future internet

Article

A Trustworthy Communication Hub for Cyber-Physical Systems

Juhani Latvakoski * and Jouni Heikkinen

VTT Technical Research Centre of Finland, Kaitoväylä 1, 90570 Oulu, Finland; Jouni.Heikkinen@vtt.fi

* Correspondence: Juhani.Latvakoski@vtt.fi; Tel.: +358-40-5200-149; Fax: +358-20-722-2320

Received: 17 June 2019; Accepted: 19 September 2019; Published: 8 October 2019

Abstract: The motivation for this research arises from the challenges in the trustworthy communications related operation of cyber-physical systems (CPS), especially in the energy and mobility domains. The increasing amount of distributed energy resources (DERs) of prosumers and electric vehicles requires new ways for CPS communications to enable information exchanges for smart operation in peak consumption hours and balancing power levels in the energy grids in order to lower the energy cost. The huge number of mobile appliances and the related service providers do not serve properly the privacy of the owners, owing to the vertical silo type of operating model in industries. As the results of this research, we provide a trustworthy communication hub for CPS (CPS hub) for solving the challenges related to trustworthy communications between physical resources owned by different stakeholders. The CPS hub realizes the communication spaces concept, and enables combined trust and communications processes when dynamic resources owned by different stakeholders are exchanging information. The evaluations showed that the provided CPS hub enable information exchanges between distributed energy resources of different stakeholders, so that they can join the aggregation process for more flexible and efficient resource usage in energy markets. The CPS hub enable interaction between heterogeneous physical devices of multiple stakeholders to exchange information so that, for example, authorities can see the situation in the emergency area and, simultaneously, the policies of the owners can be taken into concern. Despite limited evaluation scenarios, it is shown that consideration of the ownership issues in the trustworthy communication for information exchanges between heterogeneous physical resources (devices) is possible and feasible. Several future research items, such as, for example, scalability; real-time and streams based operation; as well as consideration of the security, privacy, trust, and safety challenges, were detected. However, the evaluations showed that the constructed CPS hub contribute a set of very essential technical enablers for future smart CPS systems and create strong a basis for such future research towards a future smart society.

Keywords: cyber-physical systems; machine-to-machine communications; Internet of Things; smart energy systems; smart mobility systems; communications; security; trust

1. Introduction

Today, industries and consumer markets are increasingly using services exposed from various physical devices, such as, for example, sensors and actuators, via heterogeneous networks. The aim of such systems is to enable the physical world to collaborate with the cyber-world to boost the real-time economies of companies. Such cyber-physical systems usually consist of physical resources (devices), subsystems, and service clouds owned, provided, and/or hosted by different stakeholders. The essential grand challenge arises from the need for trustworthy interactions between the referred resources and different stakeholders. This research focuses on solving this grand challenge related to trustworthy communications in such cyber-physical systems (CPS), especially in the energy and mobility domains.

There are multiple cyber-physical entities in the energy domain, such as, for example, solar power plants; wind mills; electric vehicles; buildings; energy sensitive household appliances; and other kinds of distributed energy resources (DERs) consuming, producing, or storing energy, which have caused challenges for distribution network operators in balancing power levels in the energy grid. The peak consumption hours are becoming ever more expensive for the energy sector, energy intensive industry, and consumers. The industry is looking for more flexible and smarter operational models for the energy grid. Therefore, an essential industrial objective has been to cut down the peak loads of a day to lower the cost of energy and its distribution. Such flexibility capabilities require trustworthy communications for information exchange between the cyber-physical entities from multiple energy sensitive domains and energy domain systems and stakeholders.

There is huge number of appliances in the mobility sector, such as smart watches, smart phones, sensors, tracking devices, vehicles, and multiple stakeholders, which are often not able to interact with each other. This is because, usually in CPS business sectors, a service provider (SP) hosts specialized physical resources (e.g., products of the SP) and the related exposed data/information in their own service cloud as a kind of vertical silo. However, the owners of the referred physical resources may not be the SPs themselves, but instead their customers, which may be individuals (private persons or their groups), companies, organizations, or a combination. Today, such owner stakeholders require ever more trustworthy, smart, and interoperable operation from their SPs, which is in line with their own collaboration agreements and privacy regulations (GDPR, General Data Protection Regulation (EU) 2016/679). For example, if some unexpected emergency type of event, such as, for example, a traffic accident, happens, it is challenging to know the situation, even if the information could be available. There are people, vehicles, and other referred devices that have the capabilities to collect data/information from the event. However, the devices cannot interact with each other, and thus it is very challenging to know the situation even if the information could be available. These situations require trustworthy communications for information exchange for smart operation with the appliances from multiple sectors, hosted by multiple SPs, and SP service systems/clouds.

