A Framework to identify People, Devices and Services in Cyber-physical system of systems

Christoph Klikovits[2], Patrick Abraham[1], Rene Rambacher[1,2]

[1]*University of Applied Sciences Burgenland* - Eisenstadt, Austria
[2]*Forschung Burgenland* - Eisenstadt, Austria

***Abstract*—Many online services and their service providers require the electronic proof of identity for the secure authentication of citizens. Internet of Things (IoT)- and Cyber-Physical Systems (CPS)-services and devices are increasing and these are used in different areas. Furthermore, the increasing distribution of online services and IoT devices need to be monitored, especially in critical infrastructure. The proposal of a framework to authenticate and identify people, devices and services can be a useful tool to improve security and trust in CPS, linking them with identified people by utilizing and combining tools which do exist in isolation. IoT frameworks and identity protocols combined with responsible people, hardware, smartphone-applications, and certification authorities can provide secure authentication, trustworthy communication and the management of identities and permissions. This position paper proposes an IoT-framework for (critical infrastructure) service providers and public administration to authenticate, identify and manage their running devices and services as well as people, their electronic identification and sent records. This can improve the reaction time and processes additionally providing trust and secure communication between people, devices and services, especially for authorities in critical infrastructure areas, where humans and their safety are particularly important.**

***Index Terms*—Cyber-Physical system, Internet of Things (IoT), electronic identification, eID, MOA-ID, LoRa-WAN, eIDAS**

I. Introduction

The consideration of trustworthiness and security is important for the acceptance in data and technology. Especially for the use of an application which uses the cloud or wireless technologies. Critical infrastructure areas such as disaster management, data leaks and security gaps can cause enormous damage [2]. This damage often impacts the acceptance of an application and the trustworthiness of data. Authorities, organisations, service providers and the people behind them take responsibility for various attacks and liability. In disaster management in particular, every critical decision can affect a human life. IoT components which require trustworthy communication, can be used to improve the reaction time of disaster management processes. Therefore the involved responsibilities and hardware or software components must be identified.

978-3-903176-32-4

One of the main goals of the EFRE project (FE07) "Civis 4.0 Patria" is to develop a citizen participation and disaster management platform [8]. The project team considers to place IoT sensors in two municipalities with the aim of giving disaster warnings to the citizens and local authorities. In addition, people can report incidents such as open manholes or potholes to the local administration [1]. To enable this use case, wireless technology is planned to implement the IoT-based applications in a Long Range Wide Area Network (LoRa-WAN) [9]. The increasing number of IoT components including various devices and services lead to complexity and it is challenging for service providers to keep an overview or rather identify them and the communication among each other. There are various frameworks which can help to manage the IoT-components and to control how they interact with each other. The Arrowhead Framework with its core services (Service Registry, Authorization and Orchestration Service) [7] and a planned support service called Admission Ticket Provider (ATP) can be a representative tool to show a framework in this work to identify people and implemented devices or services by linking them with identified responsibilities. Disaster management is a sensitive area where critical infrastructure is used. Regarding these points, it is important to focus on the topics: trustworthiness, responsibility, and security. One of the main tasks in disaster management is to create a common overview of the situation. To improve this, it is important to communicate effectively and efficiently. Responsible instances in disaster management must trust each other in their cooperation and be able to interact safely [10]. Available solutions [12] [3] can be implemented in the applications of service providers to identify either people or devices (not both), ignoring identification of transferred data.

The contribution of this paper is to show a framework of unique identification of all cooperating entities in a disaster management system and its transferred data records. In the use case of the Civis 4.0 Patria project, reported incidents of citizens, sensor nodes (e.g., wireless components) and services (cloud platforms) can be identified related to a responsible person. The proposition of implementing a bootstrapping process before devices, or services are technically connected/onboarded [16] can be used to identify various types of objects by linking them with responsible, identified people.

This framework shows a technical proposition how people, devices, services, and transferred data can be identified and managed in a single internet of things framework using proved technologies of public administration to improve the reaction time of their processes.

The remainder of this paper is organized as follows: Section II provides the related work in the field and presents the background of this paper. Next, in Section III, we describe the use case and the framework for identifying people, devices and services. Finally, in Section IV a conclusion and an outline of future work is shown.

