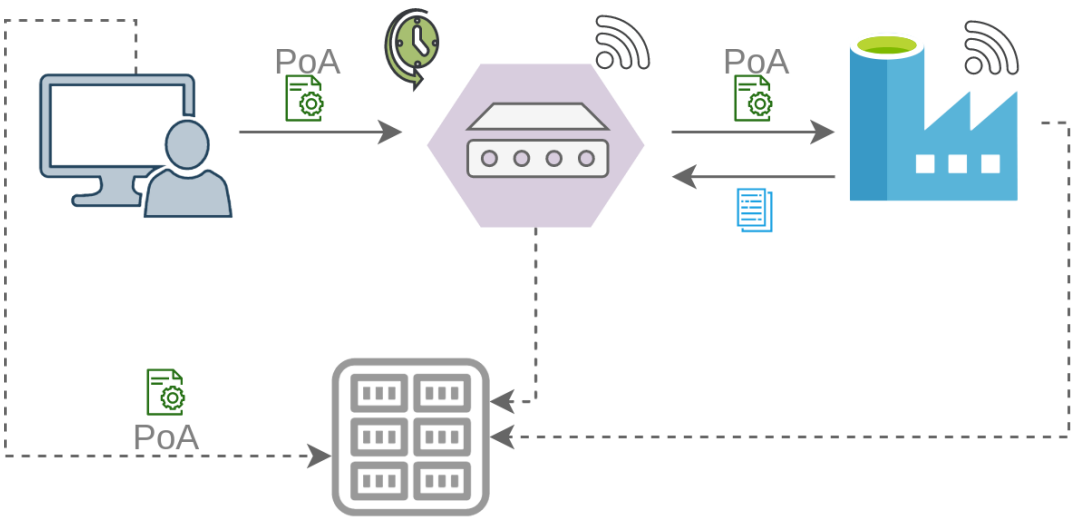
DOCTORAL THESIS

Digital Power of Attorney for authorization in industrial cyber-physical systems



Sreelakshmi Vattaparambil Sudarsan

Cyber Physical Systems

LULEÅ UNIVERSITY OF TECHNOLOGY

Digital Power of Attorney for authorization in industrial cyber-physical systems

Sreelakshmi Vattaparambil Sudarsan

Dept. of Computer Science and Electrical Engineering
Luleå University of Technology
Luleå, Sweden

Supervisors:

Olov Schelén, Ulf Bodin

To Abhi and my family...

Abstract

Since ancient times, there has been a practice to authorize individuals that we trust. Today, we grant credentials and privileges digitally, making authorization a crucial part of security control and extending its use cases beyond people and web applications. Authorization plays an important role in emerging technologies such as the Internet of Things (IoT) and Cyber-Physical Systems (CPS), and there is a trend toward intelligent devices such as autonomous vehicles that are capable of executing tasks on our behalf.

However, there are challenges in facilitating this evolution. Industrial use cases with many devices, contractors, subcontractors, and other parties need to maintain trust by sub-granting in one or many steps to define a trust chain. Ultimately Industrial CPS and semi-autonomous devices should be authorized to work as agents with defined credentials on behalf of their contractor. This would enable them to function self-sufficiently at a target site or network for a set amount of time.

The scope of this thesis is a new way of authorization known as the Digital Power of Attorneys. Traditionally, Power of Attorney is a legal document that is used for granting a person's authority to a trusted individual to act/work (e.g., running a business) on behalf of the first person. The objective of this thesis is to develop digital Power of Attorney based authorization for Cyber-Physical Systems and the Internet of Things. This technique enables devices (agents) such as autonomous or semi-autonomous devices to work/act on behalf of human beings (principals), even if he/she is not available online.

The literature study includes both academic concepts and industrial authorization solutions, protocols, and standards such as OAuth, UMA, GNAP, and ACE. PoA based authorization is inspired by the concept of proxy signatures by warrants and developed for industrial use, both as stand-alone libs and as extensions to existing standard protocols. The major standards that we propose to be extended with the PoA based authorization are IETF standards OAuth and ACE. In this way, the work in this thesis is highly correlated with the IETF. In addition to the academic papers on PoA based authorization and its applications, this thesis includes IETF Internet-Drafts as part of the standardization process of the PoA based authorization technique.

The development of PoA based authorization technique begins with designing a Proof-of-Concept based on the gaps identified in existing authorization techniques. For implementation in current networks, different ways of providing PoA-based authorization are explored. First, by extending the OAuth protocol as a new OAuth grant type to add the principal entity to the OAuth protocol that can delegate the client. Second, by extension of the ACE framework, which adds a notion of PoA based delegation to ACE. Third, by implementing an open-source library that can be downloaded and used independently

by each entity to interpret the PoA. These approaches address the PoA interpretation challenges and enable every entity being part of the process to use and verify PoAs.

This thesis defines the architecture, protocol flow, and PoA structure of the proposed authorization technique and demonstrates its implementation in several use cases such as zero touch-device onboarding and delegation of smart devices in a mining station. Furthermore, possible security threats and vulnerabilities of the proposed system are thoroughly analyzed using different approaches such as threat modeling, risk assessment, and exploiting the system in the context of different attack scenarios.

Publications

The content of this thesis has been published in different peer-reviewed conferences and journals. This thesis comprises multiple IETF Internet drafts (IDs) that were submitted and presented to different IETF working groups in an effort to standardize the proposed authorization technique.

Peer-reviewed Articles

1. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, "A Model for Signatories in Cyber-Physical Systems," 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria, 2020, pp. 15-21, doi: 10.1109/ETFA46521.2020.9212081.

2. **S. V. Sudarsan**, O. Schelén and U. Bodin, "Survey on Delegated and Self-Contained Authorization Techniques in CPS and IoT," in IEEE Access, vol. 9, pp. 98169-98184, 2021, doi: 10.1109/ACCESS.2021.3093327.

3. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, "Multilevel Subgranting by Power of Attorney and OAuth Authorization Server in Cyber-Physical Systems," in IEEE Internet of Things Journal, vol. 10, no. 17, pp. 15266-15282, 1 Sept.1, 2023, doi: 10.1109/JIOT.2023.3265407.

4. **S. V. Sudarsan**, O. Schelén, U. Bodin and N. Nyström, "Device Onboarding in Eclipse Arrowhead Using Power of Attorney Based Authorization", 2022 IEEE 27th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Paris, France, 2022, pp. 26-32, doi: 10.1109/CAMAD55695.2022.9966899.

5. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, "Token Interpretation and Security Evaluation of Power of Attorney based Authorization Technique," Submitted to IEEE IoT Journal.

IETF Internet-Drafts

1. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, Delegation based Device Onboarding using PoA authorization, "vattaparambil-iotops-poa-based-onboarding-02", Internet Engineering Task Force, 2023.

2. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, Positioning of PoA, "draft-vattaparambil-positioning-of-poa-01",Internet Engineering Task Force, 2023.

3. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, OAuth-PoA Grant Type, "draft-vattaparambil-oauth-poa-grant-type-01", Internet Engineering Task Force, 2023.

4. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, PoA based Device Registration in ACE framework, "draft-vattaparambil-ace-wg-poa-device-reg-00", Internet Engineering Task Force, 2023.

Other works

1. **S. Vattaparambil Sudarsan**, O. Schelén and U. Bodin, Decentralized PoA based authorization, "draft-vattaparambil-irtf-dinrg-poa-00", Internet Engineering Task Force, 2023.

Contents

Acknowledgments

My journey so far has been made possible by the encouragement and support of my teachers, family, and friends. Even though I can not mention everyone, I would like to express my gratitude to each and every one of them. This thesis is not the work of a single person; rather, it is the result of the efforts of many people who assisted me along the way.

Above all, I would like to express my sincere gratitude to my supervisors Olov Schelén and Ulf Bodin for their unwavering support and amazing advice during my PhD journey. I am so grateful for your guidance and insight in helping me grow, and I am thankful to you for everything I have accomplished in the last four years. Your helpful feedback has constantly inspired me to aim for success. I would like to thank Rajesh Koduri and Sabu M. Thampi for introducing me to the exciting field of research. I am always motivated by your advice and insights in expanding my horizons of research.

I am thankful for all my friends and colleagues at EISLAB who have been a valuable part of this fascinating journey. I cannot forget the times we spent together, the exciting Magic: The Gathering games we played, and the harmonious notes from our music band.

I had the good fortune to have many Malayali friends with me in Luleå, who helped me feel at home. I sincerely thank each and every one of you for all the wonderful memories in Luleå.

I am out of words to show gratitude to Sruthy and my parents who always stand by my side and encourage me. I am always inspired by you both and you are always my role models. Without you, nothing would be possible. Thank you so much, Abhi for your support throughout this adventure. You've always been there for me and have always encouraged me. And I'm always motivated by your space research.

Thank you!

Part I

Chapter 1

Introduction

In our fast-paced lives, sometimes it is not easy to finish all assigned tasks within the timeframe. We can address this by transferring our authority to our trusted ones to carry out some of our important tasks. Transfer of authority is always restricted to a set of privileges because if someone is allowed to carry out a task on behalf of us, they are only allowed to access credentials related to that particular task. For example, we prefer that the person who represents us at a meeting does not possess access to our confidential banking information. These human-to-human agreements and contracts are protected by legal regulations and procedures. A formal approach is using the Power of Attorney (PoA) that delegates the secondary party to take over our assets or business. It is a legal document that outlines the agreement between the involved parties and is officially tied to governmental laws. Today, with the proliferation of digital transformation, we tend to rely on our trusted devices more than on people. These intelligent devices can be used for a wide range of applications, from personal use cases to large-scale industrial use cases. This opens a possibility for humans to delegate their trusted devices to work on the user's behalf, which enables the access of data from third-party resource owners. However, in this case, where the involved parties are smart devices rather than humans, we need a digital technique that can systematically represent the agreements between the parties. Speaking in terms of computer security, we need an *Authorization technique* that enables users to delegate their trusted devices to act/work on their behalf by accessing data from third-party resource owners.

The following sections of this chapter outline the significance of this research by discovering the gaps, motivating the need, and formulating the research questions that can resolve the identified challenges.

1.1 Motivation

Authorization is an inevitable process in network management and cyber security to prevent illegitimate access. It is the process followed by authentication for regulating access to protected resources with different privileges using different access control mod-

els. There are different types of authorization techniques that range from traditional role-based access control methods to industry-standard delegation-based authorization techniques. The appropriate authorization technique is determined by the specific application scenario in which it has to be implemented. Delegation-based authorization techniques are the most suitable authorization techniques for a user to make his/her trusted CPS or IoT device work on their behalf. These techniques enable the user to grant limited privileges to devices, that allow them to act on behalf of the user.

Consider a simple use case scenario in which a user is required to retrieve a package from the post office and he/she is currently unavailable. Suppose the user trusts an autonomous vehicle that can be used to collect the package on the user's behalf. This is a small-scale scenario where a user leverages smart IoT/CPS devices to enhance their productivity. Similarly, in a large-scale industrial scenario, there will be multiple situations:

Situation 1: Consider a single user who can be assigned to perform several tasks with different access privileges. For example, a contractor working on the collection of raw materials from the supplier will be also part of some other tasks within the supplier company. What if the contractor's trusted automatic or semi-automatic device (e.g., a smart truck) can work/act on behalf of the user with his/her same power? How does the supplier at the other end who trusts the contractor verify and provide the required resources to the device?