Both energy flexibility and traffic accident cases indicate the needs for smart, trustable, secure, and interoperable communications for information exchanges between physical resources owned by different stakeholders, that is, the focused grand challenge of this research. This inherently includes such aspects as privacy, confidentiality, end-to-end security, secure data management, and access control. In particular, which other CPS entities and users are allowed to communicate and exchange data with this specific CPS entity. Such communication access rights depend on the privacy and security policies of the owner and the service provider (SP) of the referred entity. It is also well known that some application ecosystems have very much the same types of challenges to collaborate. For example, Apple's iPhone is tightly coupled with its cloud storage service iCloud, Android smart phones with Google Drive, and Windows ecosystem with OneDrive. Accordingly, wearables, home automation devices, machines, and so on are tightly coupled to operate with the specific SPs' clouds. These realities cause significant barriers for smart communications between CPSs required by the owners.

The owners require trustworthy and secure communications, and data/information exchange exposed from their owned CPS entities with the other owners without compromising their privacy. This means that the owners need to manage access rights across several SPs that host their CPS entities. Currently, there is lack of proper means for owners to monitor and control the policies used to regulate access to their CPS entities and exposed data. Furthermore, each SP usually uses its own specific solution for access control. This requires owners to redefine their policies for each SP system, which causes difficulty in synchronizing them across multiple SPs. The situation becomes even more challenging when owners want to share their CPS entities with other owners who are not registered to the same SP, and SPs do not have any means of verifying authorizations for unknown users. However, owners require more and more trustworthy, smart, and interoperable operation from their SPs, which is in line with their own collaboration agreements, and their regulated privacy and ownership rights related to the data/information exposed from their physical CPS entities (resources).

The selected research method is experimental/constructive relying on hybrid simulation based prototyping and systematic evaluation of the solution constructions. The hybrid simulation refers to a method in which simulated entities and models are executed together with selected real entities in order to validate the operation as much as possible representing real system behavior [1]. The results from the preceding steps of this research, the dynamic communication spaces concept, are applied as an essential starting point for this research [2]. Accordingly, it is expected here that each user/owner has its own communication space, which consist of links to the services, networks, content, and devices of the specific user. In the preceding steps, the required capabilities as separate functionalities for enabling the concept were studied; however, the challenges related to trust and security were not considered and any proper design of the communication spaces solution was not proposed. In this research step, we focus on solving these challenges and prototyping a novel solution realizing the concept, which is especially targeted to fulfill the needs of energy flexibility and traffic accident cases. As the result, we provide a trustworthy communication hub for CPS (CPS hub), describe its' main conceptual enhancements with design of building blocks, and clarify the evaluations. Special novelty arises from the combined trust and communications process when dynamic resources owned by different stakeholders are exchanging information. The solutions provided are developed in a step-by-step manner and evaluated accordingly in the energy flexibility and traffic accident cases.

The reminder of this paper is organized as follows. Related works of this research are discussed in Chapter 2. The main concepts of the CPS communications hub are provided in Chapter 3. The building blocks of CPS communication hub are described in Chapter 4, and respective solutions in Chapter 5. The evaluation results are clarified in Chapter 6. Finally, the conclusions are presented in Chapter 7.

2. Related Works

The targeted grand challenge of this research dealing with communications of cyber-physical systems arises from the accessibility, trustworthiness, heterogeneity, mobility, and ownership of physical entities. The interaction with physical resources (devices) over the communication networks shall concern the ownership, communications, and trust aspects. The adopted solution approach is based on the application of communication overlay and security technologies in a novel combined way for experimental realization of the communication spaces concept, represented in the proceeding step of this research [2]. The communication spaces concept applies the idea of making a kind of virtual home for people and their resources. The respective idea has been applied earlier, for example, in the concept of virtual home environment for supporting roaming ecosystems in the mobile context for the mobile device of a user [3]. The same type of concepts has also been developed for sensors devices, for example, virtual sensor services, called the µSMS (micro subscription management system) middleware, for smart environments over sensor networks from tiny in-network services based on agent technology is provided in the work of [4]. The respective required functionalities are included e.g., in the smart instant messaging (SIM) system with presence management, user centric configuration and adaptive grouping [5]. However, the requirements arising from ownership, trust, and communications when dynamic resources owned by different stakeholders are exchanging information are not known to be considered earlier in such energy flexibility and mobility cases.