II. Related Work

Above all, disaster management requires discipline and trustworthy communication from all people and responsibilities involved in order to allow quick responses. New technologies are used in all areas of disaster management including preparation, reaction, and reconstruction to disaster. Regarding IoT devices, intelligence is created in various objects to collect environmental parameters to analyse this information to predict events or respond timely to any event. Even programs and systems for human performance are important tools in disaster management. Errors in this sensitive area, both from a human perspective and from the IoT devices used, can have devastating consequences [10].

A contribution of Sreelakshmi Vattaparambil Sudarsan [12] shows that CPS are used as agents that can automatically sign events and transactions. This approach shows, how people can be integrated in an automated document signature process when they give a power of attorney to IoT devices. While most related works focus on authentication and authorization, this approach provides digital power of attorneys in combination with signatory registry and authorization methods and signing events and could also be used in disaster management.

The Arrowhead Tools project integrates IoT-sensors into the Arrowhead local Cloud. Therefore its core- and support services are used. A support service was developed in an experiment of the Arrowhead Tools project called: connector. Various components like IoT devices, services, and nodes can be identified and managed with connectors of the Arrowhead Framework to strengthen the interoperability [11].

Available e-government solutions are the eID, the Module for Online Application-Identification (MOA-ID), the citizen card and mobile phone signature which are common solutions and enable secure identification of people over the national service and certificate authorization authority [3]. Various identification protocols give service providers the possibility to implement common e-government solutions in their backend applications to enable people secure online identification and usage of online services. Initially, the citizen card was introduced, which can be used to identify people. The citizen card requires card-reading devices and special applications, which decreases acceptance and usability. Furthermore server-based signatures services were rolled out protected through multi-factor authentication (e.g., personal computer and mobile phone) called the Austrian mobile phone signature. The mobile phone signature has found recognition in Austria and is a well-used identification method [4] [5]. Service providers can implement the mobile phone signature or the citizen card in their online applications to identify and authenticate people while the login or registry process. The implementation of the mentioned e-government solutions requires the use of an additional module called MOA-ID-Auth. This module represents an interface function between the signature process and the backend of the service provider. The electronic identification, authentication, and trust services (eIDAS) regulation has in all 28 EU member states lead to mutual recognition of nationally established electronic signature and identification solutions. It led to an identification method being developed further called eID [6]. The eID is a further advancement of the citizen card and mobile phone signature and will enable further options for users, as well as a restructuring of the registration process. It's planned to register through authorities and roll out the eID to people requesting a passport, unless expressly refused. The eID represents a universal electronic identification method and opens possibilities for identification and authorization of online services (e.g., electronic driver license). After the launch of the eID, MOA-ID-Auth will be replaced by other identification protocols: Security Assertion Mark-up Language 2.0 (SAML2) for browser-based applications for exchanging authentication and authorization identities or OpenID Connect for service providers who want to integrate an eID login in their mobile applications [13]. The explored approaches and technologies in the field have all major limitations:

- They either focus on identifying people during the login or registration process
- The identification of transferred data records is not supported and not linked with a trustworthy identity-provider

In contrast to other work this position paper proposes to combine secure, trustworthy identification covering people, devices, and services with the use of the Arrowhead Framework and a common identity provider building a CPS. Various components in the use case scenario of a citizen participation and disaster management platform are considered which can be identified through certification authorities and used by service providers and their online applications. The ability to integrate and identify people, devices and services opens new possibilities to service providers to ensure unique identification. Especially in disaster management, devices like IoT sensors and of course cloud services are commonly used and require secure and trustworthy deployment to prevent unforced and forced errors in case of emergency and to allow quick responses. Furthermore, we present a framework in this position paper which is capable of managing identities and identify data records of people, devices, and services. The Arrowhead Framework can be used to manage identities automatically to enable a server-side authorization and identification of datasets (e.g., reported incidents in case of emergency or forwarded payloads from different IoT Sensors). This framework can avoid usability issues, enables the verification and identification of sent payload to the backend-system from