Situation 2: Consider a more complex scenario in which the contractor has n number of devices at their work site that can be used to complete either a single task or multiple tasks. How can the contractor enable the chain of devices to work on the contractor's behalf by transferring his/her authority with limited privileges?

Situation 3: Consider if the device has to execute the designated tasks, even if the contractor is not available online. How does the contractor delegate the device in a self-contained manner, without the need to remain online during the entire process?

All these questions inspired this research to examine different authorization techniques to identify their unique properties and relevant applications. The study of authorization techniques started with surveying academic publications and identified several high-level authorization techniques. Later, the state-of-the-art narrowed down to delegation-based authorization techniques and found several works proposing delegation-based authorization from different perspectives that may or may not be used in the industry. The search ended up in different Internet Engineering Task Force (IETF) standards for authorization that facilitate the industry uptake. This research is inspired by different security standards developed by the IETF community, which provides standardized solutions that can be used to build different applications across a wide range of industries.

1.1.1 Challenges

Challenges were indeed present throughout this research. They are identified in each stage of the research process and a solution to one challenge emerges a newer one. The following challenges are formed in four distinct phases of this research, and they are interconnected to each other.

Challenge 1: To identify if there is a pre-existing authorization technique that is applicable in the above-mentioned situations.

Challenge 2: To design and implement a subgranting-based authorization technique from scratch, that allows the user to grant their authority to their trusted device, allowing the device to work on behalf of the user.

Challenge 3: Identify potential security concerns that must be addressed during the above-mentioned situations and provide mitigation strategies.

Challenge 4: Examining different authorization standards to assess their extension and applicability in the situations as mentioned earlier, while outlining the proposed solution's potential to fill the existing gaps.

1.2 Research Questions

To overcome the challenges identified in this research, the following research questions are formulated [Fig 1.1]. These research questions outline the scope of this research and guide this research to examine the state-of-the-art and propose solutions to address the identified gaps.

RQ1 *Which existing authorization techniques allow the users to subgrant their authority to their trusted CPS/IoT devices to make them work/act on behalf of the user?*

RQ2 *How to build a subgranting-based authorization framework that allows the user to transfer their authority to their trusted devices in a self-contained manner, and enables them to work/act on behalf of the user even if they are offline? What are the primary security concerns that must be addressed during this authorization process?*

RQ3 *How to standardize the proposed authorization technique by integrating it with the existing delegation-based authorization standards to enhance the scope of authorization, ensuring compatibility and interoperability?*

1.3 Research methodology and Approach

A formalized research methodology is designed to systematically investigate the research questions from different perspectives with respect to the identified challenge. The research

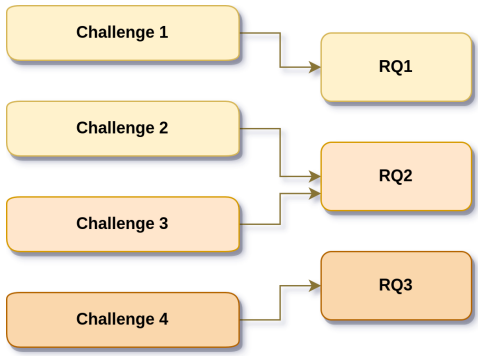


Figure 1.1: ***Connection between challenges and research questions***

methodology used in this thesis falls under the category of Experimental computer science and engineering (ECSE) research. "ECSE is the fundamental underpinning of the computer hardware and software that drive the information age". ECSE performs a main role in the creation of technical ideas emerging from academic research with adequate diversity for the industry use cases thereby developing marketable products. ECSE defines the creation of or experimentation with computer artifacts that can be both hardware and software systems to implement and thereby study computational processes, algorithms, or mechanisms. The three principles served by ECSE artifacts are proof of concept, proof of performance, and proof of existence to evaluate whether the results obtained are better than the existing alternative and their qualitative analysis, which can be subjective [7].

Proposing a new way of device authorization technique requires extensive analysis of the existing techniques, and standards, and an understanding of industrial prerequisites. This research started with the objective of designing a delegation-based authorization framework for IoT/CPS devices to work/act on behalf of the users. Later, with the analysis of existing authorization standards, the objective has been extended to standardizing the proposed authorization technique.

The first step in this research was the literature study of existing techniques in the field of authentication and authorization to identify the gaps. This method aids in narrowing down the main research area and focusing on a specific topic in the field of study. Following this, a primary research question is developed, which is considered the most fundamental. More questions are developed eventually followed by the main research question, bringing the research closer to the actual problem or gap in the research area.

Each individual research question is examined and answered by developing a Proof of Concept (PoC), prototypes, or open-source libraries based on industrial use cases. Research advancements or findings in each stage are assessed using both quantitative and qualitative analyses and the results are published in the papers that are part of this thesis.

Following this, the scope of this research has been expanded to include IETF standardization of the proposed solution. In order to achieve this goal, multiple Internet drafts are written and updated on a regular basis according to ongoing discussions.

The experiments in this study are performed using different computer software tools, and the results are evaluated. Real-time experiments with actual hardware devices and humans are not part of this lab-based research. In this study, we used the above-mentioned methodologies to gain a deep understanding of the field of study, identify potential gaps, and find solutions to existing problems.

This study follows research ethics by avoiding harm to others and being honest and trustworthy with the data. The ACM code of ethics and professional conduct [1] defines different ethical issues in computer science research and provides guidelines to address them. Accordingly, this thesis has shown respect for other people's intellectual works by including adequate references. The efforts to help others have been made by making all the publications, results, and experimental data of this research publicly available [9].

1.4 Contributions

The challenges and research questions identify a research gap indicating the necessity of a comprehensive authorization method. This thesis introduces a subgranting-based authorization technique inspired by the traditional *Power of Attorney (PoA)*, that enables IoT/CPS devices to act/work on behalf of the users for a predefined time, even if the user is not online.

The contributions start with Paper A, where the conceptual architecture and structure for the PoA based authorization are defined. Later, the proposed solution is compared with the existing techniques in Paper B, which provides an extensive survey of the state-of-the-art. The most important authorization standard identified as similar to the proposed solution is OAuth. Upon further examination of the OAuth standard, an extension of OAuth based on PoA based authorization is proposed in Paper C. Paper D is an application of the proposed authorization technique on IoT device onboarding in Arrowhead local cloud. The security evaluation of the proposed authorization technique and PoA interpretation using the ACE framework and PoA library are defined in Paper E.

An important contribution of this research is IETF Internet drafts. Draft A is on IoT device onboarding using PoA based authorization, which is part of the IoTOPS working group. Draft B explains the positioning of PoA based authorization with other existing authorization standards similar to the proposed solution. Draft C is on the OAuth-PoA grant type, which is part of the OAuth working group. Draft D explains the client registration and the AS validation problems in the ACE framework, which is part of the ACE working group.

Other contributions include the open-source library poa_lib for PoA interpretation and other source code for different use case implementations. The connection between research questions, papers, and IETF drafts is shown in Fig 1.2.

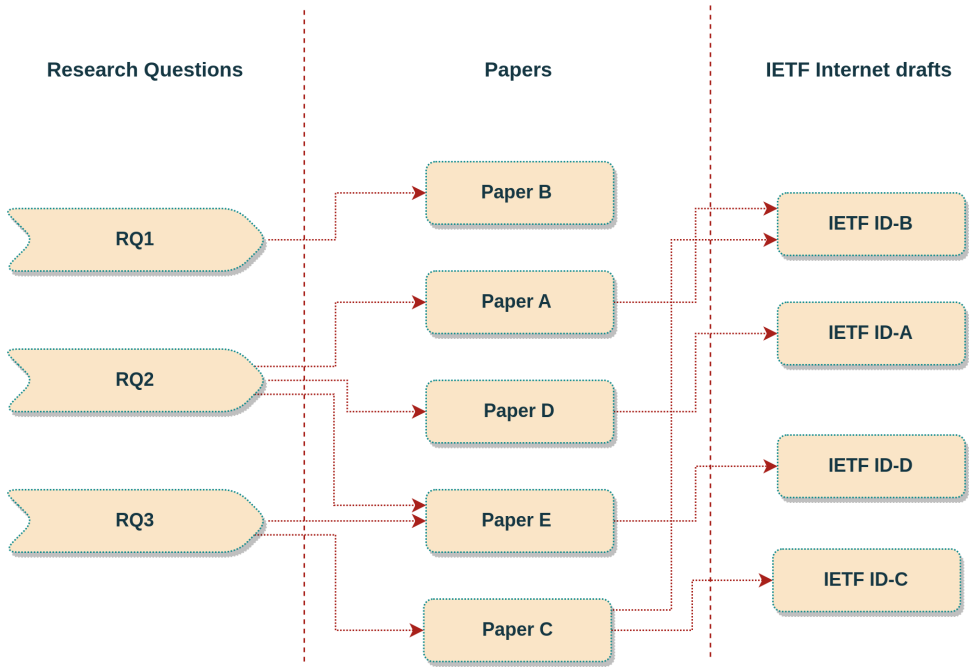


Figure 1.2: ***Connection between research questions, papers, and Internet drafts in this thesis***

1.5 Thesis outline

This compilation thesis consists of two parts: Part 1 of this thesis contains eight chapters. Chapter 1 ends with this section and Part II of this thesis contains papers and internet drafts that have been reformatted to comply with the thesis format.

Chapter 2 **Research Background**
This chapter defines different background concepts that are considered important for this thesis. The important background defined in this chapter are Cyber Physical-System, Internet of Things, authorization techniques in CPS and IoT, and an introduction to device onboarding.

Chapter 3 **IETF Standardization**
This Chapter describes the standardization process detailing different processes part of IETF standardization such as internet drafts and RFCs. This chapter defines the PoA based authorization in the context of IETF and provides an outline of the different internet drafts part of this thesis.

Chapter 4 **Onboarding Concepts**
This Chapter defines the important onboarding concepts mainly IETF standards or protocols on device onboarding that are used in the industry. The main standards included here are FIDO and BRSKI protocols.

Chapter 5 **Use Cases**
This Chapter defines different use cases where PoA based authorization can be used. This includes basic use cases such as device onboarding, mining station use cases, and use cases that are selected from the ACE framework.

Chapter 6 **Contributions**
This Chapter provides the contributions of this thesis by including an outline for the different papers and internet drafts published as part of this work.

Chapter 7 **Conclusions**
This Chapter concludes this thesis by answering the different research questions that are raised at the beginning of the thesis.

Chapter 8 **Findings, Discussion, and Future Work**
This chapter discusses various findings from this thesis that have been published through papers and internet drafts. It also outlines the future directions for improvements and research.

Chapter 2

Research Background

This chapter provides an overview of the research area where the proposed authorization technique is used. It provides the necessity for a secure authorization technique, especially the relevance and significance of delegation-based authorization techniques in the field of Cyber-Physical Systems (CPS) and the Internet of Things (IoT).

