60-7102-2 (printed)
ISBN 978-952-60-7101-5 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

Aalto University
School of Science
Computer Science
www.aalto.fi

BUSINESS +
ECONOMY

ART +
DESIGN +
ARCHITECTURE

SCIENCE +
TECHNOLOGY

CROSSOVER

DOCTORAL
DISSERTATIONS