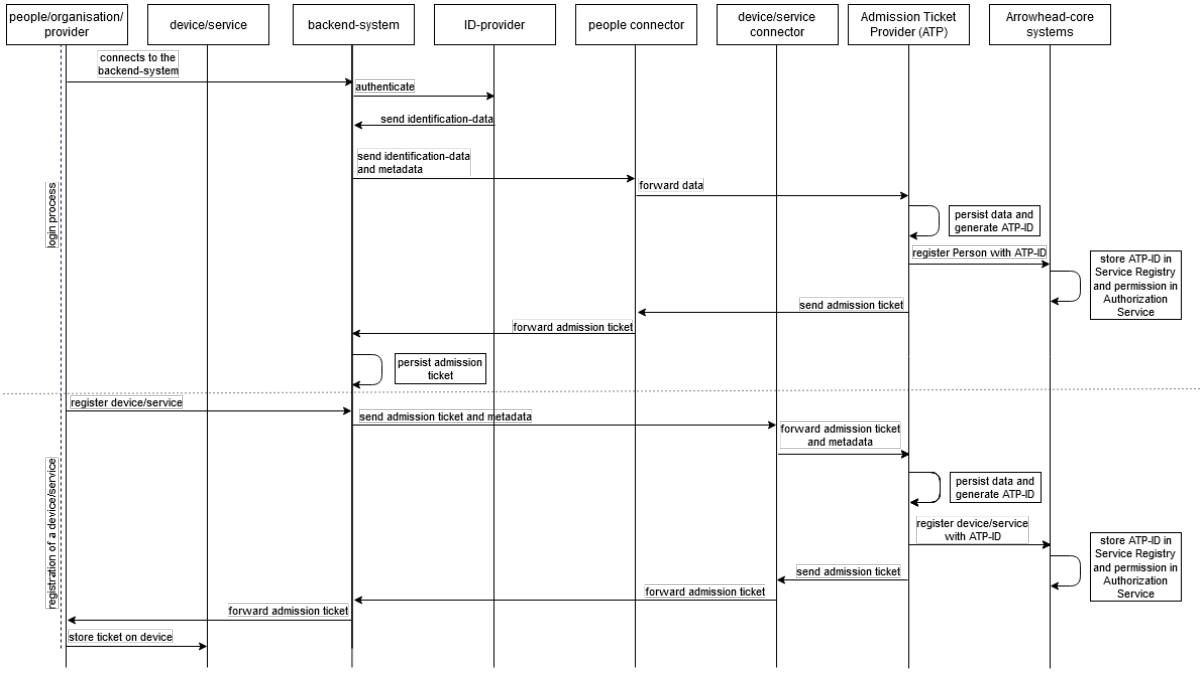

Fig. 1. The sequence diagram for the login- and device/service registration process

various instances and can provide a possibility how to prevent man-in-the-middle attacks by checking every data traffic. This can lead to Internet of trusted things as presented by N. Zivic et al. considering various components and technologies linking with IoT [14].

III. Proposal for a framework to identify people, devices and services

In this section we describe how the framework ensures that the data being received comes from trusted people, devices, or services. The information about who is sending the data and who is configuring the services and devices has for this use case a high priority. For integrating the different identification solutions into a single framework, we decided to use Arrowhead. To provide flexibility we decoupled our services from the authentication and identification for being able to send data to the backend-system. The features used in the Arrowhead Framework create a dynamic orchestration framework, which is a System for automating processes in the IoT domain, with security build in natively. The framework offers a variety of services with different purposes. In our use case only the core systems are needed. The core systems consist of three services. These are called Authorization Service, Service Registry and Orchestrator Service. The goal of the Service Registry is to store information about the different services that want to use the connector. The Authorization Service needs this information to authorize and authenticate the services to enable them to communicate with each other. The interaction happens by requesting information from the Orchestrator Service. The Orchestrator Service is there for providing a discovery-service which relies on rules defined in Authorization Service [15].

Since our services are decoupled from the Arrowhead-cloud there is no need for storing any Arrowhead-certificates locally. That is where the connectors step in. The connectors get implemented through a certificate in the Arrowhead cloud using the Onboarding Procedure [16]. Further they receive data and manage it by asking the Orchestrator Service if they are allowed and where to send it.

A. Login Process

The purpose of the login process as shown in Fig. 1 is to enable the identification of a person. Therefore, the person the organisation or the service-provider has to logon to the backend-system, which is linked with an ID-provider to prove their identity. The ID-Provider could be an identity system of any public administration. In our use case we focus on MOA-ID an interface which is linked to the ID-provider of the public administration of Austria. Afterwards the identification-data will get send to a service called Admission Ticket Provider (ATP) through the people connector. Next, the ATP stores the data and generates a unique ATP-ID using a hash function on the transferred data. This ATP-ID needs to be stored in the Service Registry and the permission needs to be stored inside the Authorization Service. Once this is done the ATP will send an admission ticket to the people connector which forwards it to the backend-system. The ticket will be stored in the backend-system and is mandatory for identifying a person. A person, organisation, or a service-provider can now be identified by checking the unique ATP-ID in the Service Registry inside the Arrowhead-Cloud.