2.1 Cyber Physical-Systems and Internet of Things

2.1.1 Cyber Physical-System

CPS integrates Internet Technologies (IT) with electronic or mechanical devices that can control and monitor the physical world over data exchanges [21]. An important property of CPS is the interaction between cyber components (eg: processing units, and computing devices) and physical components (eg. sensors and actuators) of CPS [11]. The CPS uses computer-based algorithms for the automated and controlled functioning of hardware and software components in the network.

In contrast to IoT, which primarily pertains to the interconnection of things via the Internet and the exchange of data between them, a CPS is typically more domain-specific, with the interaction between more advanced, often semi-autonomous, physical, and cyber environments achieved through the integration of algorithmic computations. A common aspect is that both the IoT and CPS pose high security and privacy concerns [2].

CPS comprises three components: 1) communication, 2) control, and 3) computation, that are all integrated with the physical world. Since 2006, there has been an interesting evolution of embedded systems from information management systems (the 1960s) to CPS. CPS has more physical components than embedded systems. CPS, unlike embedded systems, focuses on the link between computational and physical elements rather than the computing element itself. The communication is established for data exchange between the physical and computing elements through the CPS communication component.

The general workflow of CPS includes three different steps: monitoring, networking, computing, and actuation. The monitoring step monitors the physical environment of

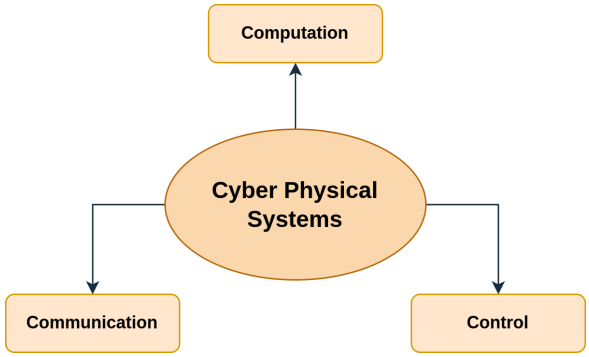


Figure 2.1: Three main components of CPS [24]

the system, which includes different sensors and actuators. In the networking step, aggregation and diffusion of a large amount of real-time data from different types of sensors are carried out. The aggregated data is used by the analyzers to process further. The data collected from the physical environment is analyzed and checked in the computing step to see if the physical process meets certain pre-defined criteria. If the system fails to meet the criteria, the system will suggest corrective actions. In the actuation step [22], the actions determined in the computing step are carried out. The complex concept of

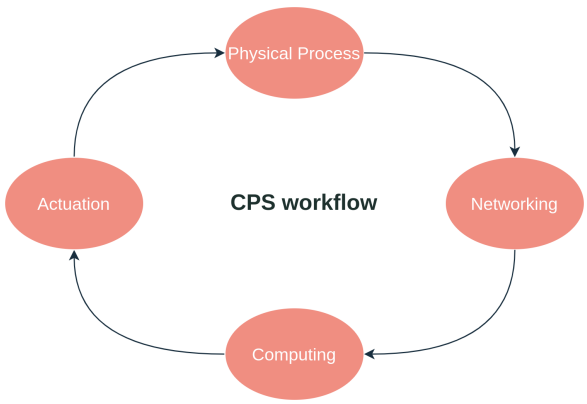


Figure 2.2: CPS workflow [22]

CPS is defined using a concept map [20], which defines CPS as networked/distributed control systems that are intelligent, adaptive, and predictive systems that possibly interact with humans in real-time. The CPS can be used in different application domains such as consumer and industry, smart energy systems, healthcare, military, robotics, and

transportation. The primary requirements of CPS are improved design tools, design methodology, and cybersecurity. Cybersecurity is mainly concerned with resilience, privacy, intrusion detection, and malicious attacks. The increased interaction between the cyber system and the physical system of the CPS can lead to an increase in the number of security vulnerabilities in the cyber system. This thesis targets the cybersecurity requirements of the CPS [20].

2.1.2 Internet of Things

Kevin Ashton coined the term "Internet of Things" in 1999 for supply chain management. However, people are now using IoT for a variety of applications such as healthcare, utilities, transportation, smart homes, smart cities, and so on [10]. The number of connected things in the world has now reached billions or trillions. IoT technology connects things and smart objects that can sense and monitor their surroundings, as well as process and transmit the collected sensor data. The Industrial IoT (IIoT) is a subset of IoT that is used to connect all industrial assets through automated M2M and industrial communications. The ACE framework is an IETF standard that is specifically designed for constrained environments such as IoT or IIoT using protocols such as CBOR and CoAP that are suitable for resource-constrained devices.

IoT consists of three components: 1) hardware, 2) middleware, and 3) presentation. Sensors, actuators, and embedded communication hardware are all part of the hardware. The middleware primarily provides the computational tools and storage required for data analytics. The presentation includes tools for visualization and interpretation that can be used on a variety of platforms and applications. Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), addressing schemes, data storage, and analytics, visualization are important technologies that make up these IoT components.

IoT architecture

There are different IoT architectures with different layers. According to many works such as [27], [13], and [3] the most basic IoT architecture has three main layers: a perception layer or device layer, a network layer, and an application layer. The functions and features of each layer are defined based on the devices present within it. The perception layer mainly consists of physical devices such as RFIDs, sensors, and actuators. The main functions of this layer are data acquisition, data processing from physical devices, and transmitting data to the higher layers. These valuable sensor data are then transmitted to the network layer [14] [25]. This layer also performs IoT node collaboration in local and short-range networks.

The network layer is the middle layer of the IoT architecture, which primarily contains network devices. The main function of this layer is to route data between heterogeneous networks and devices using different network devices (switch, hub, router, etc.), communication technologies (Bluetooth, WiFi, etc.), and different protocols such as CoAP and MQTT [12].

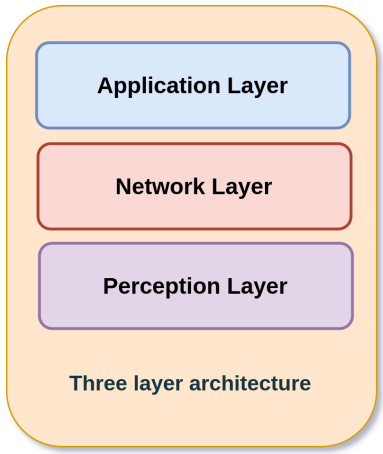


Figure 2.3: ***IoT three-layer architecture***

The application layer is the high-level IoT layer, that defines different IoT applications and provides the end-user with the processed data from different IoT devices [3]. Fig. 2.3 shows the IoT security architecture with three different layers.

Some works demonstrate a five-layer IoT architecture that introduces two more layers, referred to as the midware layer and business layer, for service management and management of the entire IoT architecture using business models [12].

There are different security procedures in the IoT network, such as network entry and secure connection to a distant peer. The network entry procedure specifies how IoT devices are authenticated for remote servers. In the secured connection to a distant peer procedure, the connection between an IoT device and an unconstrained node is defined using two secure channels via a gateway [4]. There are different challenges in IoT security such as object identification, authentication, authorization, privacy, lightweight cryptosystems, and security protocols, software vulnerability and backdoor analysis, malware in IoT, and security issues from Android [26].

2.2 Authorization techniques in CPS and IoT

There are different security requirements such as identity management, authentication, authorization, confidentiality, and integrity, which are interconnected to provide different aspects of security in the research domain of CPS and IoT [8]. In this thesis, the focus is on authorization techniques, that are used to provide access to protected resources based on the access privileges. Authorization is closely related to access control, where authorization is part of the policy definition phase of access control, and access policy enforcement is based on the authorization process in the policy definition phase. There are different types of authorization techniques, most of the applications use access control

models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role-Based Access Control (RBAC) to control access to protected resources. Another important type of authorization technique is Delegation-based authorization, where users provide or delegate their privileges to other entities or client services [17].

A common delegation-based authorization used in the industry is the Open Authorization (OAuth) protocol, which is a web-based authorization standard based on the representational state transfer (REST) protocol. It is primarily used to authorize third-party services without sharing the password credentials. The main entities that are part of this authorization are the client, resource owner, authorization server, and resource server. Here, third-party services (clients) access the resource owner's protected resources on his/her behalf via the authorization server. Access to the requested resources is provided by the authorization server in the form of access tokens. These access tokens are time-limited, entail that they expire after a certain period of time, and are encoded and digitally signed to prevent security attacks. Certain parts of the OAuth protocol flow are explicitly acknowledged as beyond the scope of the standard and are deliberately left open for further extensions.

Another significant authorization framework that is specifically designed for constrained devices is the Authentication and Authorization for Constrained Environments (ACE) framework. ACE is built on OAuth with a similar protocol flow or interactions. Other building blocks of ACE include CoAP, CBOR, and COSE. Different entities that are part of the ACE framework are the client, authorization server, and resource server. Here, the protocol flow starts with the client sending an access token request to the authorization server, different from the OAuth protocol, where the client starts the protocol communicating with the resource owner.

In addition, an interesting academic work on delegation-based authorization is Proxy signatures, which is an inspiration for PoA based authorization. Proxy signatures allow a proxy signer to sign on behalf of the original signer based on cryptographic algorithms such as DLP, RSA, and ECDSA. This method is used when the user requires to sign and is currently unavailable. There are different ways of providing delegation in this method such as full delegation, partial delegation, and delegation by warrant. The last way of delegation is more useful when the original signer needs to share limited credentials with the proxy signer. Similar to other authorization tokens, the proxy signature with a warrant is time-limited. The application of proxy signatures in the industry is challenging and requires an industry-standard format for the warrant.

2.3 Device Onboarding

Device onboarding is an area that is subjected to extensive industry research as part of standardization; different standards have been developed and further research is now being conducted for onboarding in particular application scenarios and with specific features. The range of application scenarios includes constrained devices, non-constrained devices, devices without real-time connectivity, etc. Different emerging features include late binding, zero-touch onboarding, etc. The ability to track a device's ownership as it

moves through the supply chain from the manufacturer to the device owner is one of the key features that are emerging. The different emerging features of onboarding that this thesis focussed are on the use of delegations, transfer of ownership, reselling the device, and bootstrapping devices with no real-time connectivity with the device owner. PoA based onboarding uses delegation or subgranting features to onboard or bootstraps the devices to the target network with self-contained PoAs that allow the device owner to be offline during the imprinting stage of bootstrapping. More details on device onboarding are presented in Chapter 4.

Chapter 3

IETF Standardization

The Internet provides seamless communication around the globe through numerous interconnected networks using open protocols and procedures such as TCP/IP that are defined by Internet Standards. The Internet Engineering Task Force (IETF) is a Standards Development Organization (SDO) founded in 1986. IETF achieves its goal *to make the Internet work better* by developing high-quality, relevant technical and engineering documents. This chapter provides an overview of the IETF standardization process and its significance in this research.