A review of some communication overlay technologies is represented in Table 1 (see also the works of [2,6]), and discussed in the following. An essential required feature in CPS systems is delivery of information from one source to one (1–1) or multiple destinations (1–N) according to the needs of the destinations. Therefore, the capability to realize publish/subscribe paradigm was seen to be more relevant than the pure client/server model [7]. For example, extensible messaging and presence protocol (XMPP) technology [8,9] has such a publish/subscribe mechanism, which is based on the concept of a specific entity called "pubsub" node [10–12]. Such a "pubsub" node acts in a way as the publish/subscribe service established to work in the XMPP server. A publisher can publish information into the "pubsub" node. A subscriber can subscribe the referred information, and receive event notification when the information is published. However, the referred XMPP based publish/subscribe means have proved to be quite complicated. The publish/subscribe capabilities of the message queue based telemetry transport (MQTT) protocol have proved to be much more simple and lightweight for physical resources [13,14]. There are also other respective message queues; broker-based (e.g., data distribution service (DDS), advanced message queuing protocol (AMQP), and simple text oriented messaging protocol (STOMP)) or broker-less (e.g., zero message queue protocol (ZeroMQ)).

Table 1. Review of communication overlay technologies.

Technology	Forum(s), References	Main Contribution
Extensible Messaging and Presence Protocol (XMPP)	- Core XMPP protocols defined in Internet Engineering Task Force (IETF) Requests for comments (RFCs) 6120, 6121 and 6122. - XMPP Standards Foundation (XSF), http://xmpp.org/, also publishes extensions to the core protocols (XEPs) - E.g., Sensor-over-XMPP, XMPP extension [15]	- XMPP provides capabilities for instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of Extensible markup language (XML) data - Sensor-over-XMPP is a payload format for communicating sensor and actuation information
Session Initiation Protocol (SIP)	- IETF RFC 3261 [16]	Establish and control of multimedia sessions over the Internet
Hypertext Transfer Protocol (HTTP)	- IETF RFC 7231 [17] - RESTful architectural style	Protocol for transferring hypertext information
WebSocket protocol	- IETF RFC 6455	Two-way communications with low-overhead transport (single transmission control protocol (TCP) connection)
Simple Mail Transfer Protocol (SMTP)	- IETF RFC 7504	Transfer of emails in a reliable and efficient way
MQ Telemetry Transport (MQTT)	MQTT Eclipse Machine-to-Machine (M2M)Industry Working Group	Lightweight publish/subscribe binary messaging protocol
Advanced Message Queuing Protocol (AMQP)	OASIS AMQP standard	Broker-based messaging, publish/subscribe
STOMP	https://stomp.github.io/	Simple text oriented messaging protocol
ZeroMQ	ZeroMQ protocol	A lightweight publish/subscribe type of messaging protocol designed for constrained devices and low-bandwidth, high-latency, or unreliable networks
Data Distribution Service for Real-Time Systems (DDS)	OMG DDS http://portals.omg.org/dds/	Middleware protocol and application programming interface (API) standard for data-centric connectivity for Internet of Things (IoT) applications
CoAP	IETF's constrained RESTful environments (CoRE) working group RFC [18]	An application layer protocol designed for constrained devices allowing them to communicate over the Internet

The other required feature is related to naming and identification of the owners. A very natural way to name the source and destination of messaging is provided by the electronic mail systems with protocols such as Simple Mail Transfer Protocol (SMTP, RFC 5321 and 5322), Post Office Protocol (POP), and Internet Message Access Protocol (IMAP). XMPP and session initiation protocol (SIP)/SIMPLE have also such capabilities to name the owner, and they also support the naming of the resources of the owner. Naming and identification of the physical resources (devices) that belong to an owner is an essential feature in CPS systems. However, this is not enough because there is the need for dynamically defining and maintaining the relationships of owners, which is supported by XMPP in the form of the contact "Buddy" list management feature.