B. Identifying data using the people connector

The use case of Civis 4.0 Patria includes the functionality for citizens of municipalities to report incidents to the local administration. For people who want to send such incident reports to the backend-system, it is necessary to go through the login process as shown in Fig. 1. After the successful login, a person can now send data to the backend-system (Fig. 2). This is also the destination where the admission ticket of an identified person is stored. For a request to successfully reach the backend-system it is mandatory to have a valid admission ticket. The backend-system forwards the request with the admission ticket to the people connector which triggers the Orchestrator Service of the Arrowhead Framework. The Orchestrator Service tries to identify the person via the Service Registry by using the admission ticket, checking the ATP-ID and the permission by consuming the Authorization Service. If the person fulfils both requirements, the data will be sent from the people connector to the backend-system. Now, the backend-system can trust the payload from the people connector and publish the transferred and verified incident report.

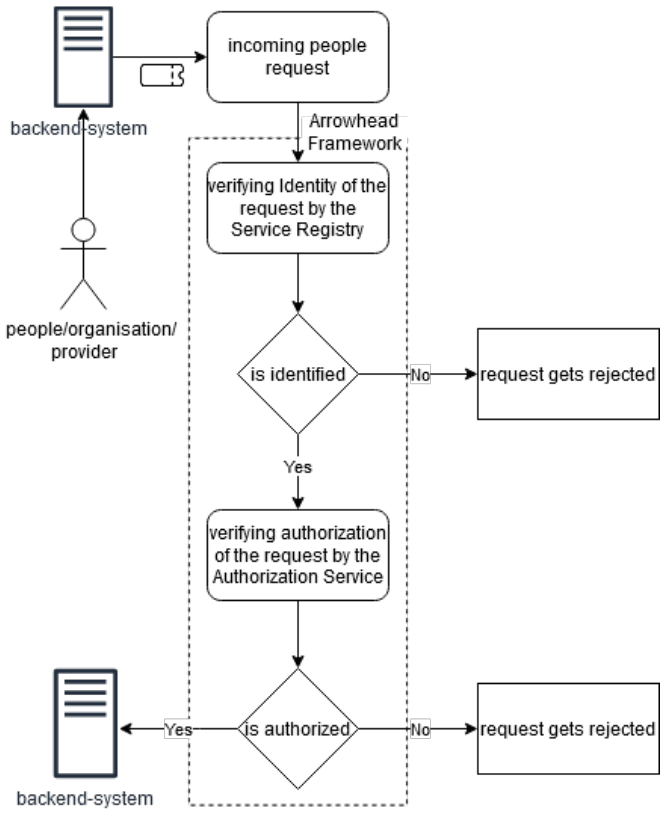

Fig. 2. Description of the process when people send a request to the backend

C. Registration of a device or service

The purposed framework shows an identification method by combining different objects (e.g., people, devices, and services) with identified responsibilities. To register a device or service (Fig. 1) the responsible person, who is identified through the login process as seen in Fig. 1, has to login into the backend-system. The person must send the data needed for registering a device or service (e.g., Internet Protocol (IP)-address, Media-Access-Control (MAC)-address, initial device identifier) to the ATP through the device/service connector. Then the ATP again starts to generate a unique ID (ATP-ID) for the device or service and stores the results as well as sending the ATP-ID to the Service Registry and the permissions to the Authorization service. Afterwards an admission ticket gets send and forwarded to the responsible person via the device/service connector. The person/organisation/provider who registered the device must check the result and store the admission ticket locally on a device. Once this is done the device can start sending authorized data requests.