3.1 Standardization Process

The stages in the standardization process are formally defined in RFC 2026 [5] which begins with the creation of an Internet draft. It is then submitted and made available in the Internet drafts directory for others to comment on in order to build an evolving working document. The Internet drafts are initial proposals of novel protocols or extensions to existing standards and techniques. This is accomplished in different ways such as defining the need for a new protocol, identifying a potential limitation, and extending the existing internet protocols. The proposal undergoes multiple iterations of comprehensive review and revision produced as part of discussions through open meetings and electronic mailing lists. These reviews and feedback from the relevant working groups ensure the technical accuracy of the draft and improve its quality. After undergoing several revisions when the drafts fulfill and address the comments from the internet community it is considered advanced for an RFC. RFC is a document with both technical specifications and organizational notes for the Internet. Internet drafts are work-in-progress documents that are subject to change or removal at any time. An internet draft will get expire after six months and the authors can replace the older version by updating the draft to a recent version.

3.2 IETF and PoA based authorization

As mentioned above, the first stage of the standardization process begins with the writing of an Internet-Draft (ID), where the idea is proposed. We have started with ID-A targeting the IoTOPS working group, where ID-A is submitted and presented, which specifically focuses on the onboarding or bootstrapping use case using the PoA based authorization. In this case, two steps of delegation are proposed 1) Target network onboarding controller delegating the device owner to onboard trusted devices, and 2) Device owner delegating the trusted device to bootstrap or onboard to the target network.

Later, with the feedback from the IoTOPS group, we wrote ID-B, and ID-C and submitted and presented them to the OAuth working group. ID-B explains a new grant type based on PoA based authorization by adding the principal entity to the OAuth framework. However, the OAuth protocol is not designed for resource-constrained client devices or sensor devices in an IoT environment. ID-C is an informational draft on the comparison of PoA based authorization with other existing authorization standards such as OAuth, Grant Negotiation and Authorization Protocol (GNAP), techniques such as proxy signatures, and extensions such as User Managed Access (UMA). Later, ID-D is written and presented in the ACE working group, where the problems of client registration and AS validation of the ACE framework are explained in connection with PoA based authorization. Integration with the ACE framework enables PoA based authorization to be used in constrained ecosystems along with the use of CBOR instead of JSON web token format. Figure 3.1 illustrates the development of different IDs on PoA based authorization technique. The following are the different internet-drafts on PoA based authorization:

ID-A) Delegation based Device Onboarding using PoA Authorization: The draft proposes an administratively scalable network layer onboarding method using PoA based authorization. This allows the user to generate a PoA for the IoT device and onboard it to the target network temporarily or permanently. This method is based on loose coupling, where the manufacturer is not required to build the device with the specific onboarding credentials. In this approach, the trust between the onboarding controller, the device, and the device owner is implemented by subgranting the ownership credentials using PoAs. The whole onboarding process is designed based on NIST onboarding guidelines.

ID-B) Positioning ofPoA: The draft positions the PoA based authorization with the other relevant authorization standards and delegation techniques such as OAuth, UMA, GNAP, and proxy signature. It explains the unique aspects of PoA-based authorization and outlines its potential to fill the gaps in existing solutions.

ID-C) OAuth-PoA Grant Type: The draft proposes a new grant type for the OAuth protocol based on the PoA based authorization. This grant type adds an additional entity referred to as the Principal to the OAuth protocol flow, with a separation between the principal and the resource owner. The proposed grant type makes OAuth usable in scenarios, where the client is owned by a user entity or principal. This grant

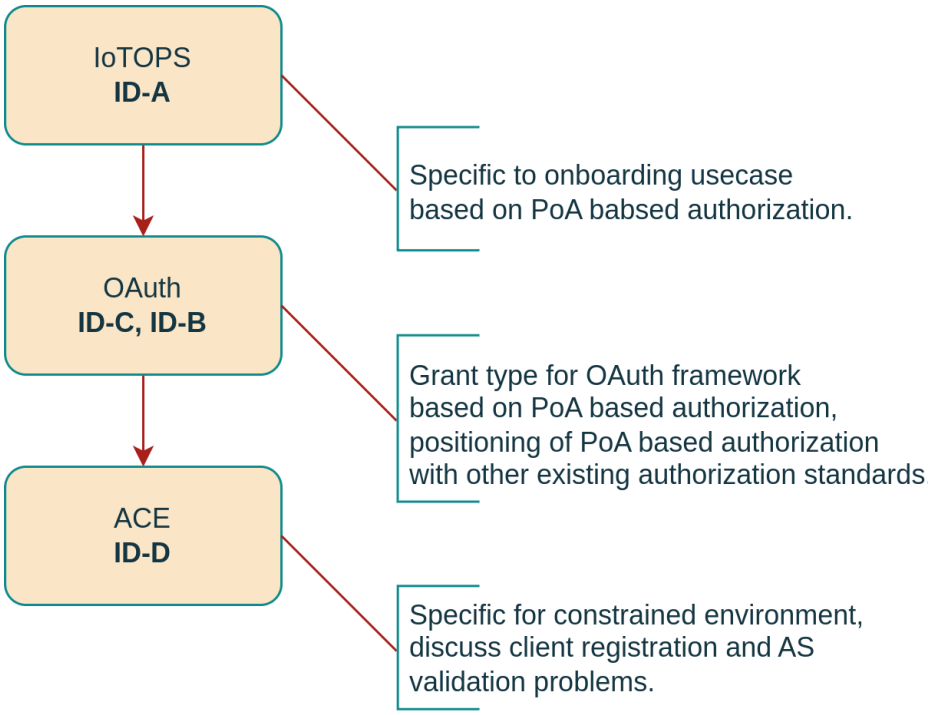


Figure 3.1: ***IETF and PoA based authorization***

type allows the principal to subgrant authority to the client, allowing the client to access resources owned by the resource owner on the principal's behalf via the OAuth authorization server.

ID-D) PoA based Device Registration in ACE framework: This draft proposes an extension to the ACE framework with the Power of Attorney (PoA) based authorization. This is proposed following the identification of a mutual authorization problem between the client and the AS in the ACE framework, which demands secure registration of the client to the AS and a mechanism for the client to validate the AS. The proposed system adds a new entity referred to as the Device Owner of the ACE framework that delegates the client device and provides information (in a PoA) regarding the AS to which the client is intended to communicate.

Chapter 4

Onboarding Concepts

It is an important use case of PoA based authorization and is outlined in this thesis as part of the standardization process. To understand the proposed PoA based device onboarding, this chapter provides details on existing onboarding standards, limitations or gaps within them, and their relation with PoA based onboarding. Here, different existing onboarding standards to bootstrap or provision a device to the target network is defined. The onboarding specifications discussed here are mainly part of IETF and are used by industries today and are undergoing research for improvements as part of the standardization process. The different onboarding techniques and standards discussed in this chapter are FIDO and BRSKI.

4.1 FIDO

FIDO device onboarding [6] is a late binding-based automatic onboarding specification, where the device can be onboarded to any IoT platform by configuring the onboarding credentials at a late phase of the device life cycle. Here, the device is manufactured with a processor containing a Restricted Operating Environment (ROE), a FIDO device onboard application, and a set of device ownership credentials. Specific to the security concerns of the application, the device can also include a microcontroller unit (MCU), and an OS daemon process where the keys are stored in a Trusted Platform Module (TPM).

With the late binding feature, the device does not need to know the target network credentials from the manufacturing phase. Because of this reason, the FIDO onboarding standard uses the rendezvous server to store network credentials from the target IoT platform. The IoT platform sends the network onboarding credentials for the device to the rendezvous server and the device later connects to one or more rendezvous servers until it connects to the target IoT platform. To connect to the rendezvous server, the manufacturer configures the device with instructions (rendezvous info) that are used to query the rendezvous server that is part of the local network and later to the internet-based rendezvous server.

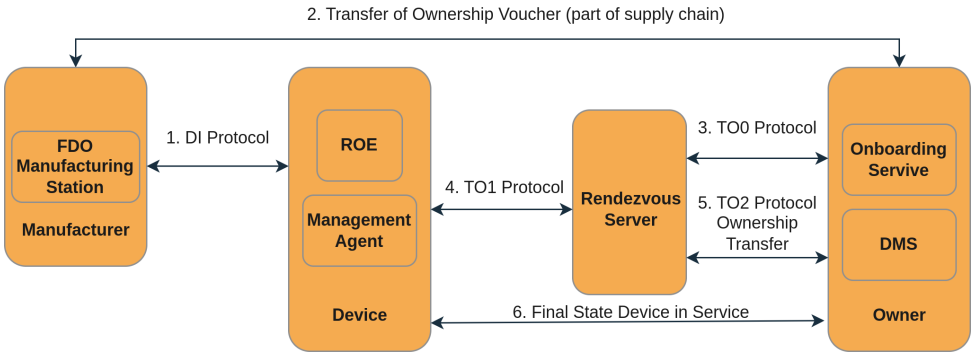


Figure 4.1: ***FIDO device onboarding entities and entity interactions (taken from the specification) [6]***

Another important feature of the FIDO device onboard standard is the transfer of ownership of the device using the ownership voucher. As mentioned earlier, during the manufacturing phase, the device is configured with ownership credentials to identify its current owner. In the later phases, the chain of ownership transfers is tracked using the ownership transfer mechanism until it is provisioned to the IoT platform.

All keys that are used in the FIDO device onboarding or exposed by protocol entities are limited to use for onboarding alone, so different sets of keys are used during device operations. This is to prevent correlation attacks, that are caused by the attacker using the device's appearance to correlate it with a previous onboarding location, system responsibilities, and potential vulnerabilities. This is considered an important security concern even though the newly manufactured device does not include any Personally Identifiable Information (PII). The identification of the device plays an important role in the prevention of correlation attacks, if the keying material identifies uniquely a device, then it should only use the FIDO device onboard once in its lifetime meaning it should be decommissioned or destroyed thereafter or the device only use FIDO device onboard in a closed network. If Intel EPID keys are used, they can be used multiple times because the attestation of the device to the rendezvous server is through a group identity which is mainly useful for the transfer of ownership.

The base profile for each component such as the owner, rendezvous server, and the device in the FIDO onboarding is defined in a way that the device can choose any options and the other two entities are meant to support all the combinations. For example, the device owner and the rendezvous server must support HTTP and HTTPS, and the device is meant to support either one of those. The base profile includes supported protocols, device attestation signatures, ownership voucher cryptography properties (such as hash algorithm, MAC, and signature algorithms), and session cryptography.

The entity interactions between different entities in the FIDO device onboarding are shown in Figure 4.1 The different entities that are part of the FIDO onboarding standard are the manufacturer, device, device ROE, device ROE app, device to man-

ager agent, owner, manager, owner onboarding service, rendezvous server, management service (DMS), and the management agent. The onboarding process starts with the manufacturer building the device with ROE and management agent using the Device Initialize (DI) protocol. DI embeds the device ownership (key pairs) and manufacturing credentials to the device ROE and enables the manufacturer to add a first single input (manufacturer public key) to the ownership voucher.

Later, the manufacturer sends the ownership voucher through the supply chain to the owner of the device or the entity corresponding to the final public key field in the ownership voucher. The device owner entity comprises two different components: 1) the onboarding service and 2) DMS. In the next step, the owner of the device (through the owner onboarding service) identifies itself to the rendezvous server and establishes the mapping of its Globally Unique Identifier (GUID) to its IP address over the Transfer Ownership 0 (TO0) protocol. At the end of the TO0 protocol, the rendezvous server gets the following information:

- The specified interval of time that the owner onboarding server waits for the connection from the Device ROE.
- The device GUID
- The rendezvous blob contains an array of DNS name, IP address, port, protocol to which the device ROE is supposed to connect.