The capability to support maintaining the presence of physical resources (devices) so that the system knows whether the resource is available or not. This kind of feature is supported by, for example, XMPP and SIP/SIMPLE. Accordingly, there is the need for simple clients and rapid 'real-time' messaging between resources that are present in the system. XMPP utilizes a decentralized client-server architecture to keep the clients simple, and pushes most of the complexity into the servers. The architecture is different from the World Wide Web (WWW) in the sense that it supports inter-domain connections called federations. In addition, the email network uses multiple hops between servers to deliver messages, but the XMPP architecture uses direct connections, which helps the creation of real-time messaging and simple clients. SIP has been applied for instant messaging, event notification, presence, and control of networked appliance communication.

The capability to support exchanging of heterogeneous information content between heterogeneous resources so that the communication is efficient and communicating parties are capable to understand the meaning of the information is an essential requirement in CPS systems. For example, the IETF CoRE (constrained RESTful environments) working group has specified the constrained application protocol (CoAP) with the goal of supporting REST-like applications in constrained environments in a more efficient way. SIP has been developed for controlling multimedia sessions over the Internet, and after such a control process, the real streams can go directly between the endpoints of communications. Respective solutions are needed in CPS systems; for example, energy domain processes require application of specific information models to enable understanding the message content between communicating parties. Thus, it is very essential to have some "identities" for the information so that the communicating parties know what information the other entities are publishing. MQ telemetry transport (MQTT) provides a possible way for such an identification by defining the concept of "topic" name, which could be applied as the name for the shared information. However, MQTT seems not to have proper capabilities to define the owners and their physical resources in a simple way.

The last, but not the least capability is related to the needs of each owner to control who can access use of his/her/its physical resources (devices) and exposed information, as well as how, when, and in which situations this can happen. The dynamic maintenance of the owner relationship using contact "Buddy" list feature of XMPP is possible. However, this is not enough, because there is need to define more specific rules and conditions for the access of CPS resources/devices concerning such aspects as, for example, privacy in a distributed ecosystem. Needs towards more centralized management of access rights have been detected in the work of [19]. A review of the access control solutions that could be applicable for the Internet of Things (IoT) has been analyzed in the work of [20]. On the basis of the detailed analysis, the main challenges of applying access control mechanisms for IoT were detected, and especially the viewpoint of constrained environment is discussed. A dynamic, scalable, and IoT-ready model based on OAuth 2.0 protocol that allows the complete delegation of authorization, so that an access control mechanism as a service is enabled [21]. The challenges of data sharing in multi-cloud environments are analyzed and an extensible access control markup language (XACML) [22] based architecture, called SAFAX, has been provided [23]. SAFAX's architecture with prototype realization allows users to deploy their access control policies in a standard format, in a single location, and augment policy evaluation with information from user selectable external trust services. The policy based access control as a service could enable owners to define and manage their access control policies to protect their resources for multiple stakeholders.

Summarizing, the analysis of the requirements arising from our grand challenge proved that there are helpful features in some of the existing technologies; however, none of them is not capable to fulfill them all. In this research, we provide an experimental realization of the communication spaces concept by applying the XMPP, MQTT, and SAFAX technologies so that specific applicable capabilities of them are adapted to the needs of CPS. The special novelty of our contribution arises from the combined trust and communications process when dynamic resources owned by different stakeholders are exchanging information.

3. Concepts of the CPS Communication Hub

3.1. Conceptual Model for Cyber-Physical Systems

A view of the structure of cyber-physical systems (CPS) is visualized in Figure 1, and shortly clarified in the following. The CPS system usually consists of subsystems such as a capillary network, gateway, infrastructure, and service systems, which are usually hosted by different stakeholders such as service providers, infrastructure providers, mobile connectivity providers, and asset providers. Each of these stakeholders usually have a number of agreements based relationship with their customers. This means that they usually have their own database of allowed users (their customers) in their service systems, which they do not necessarily want to open for the other SPs because of business reasons. However, multiple SPs can have agreements with a single user.