D. Identification of data using the device/service connector

For a citizen participation and disaster management platform various types of data and information must be gathered and stored. An unclear picture about the situation could trigger an emergency warning and cause confusion and distrust among the users of the platform. To prevent that, it is an important aspect to provide valid and verified data to the backend-system. We propose a similar framework for various devices and services as shown in Fig. 3. To gather trustworthy communication through different components, we linked every device or service with a responsible, identified person. Furthermore, we built a device/service connector which has a similar purpose as the people connector. It uses the Arrowhead-cloud for identifying and authorizing devices or services and its transferred data using the admission ticket process. The Orchestrator Service acts again as a discovery service by checking the Service Registry with a valid admission ticket for the identity and the Authorization Service for the permission.

E. Pros and Cons

With this proposed framework, the public administration can rely on the fact that the data sent comes from trustworthy identified people. It also ensures that all registered devices or services have only been configured or mounted in the system by trustworthy people. This means in the case of an incident they can take on immediately action because there is no need to check the trustworthiness. This can lead to additional administrative effort, but in return, critical infrastructure providers and public administration can respond more quickly to this foundation of trust. In our use case the advantage of speed in form of an immediate reaction overweight's the increase in administration effort.

From a security point of view, the Arrowhead-Framework acts as a proxy and disguises the location of the backend-system. This makes man-in-the-middle attacks more difficult. The attacker would not know where the backend-system resides since the only visible endpoints are the connector services. That ensures trust since the backend-system knows that only identified and authorized users can access it.

The mechanic of linking each device or service to a responsible person strengthens the responsibility and liability

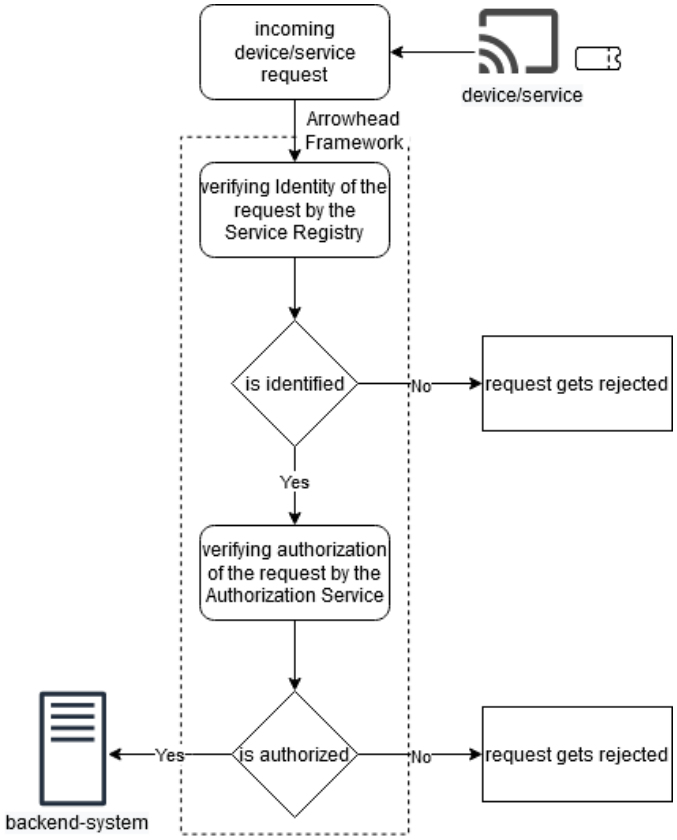

Fig. 3. Description of the process when devices or services send requests to the backend

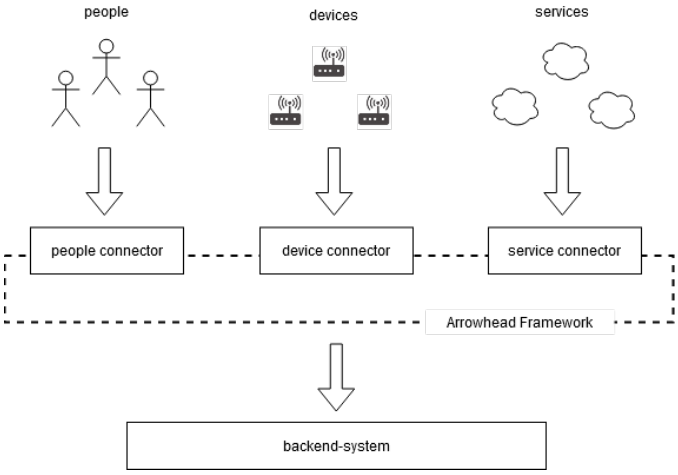

Fig. 4. Description of the high level framework

on shared data. This is solved through the admission ticket process and the admission ticket provider service. The usage of an admission ticket provider gives full control over the identification process. Public administration uses different solutions to identify people and it is necessary to abstract this layers to provide a general interface. Therefore, it is mandatory to send an admission ticket created by the ATP. Neither an unknown nor a non-authorized system can pass this procedure. More importantly, every request on its own must pass this procedure and the backend-system can trust the data and implemented components. This methodology applies to every purposed connector. Since the Arrowhead cloud is decoupled from the connector various types of entities could be identified and authenticate this way.