In the later phase of TO1, the device ROE should connect to the rendezvous server within the set time limit or specified interval of time as mentioned above, otherwise rendezvous server forgets the relationship between the GUID, and the rendezvous blob, causing an error to occur. With this connection process the device ROE identifies its owner through the rendezvous server. With a successful rendezvous connection, the device can directly connect to the owner onboarding service using the rendezvous blob over the TO2 protocol to transfer the ownership to the new owner. This process includes the device onboarding service replacing the current device credentials with its own credentials except the device attestation key. Using the new credentials obtained from the owner onboarding service, the device ROE can invoke the correct device to the manager agent (also transfer the credentials) and connect to DMS using ServiceInfo for Ex., key values are exchanged or sent CSR requests. Following this step, DMS provides a certificate in return using the keys provided.

4.1.1 Ownership Voucher

FIDO device onboarding uses the ownership voucher to transfer the ownership of the device from the manufacturer (first owner) to different entities that are part of the supply chain up to the device owner (final owner). Here, the manufacturer builds the device with device credentials such as:

- DCActive: Indicates if the FIDO device onboard is active or not.

- DCProtVer: Indicates the version of the protocol used.
- DCHmacSecret: This contains a secret initialized by the DI protocol based on a random value.
- DCDeviceInfo: It is a text string that indicates the device type.
- GUID: An identification of the device (e.g., a bar code).
- DCRVInfo: Instructions to connect to the right rendezvous server.
- DCPublicKeyHash: Hash of the manufacturer's public key. This should match the hash of the OwnershipVoucher.OVHeader.OVPubKey.

Later the manufacturer adds the first single input to the ownership voucher which is in the format of [GUID, B. PublicKey, Device info]. Here, GUID is public and visible throughout the supply chain and to the device owner, and B.PublicKey is the public key of the next owner in the supply chain (e.g., distributor), and the Device_Info indicates the device information. This collective information is signed by the manufacturer using their private key. When the distributor (with B.PublicKey) receives the ownership voucher, it performs the same process by signing the public key (C.PublicKey) of the next owner in the chain. In the end, the device owner (final owner) receives the ownership voucher with his/her signed public key. The device owner uses their private key to prove his/her connection to the ownership voucher. One method used by the device owner to perform this verification is by signing a nonce using their private key and verifying it using the public key extracted from the ownership voucher.

The contents of the Ownership voucher are:

- OVHeaderTag: OVHeader
- OVHeaderHMac: Hash of the OVHeader values with the DCHmacSecret (secret stored only in the device) in the Device ROE (hmac[DCHmacSecret, OVHeader])
- OVDevCertChain: OVDevCertChainOrNull
- OVEntryArray: OVEntries

The OVHeader includes parameters such as OVProtVersion, OVGuid, RendezvousInfo, OVDeviceInfo, mfg public key, and OVDevCertChainHash. Later, the owner proves his ownership of the device (TO2 protocol) by sending the ownership voucher and signing the message using their public key (the last key in the ownership voucher). At the end, the device verifies the ownership voucher by matching its public key in the device ROE with the A.PublicKey available in the OVHeader (header of the ownership voucher) along with the HMac value. The device verifies the HMac value by recomputing the HMAC using its stored secret in the device ROE. After the verification process, the device ROE and the Owner Onboarding Service start the key exchange protocol.

4.2 Bootstrapping Remote Secure Key Infrastructures (BRSKI)

BRSKI [15] provides a solution for the secure zero-touch bootstrapping of devices. According to BRSKI, bootstrapping of a device refers to the successful deployment of the cryptographic identity of the secure key infrastructure to the device. Here the device is referred to as *pledge* built with unique credentials by the manufacturer. BRSKI defines mutual authentication and authorization between the pledge and the target network domain element which is referred to as the *registrar* using X.509 certificates, TLS connection, and IDevID.

The main components of the BRSKI bootstrapping model are the following:

- Pledge: It is the device built by the manufacturer with a unique identifier (X.509 IDevID) that uniquely identifies the device. IDevID contains two different components Distinguished Name (DN) and the subjectAltName (SAN) that make it unique. To identify the MASA during the onboarding process, the IDevID includes a complete URI with scheme, authority, and path parameters. The complete URI is typically used for diagnostic or experimental purposes, otherwise (for example, in a constrained environment), the URI includes a single parameter authority.

- Join-Proxy: The entity that is present between the pledge and the registrar to make the HTTPS connection possible between them.

- Domain Registrar: Commonly called registrar aka JRC, which is the element of the domain network, and presents in between the pledge and the Manufacturer Authorized Signing Authority (MASA).

- MASA: Manufacturer service entity that accepts the request for vouchers from the registrar and provides signed vouchers [23] for ownership tracking and device audit log data to the registrar.

The communications between the above-mentioned entities in the BRSKI onboarding to onboard the pledge is shown in Figure 4.2.

The pledge discovers the join proxy using a local service auto-discovery Generic Autonomic Signaling Protocol (GRASP) or Multicast DNS (mDNS), that connects the pledge with the registrar. The join proxy forwards the messages from the pledge to the registrar. The communication between these two entities is over an IPv6 link-local address. To discover the proxy, the pledge must have a local address using IPv6 methods, preferably a temporary address, to limit pervasive monitoring. Once connected to the proxy, the proxy forwards the messages to the registrar from the pledge. For this, the registrar should announce itself using the GRASP_M_FLOOD messages including the port number to join.

The pledge identifies itself to the registrar via the join proxy using credentials such as serial number, and IDevID certificate over a TLS handshake through the communication

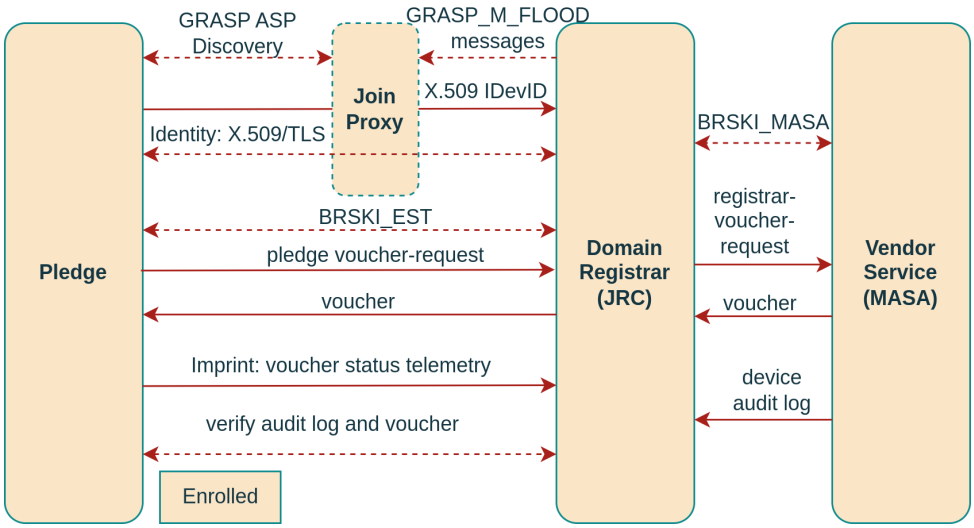


Figure 4.2: ***BRSKI - Protocol Flow Diagram (taken from the specification [15]***

channel BRSKI-EST. The next step is the request join step, where the pledge sends a request for the voucher (pledge voucher-request) by signing the request with its IDevID to the registrar along with other fields. These fields in the voucher-request include the following:

- created on: Recommended if the pledge has a real-time clock, otherwise omitted.
- Nonce: A strong random number value that is different for each bootstrap.
- Assertion: Indicates the support for the mechanisms recommended by BRSKI and sets to the value *proximity*.
- Proximity_registrar_cert: Indicates the certificate of the registrar.
- Serial number: For sanity check only.

When the registrar receives the request, it can decide whether to accept or reject the device by contacting the vendor service (or MASA) by making a registrar voucher-request signed by the registrar key pair. If the request is successful, the registrar forwards the pledge credentials including the IDevID to the MASA. The communication channel between the registrar and the MASA is referred to as BRSKI-MASA. If the request is successful, the MASA sends a voucher to the registrar with nonce if provided. There are nonce-less bootstrapping, which is useful in the case of offline pledges, which cannot provide fresh voucher request to MASA.

In the next step, the registrar forwards the voucher to the pledge to enter the imprint stage. In this stage, the pledge verifies the voucher generated by the MASA and completes the authentication of the registrar. The enroll stage starts with an authenticated TLS connection between the pledge and the registrar to obtain a domain certificate from the registrar using Enrollment Over Secure Transport (EST) protocol [16].

4.2.1 Voucher Artifact

The voucher artifact is used to securely assign the pledge to an owner, by signing the artifact directly or indirectly by the manufacturer (MASA). The format of the voucher artifact is JSON, and the signature is signed using the Cryptographic Message Syntax (CMS) structure. The main components or parameters part of the voucher artifact are the following:

- Created-on: Indicates the date and time on which the voucher is created by the MASA.
- Expires-on: Indicates the date and time on which the voucher expires.
- Assertion: Indicates that the MASA positively verifies the ownership of the pledge.
- Serial number: Uniquely identifies the hardware or the pledge, and the pledge must ensure that this value matches its serial number during the processing of the voucher.
- IDevID issuer: The authority key identifier, which must be verified by the pledge during voucher processing, if the IDevID issuer is included, it is not mandatory.
- Pinned-domain-cert: An x.509 certificate used by Pledge to verify the domain certificate.
- Domain-cert-revocation-checks: The processing instructions to the pledge to verify the revocation status of the pledge domain certificate.
- Nonce: Random generated value, that is used to protect from replay attacks.
- Last-renewal date: The last date of renewal of the voucher by the MASA.

4.3 Analysis: FIDO and BRSKI

The main properties of FIDO device onboarding are the late binding and the ownership voucher. With the late binding, the manufacturer can increase the scalability by designing devices not specific to a target network. The device is populated with the network onboarding at a late stage of the onboarding process with the late binding feature. Here, the manufacturer sends the device through the supply chain with many different entities and finally, the device owner receives the device. To track the identity of each entity that

is part of the supply chain, FIDO onboarding uses the ownership tracking mechanism using the ownership voucher.

Both these onboarding techniques are used for specific use cases relevant to the application scenario. FIDO includes the entities such as the manufacturer, device owner, and the rendezvous server. BRSKI includes different entities such as the pledge, registrar, MASA, and a join proxy in between the pledge and the registrar. The pledge in BRSKI is the same as the device in FIDO, the registrar can be considered as the device owner in FIDO, and both these components are considered as part of the target network. MASA is the manufacturer service in BRSKI, which is not directly connected with the pledge during the onboarding process.

BRSKI solves the authentication and authorization problem from the registrar (part of owner onboarding) to the pledge (device) using the X.509 certificates, TLS, and the IDevID. Similarly, the authentication and authorization from the pledge to the registrar using the voucher artifact and the MASA. In the case of FIDO onboarding, the authentication and authorization from the registrar or device owner is using the device credentials such as Hmac secret, device hash, etc. that are part of the device credentials. Similarly, the authentication and authorization from the device to the device owner onboarding using the ownership voucher. In the case of FIDO, it doesn't use the MASA as in FIDO, to verify the voucher for ownership transfer. Instead, use the rendezvous server to connect the device with the right owner.

Chapter 5

Use cases

PoA based authorization is a generic authorization technique that can be applied to a vast number of use cases including web applications, and constrained and non-constrained use case scenarios. The use cases where the PoA based authorization is implemented, and performance analyzed are device onboarding and mining station use cases. These two use cases fall in the category of non-constrained environment use cases, where the agent or client device is expected to have adequate computational power, memory, and other resources to engage in the whole authorization process.

5.1 Basic Use cases

5.1.1 Mining Station Use case

The contractors or subcontractors in a mining station are often assigned to multiple tasks and possess multiple smart devices. These devices are mostly CPS devices with enough computing power and memory (for example, smart trucks). Here, the subcontractor can delegate or subgrant their authority to their trusted devices to enable the devices to work/act on behalf of the subcontractor which can increase overall productivity. In this case, with PoA based authorization, the contractor can delegate his/her authority by generating a PoA to their trusted device (mining truck) that allows the smart truck to collect mining-related data on behalf of the subcontractor from the resource owner (mining station). This is also useful when there are multiple smart trucks that can form a chain of trust between the subcontractor and the mining station. In this case, an assumption made is the established mutual connection between the subcontractor and the mining station.

5.1.2 Onboarding Use case

Another important use case where PoA based authorization can be used is the zero-touch device onboarding. In this case, the manufacturer builds the device and transfers

the device to the device owner through a supply chain. The important concepts in device onboarding are the transfer of ownership of the device during its life cycle and the bootstrapping process. The main entities part of this use case are the manufacturer, integrators part of the supply chain, device, device owner, onboarding controller, and the target network. The device onboarding with PoA based authorization includes the use of PoAs and is a delegation based onboarding approach especially when it comes to the transfer of ownership. Similar to other internet standards or specifications, the proposed solution features late binding, where the device obtains the network onboarding credentials in a late stage of its life cycle. Chapter 4 defines different existing onboarding standards and specifications relevant to the industry.

5.2 IETF-ACE Use Cases

In addition to the above-mentioned use cases, PoA based authorization can be used in constrained environments such as an IoT network for sensors and devices with limited computing, storage, and transmission capacities, battery-powered, and mostly without a user interface. Integration of PoA based authorization with the ACE framework, specifically with the help of the ACE authorization server along with the CBOR token format makes the PoA based authorization to be used in constrained application scenarios. With this approach, the user (principal) can delegate their trusted client (agent) device to access resources (such as sensor data, and actuators) from the resource owner via the ACE authorization framework on behalf of the user in an IoT ecosystem.

RFC 7744 [18] defines different representative use cases for authentication and authorization in constrained application environments that emerge during the life-cycle of a constrained device. Out of many listed use cases, specific use cases within specific application environments are selected and defined in this thesis. This chapter defines authorization solutions based on PoA based authorization and ACE framework to address problems in selected specific use cases referred to as U1.x and U2.x. Different application environments that are defined in this chapter are container monitoring, home automation, personal health monitoring, building automation, smart metering, sports and entertainment, and Industrial Control Systems (ICS).

5.2.1 Cargo Container Monitoring

Intelligent containers are used to transport goods by continuously monitoring the temperature, humidity, and gas content during transit and storage. The different parties involved in this application environment are the fruit vendor, the container owner, the transloading company, and the private customers. Here, the fruit vendor starts the supply chain by communicating with the container owner to keep the goods in optimal conditions using sensor data and climate control systems.

Selected problems in this use case that can be addressed using PoA based authorization are U1.1, U1.7, and U1.8.

U1.1: *Fruit vendors and container owners want to grant different authorizations for their resources and/or endpoints to different parties.*

In this case, the fruit vendors and container owners are required to grant authorizations to different parties in the whole supply chain and with different levels of privileges. Here, PoA based authorization can be used by the vendors and the container owners to delegate or subgrant their authority or power to their trusted parties in the form of a PoA. This enables them to access protected resources on behalf of the fruit vendor or the container owner. In this case, for example, fruit vendors can grant permissions to the transloading personnel by delegating the transloading personnel to access information on behalf of the fruit vendor using PoA based authorization. Here, the vendor can generate a PoA with appropriate credentials such as access only to transloading information and the expiration time set to expire right after the transloading process.

U1.7: *The container owner and the fruit vendor may not be present at the time of access and cannot manually intervene in the authorization process.*

This use case problem requires the container owner and the fruit vendor to authorize the other parties even if they are offline. With the self-contained nature of PoAs in the PoA based authorization, the fruit vendor or the container owner is not required to be online during the time of access in the whole authorization process. After the PoA generation process and sending the PoA to different parties, the different parties are not required to approach the fruit vendor or the container owner to access the resources because of the self-contained property of the generated PoA. In this case, we assume that the fruit vendor or the container owner has a pre-established trust relation with the third-party resource owner.

U1.8: *The fruit vendor, container owner, and transloading company want to grant temporary access permissions to a party, in order to avoid giving permanent access to parties that are no longer involved in processing the bananas.*

In this case, the "eat" parameter of the PoA is used to set an expiration time for the PoA, which helps to avoid stale PoAs. The fruit vendor, container owner, and the transloading company can set the expiration time and date that determines the temporary access period for the other parties.

5.2.2 Home Automation

Home automation is an IoT application that involves multiple parties such as home residents, friends, relatives, visitors, etc. This demands a robust and optimal authorization technique to control access to different connected devices in the home such as heating, ventilation, entertainment, security systems, etc. The different application environments part of home automation are Controlling the smart home infrastructure, seamless authorization, remotely letting in a visitor, and selling the house. Considering Alice and Bob own the house and control the access to their automated devices in the house. This use case defines different problems that are caused when Alice or Bob needs to transfer or grant permissions to some other users (e.g., visitors) or add a new device to their home network, and they also demand the security of their property from malicious users.

Selected problems in this use case that can be addressed using PoA based authorization are U2.1 and U2.4.

U2.1: *A homeowner (Alice and Bob in the example above) wants to spontaneously provision authorization means to visitors.*

In this case, Alice and Bob are required to authorize the visitor by granting limited privileges to the visitor to access specific devices or functionalities in the home. Here in this use case, Alice and Bob are considered the principals in the PoA based authorization context. Here, the authorization process begins with Alice or Bob generating the PoA by including different parameters that determine the level of permissions or authority of the visitor. This includes a credentials parameter that specifies the different credentials provided to the visitor, identification of the parties, keys, or identification information of the target resources that can be accessed by the visitor (such as access to door locks, light bulbs, etc.). The starting time and expiration time of the access should also be added to the PoA by Alice or Bob to provide temporary access instead of permanent access. In the end, Alice and Bob can use their digital signature to sign the PoA to prevent different security concerns such as spoofing, tampering, repudiation, etc.

U2.4: *The homeowners want to grant access permissions to someone during a specified time frame.* This is a case similar to U2.1, where authorization is provided to someone or visitors for a period of time. This problem can be specific to users such as repairmen who require permission to a specific device for a restricted time frame. Here, in this case, the house owner can generate a PoA for the repair man with limited privileges mentioning the destination device name and identification so that he/she can only access the particular device/s. Similar to U2.1, the homeowner must specify the iat and eat parameters in the PoA that determine its validity.

In RFC 9200 [19], it is mentioned that the home automation use case can be solved using the authorization code grant type or client credentials grant type of OAuth protocol. Authorization code type is a good solution, however, this is meant to be used with web applications other than constrained devices. The client credentials grant type is the preferred grant type to use in this scenario because, in this grant type, the client credentials are considered as access tokens, which reduces the communication overhead and is apt for constrained devices. However, the client credentials grant type is used in scenarios where the client is the one who owns/controls the resources, which means the client accesses resources on its own behalf (both resource owner and client are the same in this case). This is not the situation in all the above-mentioned cases of home automation applications. For example, the homeowner (Alice and Bob) grants privileges to the guest/visitor for a specific period of time, which requires a delegation process, where the visitor is accessing resources owned by another party. This is a use case where PoA based authorization (as mentioned in U2), can be deployed by introducing the principal entity and the delegation or sub-granting process between the principal and client entities in the authorization process.

Chapter 6

Contributions

The goal of this thesis is to develop a secure authorization technique that resolves the challenges defined in the introduction of this thesis. To address these challenges and answer the research questions, this thesis proposes the Digital Power of Attorney (PoA) based authorization technique, inspired by the traditional power of attorneys. Digital PoA based authorization technique can be used to allow IoT or CPS devices to access protected resources and perform tasks on behalf of the user for a predefined time period. The different entities or roles part of PoA based authorization are 1) the principal who generates the PoA and delegates the device/agent to work on behalf of the principal, 2) the Agent which is the client device that receives the PoA from the principal to act on behalf of the principal, 3) Resource owner/server is the third-party entity that verifies the PoA and provides requested resources to the agent, 4) Signatory registry (not mandatory), is database storage that stores related metadata for the authorization process.

With this authorization technique, the principal who is required to assign his/her tasks to their trusted agent can generate a PoA for the agent. This enables the transfer of authority or privileges (limited) from the principal to the agent, which allows the agent to act/work on behalf of the principal. The scope of the privileges shared or access control is determined by the contents of the PoA created and signed by the principal. The self-contained format of the PoA makes it time-limited and usable in situations where the principal is offline. The PoA typically contains the following parameters: principal public key, principal name, resource owner ID, agent public key, agent name, signing algorithm, transferable, iat (Issued at), eat (Expires at), and metadata. PoA is a key component of the proposed authorization technique, which is of self-contained JSON or CBOR format.

This thesis proposes two different ways of PoA interpretation: 1) Integrating the PoA-based authorization with a centralized authorization server such as OAuth or ACE, where most of the PoA execution functions are handled. 2) Interpretation using an open-source library/image that can be downloaded and executed by all entities participating in the authorization process. The integrated authorization model contains entities such

as principal, agent/client, authorization server, resource owner, and resource server. The principal generates the PoA and sends it to the agent (client device) so that the agent can sign on behalf of the principal; in this case, the agent does not require a separate account for communication. The agent/client receives the PoA and sends a request along with the PoA to the authorization server. The authorization server registers the client and sends back a client ID. To obtain the authorization grant, the client ID and PoA are sent to the resource owner. When the client receives the authorization grant from the resource owner, it can send a request for the access token to the authorization server. The authorization server generates and sends the access token to the client, which the client uses to obtain requested resources from the resource owner. The interpretation using the library is implemented using the python library poa_lib which can be downloaded and executed by the entities participating in the authorization process. Different primary functions part of the PoA library are PoA generation, decoding, and verification.