As shown in Fig. 4, the purposed framework can be applied to more than one type of scenario. In this context, communication via the Arrowhead Framework enables an additional layer of security, regardless of whether people, devices or services are registered or send data. The main advantage of this is that the Arrowhead Framework - for each access to the backend-system - checks the identification and authorization of the person and his transferred data records. Due to this unlinking, it is possible to make the system independent from the application that wants to access the backend-system. No matter if web or mobile app. For now, the only requirement for the connectors is the use of a Representational State Transfer (REST) interface for communication.

An example of its versatility could be an implementation into a microservice architecture as a message broker. By doing that, every microservice would be identified and authorized. As shown in our use case, this can enhance trust by preventing microservices talking to each other that are unknown or that are known but are not allowed to. Furthermore, it can be implemented in a legacy system. The interface of the Arrowhead-cloud is REST, but the connectors could use any other available technology to build an API for the communication outside of the Arrowhead-cloud. Since Arrowhead uses REST for its Application Programming Interface (API), the choice of programming language on which the connector service is built is independent. All the languages that are used to build a connector must be able to establish a communication via REST. All this flexibility can make the system universally applicable, and the use case is not just in mobile apps and web apps. Any type of application, service or device can securely transfer data through a connector via the Arrowhead-cloud.

The interoperability by using the connector makes the presented framework applicable to every design. On the basics it works as an identity management system where the identity and the authorization get stored and dynamically orchestrated. The unlinking improves the management of those components since changes about the identity and authorization are stored inside the Arrowhead-cloud.

The architecture is not only usable in various environments it also provides scalability. New services that are added over the lifetime of a system only need to be linked with the connector. They do not need to know anything about the backend, all the work is done inside the Arrowhead-cloud. The original idea of Arrowhead was to build an autonomic system for IoT devices, but with the proposed framework Arrowhead can also be used as an autonomic system for different components.

IV. Conclusion and future work

In this position paper, we propose a framework for managing and identifying components of a CPS and its data records with the intention to gather secure and trustworthy communication for critical infrastructure providers and public administration including people, devices, and services. We present the Arrowhead Framework as a representative IoT framework in combination with an external identity provider and an additional support service called ATP. The identification of people, devices, services and data records can be implemented for different purposes in various systems. In our use case, Arrowhead linked with identification thoughts is an important component to gather secure and trustworthy communication in a disaster management platform. By providing authentication and identification, on each data transmission, through the Arrowhead-cloud, it provides an additional layer of security in this type of communication and reduces usability issues by authorizing instances automatically on server-side. This proposed framework implements a bootstrapping process using the Arrowhead Framework and an external identification service of the Austrian public administration thus guarantees that the transmitted data and involved components are identified thus linked to those responsible people and act in a trustworthy and secure way. Including identification of people, devices, services, and its transferred data in a single system with the aim of becoming an internet of trusted things platform to allow quick and trustworthy responses. Reffering to our use case, responsibilities of disaster management organisations and public administration can use our proposed framework and receive trustworthy data from trustworthy instances. In addition, they can trust that a responsibility has configured a trustworthy device. Now that a trustworthy connection has been established, processes and the reaction time can be optimized to allow quick response and picture of the situation.

We have mentioned common e-government solutions used in Austria (e.g., MOA-ID). The update of the eID and its identification protocols (SAML2 and OpenConnectID) is planned to roll out in quarter 2 of 2021. To integrate the eID solution in our addressed framework and use case, further work is needed. Furthermore, the mentioned mechanism, where devices can sign on its own by using signatory registry and methods for authorization using digital power of attorney (POA) represents an interesting approach for future work. In future, the Onboarding Procedure of the Arrowhead Framework can be used to enroll the backend and the clients ensuring a chain of trust. The renewal of an admission ticket concerning the device and service connector and the implementation of the ATP in the core services of the Arrowhead Framework can be researched in future. Another idea could be to integrate blockchain-like technologies in our framework which braces the concept of being distributed and decentralized. Our plan is to demonstrate this in a proof of concept fashion in future work.