This thesis defines different security considerations for the PoA based authorization technique. As part of the security evaluation of the proposed authorization technique, different possible threats are analyzed, and mitigation strategies are proposed. The system is tested by exploiting the application using penetration testing tools on the basis of specific attack scenarios. This contributes to the best practices and mitigation strategies with the PoA based authorization.

An important contribution of this thesis is the internet-drafts part of the IETF standardization process as defined in Chapter 3. This includes contributions to the OAuth protocol as a new grant type based on PoA based authorization, client registration, and AS validation problems in the ACE framework, which are considered part of the PoA interpretation methods. Other standardization works are in the automated zero-touch IoT device onboarding or bootstrapping.

Paper A

Title	A Model for Signatories in Cyber-Physical Systems
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Published in 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2020.
DOI	*https://doi.org/10.1109/ETFA46521.2020.9212081*
Summary	This manuscript proposes a conceptual architecture for the PoA based authorization model. The paper also defines other security concepts that can be used in conjunction with the PoA-based authorization technique, such as Certificate Authority (CA) and signatory registry for PoA management.
Personal Contribution	The paper's draft was written by me, and the findings and observations were discussed with Olov Schelén and Ulf Bodin.
Relevance	This paper address research question two (RQ2).

Paper B

Title	Survey on delegated and self-contained authorization techniques in CPS and IoT
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Published in the journal IEEE Access, 2021
DOI	*https://doi.org/10.1109/ACCESS.2021.3093327*
Summary	This paper provides an overview of authorization techniques in Cyber-Physical Systems (CPS) and the Internet of Things (IoT). The survey is done in three different dimensions: access control models, subgranting models, and authorization governance. The paper focuses on authorization subgranting techniques such as delegation-based authorization and self-contained PoA-based authorization.
Personal Contribution	I conducted a literature review on the topic, wrote a draft of the paper, and discussed the findings and observations with Olov Schelén and Ulf Bodin.
Relevance	This paper address research question one (RQ1).

Paper C

Title	Multi-level Sub-granting by Power of Attorney and OAuth
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Published in the journal IEEE IoT, 2023.
DOI	*https://doi.org/10.1109/JIOT.2023.3265407*
Summary	The paper demonstrates the proof of concept for a PoA-based authorization technique. This paper analyzes and compares Power of Attorney (PoA), proxy signature by warrant, and OAuth to identify the strengths and challenges of each of these authorization techniques. Based on the comparison, a new grant type for OAuth based on the PoA based authorization and inspired by the concept of the proxy signature by warrant is proposed. The proposed OAuth extension is applied based on an industrial use case scenario; a mining station use case. This supports subgranting on multiple levels where resource owners bring in authorized contractors (principals) who can in turn authorize the devices (agents). With this approach, the contractor brings in several devices without incurring management overhead to the resource owner.
Personal Contribution	I worked on the designing of the architecture, methodology part, and the implementation of the proof of concept, analyzed and evaluated the performance of the software application, and wrote the first draft of the paper. The findings and observations were discussed with Olov Schelén and Ulf Bodin.
Relevance	This paper addresses research question three (RQ3).

Paper D

Title	Device Onboarding in Eclipse Arrowhead Using Power of Attorney Based Authorization
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, Ulf Bodin, and Nicklas Nyström.
Status	Published in IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2022.
DOI:	*https://doi.org/10.1109/CAMAD55695.2022.9966899*
Summary	This paper proposes an onboarding technique based on the PoA based authorization technique in the Arrowhead frameworks. The Eclipse Arrowhead framework, which provides a platform for industrial automation, requires reliable, flexible, and secure device onboarding to local clouds. This automatic onboarding process is useful in situations with the dynamic addition of devices (e.g., from subcontractors entering a workplace). With this approach, the IoT device is onboarded to the target arrowhead local cloud by obtaining the network onboarding credentials through the network onboarding controller. Different security concepts used in this work include the implementation of a secure gateway between the device and the local cloud, mutual TLS connection establishment, and the use of X.509 certificates along with PoAs.
Personal Contribution	I along with Olov Schelén and Ulf Bodin defined the idea of using PoA based authorization for the device onboarding issue in the eclipse arrowhead framework. I have Implemented the onboarding procedure on the arrowhead framework and evaluated the performance of the application along with Nicklas Nyström. I conducted a literature review on the topic, wrote the first draft of the paper, and discussed the findings and observations with Olov Schelén and Ulf Bodin.
Relevance	This paper address research question two (RQ2).

Paper E

Title	Token Interpretation and Security Evaluation of Power of Attorney based Authorization Technique
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Submitted in the journal IEEE IoT, 2023
Summary	The manuscript proposes two different PoA interpretation methods: using a centralized server (ACE authorization server), and an open-source library (PoA lib) that can be downloaded by different entities that are part of the authorization system. The PoA library provides two main functions, which are the generation of the PoAs and its decoding and validation. This work extends the use of PoA based authorization to constrained environments with the help of the ACE framework. Another important contribution of this manuscript is the security evaluation of the PoA based authorization. The security evaluation includes threat analysis using Microsoft STRIDE, risk assessment using Microsoft DREAD, and exploitation of the system using pen-testing tools based on different attack scenarios that are considered relevant to the proposed system.
Personal Contribution	I worked on the methodology part and the implementation of the proof of concept, poa-library, and security evaluation, and wrote the first draft of the paper. The findings and observations were discussed with Olov Schelén and Ulf Bodin.
Relevance	This paper address research question two (RQ2).

ID-A

Title	PoA based IoT Device Onboarding
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Presented to and Submitted in IoTops working group, IETF.
Summary	The ID proposes a bootstrapping or onboarding technique using PoA based authorization based on delegations. This onboarding technique includes primary features such as late binding of the onboarding credentials, transfer of ownership voucher, and mutual authorization between the device owner and the onboarding controller.
Personal Contribution	This ID is developed through discussions on onboarding and PoA based authorization with Olov Schelén and Ulf Bodin. I wrote the first draft of the ID. Feedback from the working group is used to update the draft to the next versions.
Relevance	This ID address research question two (RQ2).

ID-B

Title	Positioning of PoA based Authorization
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Submitted as an information draft, IETF.
Summary	The ID positions the PoA based authorization with the other relevant authorization standards such as OAuth, UMA, GNAP, and proxy signature. It explains the unique aspects of PoA-based authorization and outlines its potential to fill the gaps in existing solutions.
Personal Contribution	The ID is developed through discussions on different existing IETF authorization standards and PoA based authorization with Olov Schelén and Ulf Bodin. I wrote the first draft of the ID.
Relevance	This ID address research question two and three (RQ1 and RQ3).

ID-C

Title	OAuth-PoA Grant Type
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Presented to and Submitted in OAuth working group, IETF.
Summary	The ID proposes a new grant type based on PoA based authorization to OAuth protocol. The proposed grant type makes OAuth usable in scenarios, where the client is owned by a user entity or principal.
Personal Contribution	This ID is developed through discussions on OAuth, OAuth extensions, and PoA based authorization with Olov Schelén and Ulf Bodin. I wrote the first draft of the ID.
Relevance	This ID address research question two (RQ3).

ID-D

Title	PoA based Device Registration in ACE framework
Authors	Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin
Status	Presented to and Submitted in ACE working group, IETF.
Summary	The ID proposes an extension to the ACE framework with the Power of Attorney (PoA) based authorization. Discuss the AS validation and client registration issues in the ACE framework and propose an early-stage solution using the notion of delegations.
Personal Contribution	This ID is developed through discussions on the ACE framework and PoA based authorization with Olov Schelén and Ulf Bodin. I wrote the first draft of the ID. The feedback from the working group is used to update the draft to the next versions.
Relevance	This ID address research question three (RQ3).

Chapter 7

Conclusions

This thesis proposes the digital PoA based authorization that enables the users to subgrant their authority to their trusted smart devices. This allows the devices to act/work on behalf of the user, even if the user is not available online. This thesis started with the identification of different challenges, which subsequently led to the formation of three research questions. The proposed authorization technique is defined by the exploration of these research questions, and addressing them through academic papers and IETF internet drafts.

RQ1 *Which existing authorization techniques allow the users to subgrant their authority to their trusted CPS/IoT devices to make them work/act on behalf of the user?*

Authorization techniques allow the users to access target resources based on certain access control rules and regulations. Delegation-based authorization techniques enable the primary users to delegate another application or user, by providing a set of privileges. One example that is commonly used with web applications is the OAuth protocol. With the OAuth protocol, users do not have to share their credentials (such as usernames and passwords) to allow third-party web applications to use the user data. Instead, the user can issue access tokens to third-party web applications that enable them to access the protected user resources on behalf of the user. Other standards and protocols similar to or extended from OAuth are GNAP and UMA respectively. However, the use of these standards is mostly suitable for web applications or non-constrained devices. Another interesting work on delegation-based authorization is proxy signatures with the warrant, which is based on cryptographic algorithms that enable the primary user to delegate the secondary user using a warrant. In addition to this, there are other academic papers published on authorization techniques in general for IoT and CPS.

RQ2 *How to build a subgranting-based authorization framework that allows the user to transfer their authority to their trusted devices in a self-contained manner, and enables them to work/act on behalf of the user even if they are offline? What are the primary*

security concerns that must be addressed during this authorization process?

This thesis proposes PoA based authorization technique that allows CPS and IoT devices (agents) to act/work on behalf of the user (principal). The different entities involved in this model are the principal, agent, resource owner, or resource server, and the signatory registry (optional). The communication between the different entities is through the use of digital PoAs, which are self-contained documents or tokens, that allow the principal to provide his/her authority to the agent in a decentralized way (without using a centralized authorization server), allowing the agent to sign on behalf of the principal. The expiration time defined by the principal makes the agent device only use the PoA until the expiration time, otherwise, it will be considered as an invalid PoA, to remove all the stale PoAs from the system.

The self-contained nature of PoAs is an important feature that allows them to be used for authorization purposes on their own. PoA contains all of the sufficient information required for the delegation and authorization. Two parameters are used to identify the principal who generates the PoA: the principal public key and the principal name. Similarly, the agent identification information, such as the agent's public key and agent name is also included in the PoA. The identification of the resource owner is also included in the PoA as the resource owner ID parameter. Cryptographic techniques such as digital signatures are used to protect the PoA, where the principal signs the PoA with his/her private key. The parameter signing algorithm is used to indicate the type of digital signature (for eg: SHA225) that will be used for the signing. PoA may or may not be transferred by including it in another PoA, i.e., it is signed in several delegation steps. The parameter transferable indicates the number of PoA transfers; by default it is set to 0, indicating that the PoA is not transferable. The expiration time of the PoA is defined by the parameters iat (Issued at) and eat (Expires at). Application-specific information with other sub-parameters is added to the PoA using the metadata parameter.

PoA based authorization is designed considering the security issues that may occur during the authorization process. This includes the use of digital signatures, hashing, and encryption of the PoA in the case of sensitive contents, depending on the application use case. In this thesis, the security of the PoA based authorization is tested using threat modeling and exploitation steps as part of the penetration testing to identify potential threats and vulnerabilities in the system.

RQ3 *How to standardize the proposed authorization technique by integrating it with the existing delegation-based authorization standards to enhance the scope of authorization, ensuring compatibility and interoperability?*

The PoA based authorization technique is designed and implemented by examining other industry-related delegation-based authorization standards that are part of IETF. The OAuth protocol is extended with the PoA based authorization by proposing a new grant type for the OAuth protocol. This enhances the scope bother the authorization techniques. The similarities and differences between the proposed work and the other existing standards that are similar or extended from OAuth standards such as UMA and

GNAP are outlined in this thesis by positioning the PoA with other standards.

The main application area of PoA based authorization is in the device onboarding or bootstrapping. This thesis analyses prominent onboarding standards part of IETF such as FIDO and BRSKI to understand the contributions, limitations, and further improvements.

The ACE framework, which is built on top of the OAuth protocol, is an authorization and authentication protocol that is suitable for use in a constrained environment. With the addition of the principal entity from the PoA based authorization, a notion of delegation is added to the ACE framework. This thesis defines the integration of both techniques along with the client registration and AS validation problems in the ACE framework. This makes PoA based authorization suitable for constrained devices, especially with the use of CBOR format instead of JSON for PoAs. The IETF IDs mentioned in this thesis part of the standardization process are ongoing research and are frequently updated with new findings and improvements.

Chapter 8

Findings, Discussion, and Future Work

The main contribution of this thesis is the digital *PoA based authorization technique*, which enables the user (principal) to sub-grant or delegate their authority to a trusted device (agent) in the form of a PoA. This technique allows the device to act/work on behalf of the principal for a limited time period, even if the principal is not available online.

The scope of this thesis is *Authorization* techniques in the domain of IoT and CPS. With the literature study, the extensive list of authorization techniques is narrowed down to delegation-based authorization techniques in IoT and CPS. The literature study is conducted by classifying the existing works based on three dimensions: access control models, sub-granting models, and authorization governance. The literature study is connected to RQ1 and finds that the different existing delegation-based authorization models surveyed are mostly directly or indirectly based on the OAuth standard. There are certain academic works that are different from OAuth, however, there is missing information on the semantics and syntax of these authorization models.

With this finding, the main focus of this research turned to IETF standards in the area of delegation-based authorization. From the comprehensive analysis of RFCs and internet drafts published in this area, this thesis finds the relevance of the OAuth standard in the context of PoA based authorization. Even though both these are delegation-based authorization techniques, the problems they are addressing are different. In the case of OAuth, the client requests the resource owned by the resource owner, which makes the resource owner generate a token (via the authorization server) for the client, that allows the client to access the resources on behalf of the resource owner. In the case of PoA base authorization, there is another entity principal which is different from the resource owner, that generates a token (PoA) by itself and sends it to the trusted agent (client) allowing the agent to access the resources owner by the resource owner (third-party) on behalf of the principal.

Considering the above-mentioned findings, a new grant type for the OAuth protocol

is proposed that can provide a new dimension of authorization using OAuth with the addition of the principal entity which is different from the resource owner. For PoA based authorization, this integration with OAuth is a solution for the PoA interpretation challenge. This thesis positions the OAuth-PoA integration with other existing OAuth extensions and similar standards such as UMA and GNAP.

However, the use of PoA based authorization for constrained devices was challenging and required more research and improvements. With the study of the ACE framework with CBOR, CoAP, OAuth, and COSE as its foundations, it is found that PoA based authorization with ACE components can be made suitable for its use in a constrained environment. The ACE framework, which is built as an extension to OAuth to make it usable in the IoT environment, made it easier to correlate it with the PoA based authorization. In the ACE framework, the main research objectives of PoA based authorization are the AS validation and client registration issues that can be related to the bootstrapping problem of smart devices. The integration of PoA based authorization with the ACE framework is considered as another solution for the PoA interpretation challenge. Considering, device onboarding or bootstrapping as a main use case of PoA based authorization, this thesis analyses the existing industry standards that are part of IETF such as FIDO and BRSKI to discover the unique features, challenges, and ongoing research. The main challenge in the device onboarding that is considered in the scope of PoA based onboarding as far as now are the transfer of ownership and the manufacturer or device owner not being online during the bootstrapping process.

As mentioned above, the two different solutions of PoA interpretation are with the use of a centralized authorization server; integrating with either OAuth or ACE framework. Another solution that addresses this challenge is the implementation of the PoA library that can be downloaded by every entity that is part of the authorization system. The security evaluation of the PoA based authorization along with the PoA library is performed using threat modeling, risk assessment, and the exploitation of vulnerabilities based on different attack scenarios. The main finding of this experiment is to use authentication mechanisms to prevent most of the threats discovered. Most of the threats discovered based on STRIDE categories such as spoofing and tampering are considered not in scope for PoA based authorization because of the use of digital signatures. However, a large number of PoA requests can be used to perform denial-of-service attacks by forwarding them to the principal. Strong encryption standards are recommended in case of sensitive content in the PoA to prevent confidentiality-related threats.

The future steps or ongoing research with PoA based authorization are in the areas of OAuth-PoA integration, AS validation, and client registration in the ACE framework connecting with the bootstrapping process. The following points provide specifics about this thesis's future work:

- Future work on PoA based device onboarding/bootstrapping.

  PoA based authorization can be used to address the bootstrapping problem by proposing the use of delegations to implement the ownership vouchers. With current techniques, the intermediate parties such as integrators between the manufacturer and the device owner are considered device owners during the life cycle of

the device. An open research question will be, how to delegate the intermediate parties with limited privileges instead of making them device owners using PoA-based authorization. Similar to other existing works, with PoA-based onboarding, the manufacturer does not have to be online during the bootstrapping stage, which can add the offline property to the onboarding process.

- Future work on OAuth-PoA grant type.

  More discussions with the working group are needed to move forward with the OAuth-PoA integration. This requires research on the current objectives and problems that are in the scope of the OAuth protocol to figure out how the addition of the principal entity would be useful.

- Future work on PoA-ACE.

  Implementation of PoAs in the CBOR format over CoAP in the context of the ACE framework. This is a starting point to address the AS validation and client registration problems in the ACE framework with PoA based authorization. The current implementation of PoAs is in JSON format, and with this future work, the format changes to CBOR which makes PoAs suitable in constrained environments.

References

Bibliography

[1] Ronald E Anderson. Acm code of ethics and professional conduct. *Communications of the ACM*, 35(5):94–99, 1992.

[2] Rabeea Basir, Saad Qaisar, Mudassar Ali, Monther Aldwairi, Muhammad Ikram Ashraf, Aamir Mahmood, and Mikael Gidlund. Fog computing enabling industrial internet of things: State-of-the-art and research challenges. *Sensors*, 19(21):4807, 2019.

[3] Mardiana binti Mohamad Noor and Wan Haslina Hassan. Current research on internet of things (iot) security: A survey. *Computer Networks*, 148:283–294, 2019.

[4] Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. Secure communication for smart iot objects: Protocol stacks, use cases and practical examples. In *2012 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM)*, pages 1–7. IEEE, 2012.

[5] Scott Bradner. Rfc2026: The internet standards process–revision 3, 1996.

[6] Geoffrey Cooper, Brad Behm, Ankur Chakraborty, Hanu Kommalapati, Giri Mandyam, Hannes Tschofenig ARM, and Witali Bartsch. Fido device onboard specification 1.1. *FIDO Device Onboard Specification*, 1, 2021.

[7] National Research Council et al. *Academic careers for experimental computer scientists and engineers*. National Academies Press, 1994.

[8] Mohammed El-hajj, Maroun Chamoun, Ahmad Fadlallah, and Ahmed Serhrouchni. Taxonomy of authentication techniques in internet of things (iot). In *2017 IEEE 15th Student Conference on Research and Development (SCOReD)*, pages 67–71. IEEE, 2017.

[9] Don Gotterbarn, Keith Miller, and Simon Rogerson. Software engineering code of ethics. *Communications of the ACM*, 40(11):110–118, 1997.

[10] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future generation computer systems*, 29(7):1645–1660, 2013.

[11] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. Cyber-physical systems security a survey. *IEEE Internet of Things Journal*, 4(6):1802–1831, 2017.

[12] Madhusanka Liyanage, An Braeken, Pardeep Kumar, and Mika Ylianttila. *IoT security: Advances in authentication*. John Wiley & Sons, 2020.

[13] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341, 2015.

[14] Nangialay Nangial and SeyedAkbar Mostafavi. Internet of things: Architecture, security issues and solutions.

[15] Max Pritikin, Michael Richardson, Toerless Eckert, Michael H. Behringer, and Kent Watsen. Bootstrapping Remote Secure Key Infrastructure (BRSKI). RFC 8995, May 2021.

[16] Max Pritikin, Peter E. Yee, and Dan Harkins. Enrollment over Secure Transport. RFC 7030, October 2013.

[17] Moritz Schneider, Sinisa Matetic, Ari Juels, Andrew Miller, and Srdjan Capkun. Secure brokered delegation through delegatee. *IEEE Security & Privacy*, 17(4):43–52, 2019.

[18] Ludwig Seitz, Stefanie Gerdes, Göran Selander, Mehdi Mani, and Sandeep Kumar. Use Cases for Authentication and Authorization in Constrained Environments. RFC 7744, January 2016.

[19] Ludwig Seitz, Göran Selander, Erik Wahlstroem, Samuel Erdtman, and Hannes Tschofenig. Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth). RFC 9200, August 2022.

[20] Alyona Skorobogatjko, Andrejs Romanovs, Nadezhda Kunicina, et al. State of the art in the healthcare cyber-physical systems. *Information Technology and Management Science*, 17(1):126–131, 2014.

[21] Sreelakshmi Vattaparambil Sudarsan, Olov Schelén, and Ulf Bodin. Survey on delegated and self-contained authorization techniques in cps and iot. *IEEE Access*, 2021.

[22] Eric Ke Wang, Yunming Ye, Xiaofei Xu, S. M. Yiu, L. C. K. Hui, and K. P. Chow. Security issues and challenges for cyber physical system. In *2010 IEEE/ACM Int'l*

Conference on Green Computing and Communications Int'l Conference on Cyber, Physical and Social Computing, pages 733–738, 2010.

[23] Kent Watsen, Michael Richardson, Max Pritikin, and Toerless Eckert. A Voucher Artifact for Bootstrapping Protocols. RFC 8366, May 2018.

[24] N Wu and X Li. Rfid applications in cyberphysical system, deploying rfid-challenges, solutions, and open issues, c. *DOI*, 10(17464):291–302, 2011.

[25] Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul, and Imran Zualkernan. Internet of things (iot) security: Current status, challenges and countermeasures. *International Journal for Information Security Research (IJISR)*, 5(4):608–616, 2015.

[26] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, and Shiuhpyng Shieh. Iot security: Ongoing challenges and research opportunities. In *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pages 230–234, 2014.

[27] Kai Zhao and Lina Ge. A survey on the internet of things security. In *2013 Ninth international conference on computational intelligence and security*, pages 663–667. IEEE, 2013.

Department of SRT
Division of EISLAB

ISSN 1402-1544
ISBN 978-91-8048-403-9 (print)
ISBN 978-91-8048-404-6 (pdf)

Luleå University of Technology 2023

LULEÅ
UNIVERSITY
OF TECHNOLOGY