Acknowledgment

Research leading to these results has received funding the partners national programmes/funding authorities and the project Civis 4.0 Patria (FE07), funded by IWB-EFRE 2014 - 2020 coordinated by Forschung Burgenland GmbH.

References

[1] Christoph Klikovits, Elke Szalai, Markus Tauber, "Covering Ethics in CyberPhysical Systems design, ERCIM News, issue 122, 2020, https://ercim-news.ercim.eu/images/stories/EN122/EN122-web.pdf, https://ercim-news.ercim.eu/en122/r-s/covering-ethics-in-cyber-physical-systems-design

[2] Tankard, C. (2011). Advanced Persistent threats and how to monitor and deter them. Network Security, 2011, 16–19. https://doi.org/10.1016/S1353-4858(11)70086-1

[3] Lenz, T., Zwattendorfer, B. (2017). Towards Cross-Border authorization in European eID Federations. 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-16), 426–434. https://doi.org/10.1109/TrustCom.2016.0093

[4] Theuermann, K., Tauber, A., Lenz, T. (2019). Mobile-Only Solution for Server-Based Qualified Electronic Signatures. ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 1–7. https://doi.org/10.1109/ICC.2019.8762076

[5] Rath, C., Roth, S., Schallar, M., Zefferer, T. (2014). A secure and flexible server-based mobile eID and e-signature solution. The Eighth International Conference on Digital Society, 7–12.

[6] Alonso, Á., Pozo, A., Choque, J., Bueno, G., Salvachúa, J., Diez, L., Marín, J., Alonso, P. L. C. (2019). An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation. IEEE Access, 7, 88435–88449. https://doi.org/10.1109/ACCESS.2019.2926556

[7] Ivkic, I., Pichler, H., Zsilak, M., Mauthe, A., Tauber, M. (2019). A Framework for Measuring the Costs of Security at Runtime. 488–494. https://doi.org/10.5220/0007761604880494

[8] Forschung Burgenland. (o. D.-b). Forschung Burgenland. Abgerufen am 20. Januar 2021, von https://www.forschung-burgenland.at/it/civis-40-patria/

[9] Butun, I., Pereira, N., Gidlund, M. (2019). Security risk analysis of LoRaWAN and future directions. Future Internet, 11(1), 3.

[10] Ghasemi, P., Karimian, N. (2020). A Qualitative Study of Various Aspects of the Application of IoT in Disaster Management. 2020 6th International Conference on Web Research (ICWR), 77–83. https://doi.org/10.1109/ICWR49608.2020.9122323

[11] Bengtsson, K. (n.d.). Arrowhead Tools The Norwegian Mountain Bike Experiment. https://www.arrowhead.eu/arrowheadtools/publications/presentations/arrowhead-tools-the-norwegian-mountain-bike-experiment/

[12] Sudarsan, S. V., Schelén, O., Bodin, U. (2020). A Model for Signatories in Cyber-Physical Systems. 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 1, 15–21. https://doi.org/10.1109/ETFA46521.2020.9212081

[13] Hintergrundinformationen zur Architektur von ID-Austria. (o. D.). ID-Austria. Abgerufen am 20. Januar 2021, von https://eid.egiz.gv.at/infos/hintergrundinformationen/architektur/

[14] Zivic, N., Ruland, C., Sassmannshausen, J. (2019). Distributed Ledger Technologies for M2M Communications. 2019 International Conference on Information Networking (ICOIN), 301–306. https://doi.org/10.1109/ICOIN.2019.8718115

[15] Varga, P., Blomstedt, F., Ferreira, L., Eliasson, J., Johansson, M., Delsing, J., Martínez de Soria, I. (2016). Making system of systems interoperable – The core components of the arrowhead framework. Journal of Network and Computer Applications, 81. https://doi.org/10.1016/j.jnca.2016.08.028

[16] Bicaku, A., Maksuti, S., Hegedus, C., Tauber, M., Delsing, J., Eliasson, J. (2018). Interacting with the arrowhead local cloud: On-boarding procedure. 743–748. https://doi.org/10.1109/ICPHYS.2018.8390800