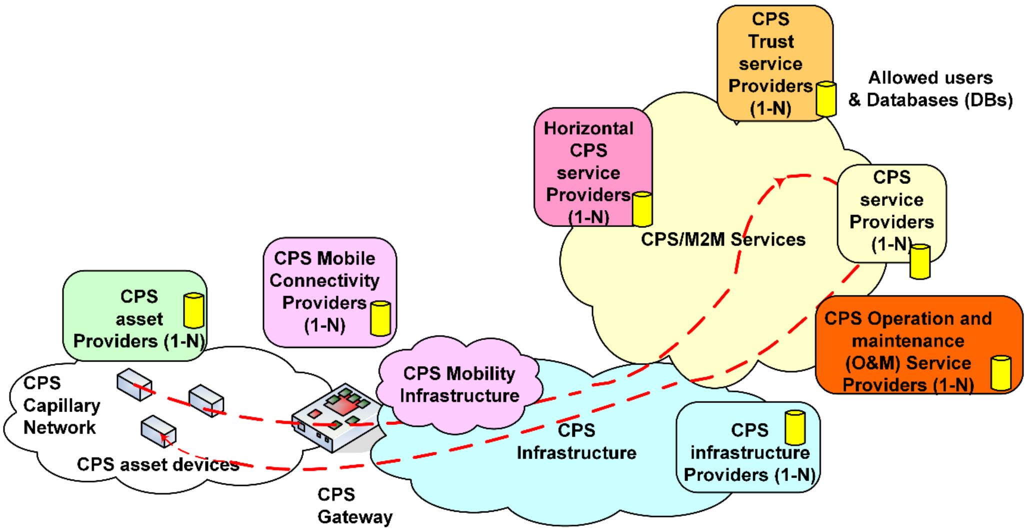

CPS Trust service Providers (1-N)
Allowed users & Databases (DBs)
Horizontal CPS service Providers (1-N)
CPS service Providers (1-N)
CPS/M2M Services
CPS Mobile Connectivity Providers (1-N)
CPS asset Providers (1-N)
CPS Operation and maintenance (O&M) Service Providers (1-N)
CPS Mobility Infrastructure
CPS Capillary Network
CPS asset devices
CPS Infrastructure
CPS infrastructure Providers (1-N)
CPS Gateway

Figure 1. A view of the structure of a cyber-physical system (CPS).

When looking at the system from the referred customers/users' point of view, another complex dimension of the system pops up. This is because usually CPS entities (devices) may belong to a user, group of users, or an organization (*owner*). It is obvious that the owners want to use all the services relying on their own M2M asset devices/resources and the extracted M2M data/information based services in a smart way. As the result from these needs and recent new GDPR (General Data Protection Regulation (EU) 2016/679) regulations, it is envisioned that the requirements of owners shall be an essential starting point for establishment of future smart interoperable cyber-physical systems.

Therefore, it is seen that the agreements between owners establish the rules according to which the access rights can or cannot be established. When looking at the agreements of an individual owner, it is obvious that there can be agreements with multiple service providers. For example, in the energy sector, the owner can have an agreement, for example, with an energy seller, energy aggregator, distribution network provider, and charging operator. The same owner can have also agreements, for example, with health and wellness service providers, among others. In addition, when looking at the relationships of the referred owner on a more detailed level, the owner can have an agreement level relationship with family/organization members and reliable friends/partners. However, it is obvious that such relationships can be under continuous change/maintenance processes. In addition, the trustability of the relationships may be fuzzy from an individual owner point of view. Therefore, there is the need for continuous monitoring of trust level.

This reasoning has led us to the assumption that the future cyber-physical systems shall be structured in a new way by taking the *ownership and trust* related requirements as the key starting point. The respective conceptual architecture model created as a part of this research and clarified in the work of [24]. According to it, the CPS system has been divided into set of CPS architectural zones according to horizontal abstraction levels of the system, system evolution perspectives, access rights, and roles of related stakeholders in the typical CPS value network. The defined architectural zones are vertical enterprises, IoT platform, demilitarized, mobility, physical resources, and authorization and trust zones; see the left side of Figure 2. The *vertical enterprises zone* consists of CPS service providers' (SP) services and their service cloud systems targeted to support domain/sector/business specific services of individual SP. The *IoT platforms zone* consists of horizontal service platforms, their components, and cloud systems of platform providers, which can be applied in multiple domains/sectors/businesses in vertical enterprises zone. The *demilitarized zone* contains Internet type of networks, which can be open or limited for special use only. The *mobility zone* consists of services of mobile access/connectivity providers such as mobile telecom operators. The *physical resources zone* includes all the physical CPS entities (devices) that are able to bind the physical world with the virtual world clouds. Such entities may need gateway capabilities towards the mobility zone, operation over the Internets/Intranets, operation with the clouds/virtual means of IoT platforms, operation with vertical SP, operation with the local networks of physical devices, and operation with access and authorization systems. The *authorization and trust zone* consists of horizontal service providers that are especially focused on providing services of authorized access control and trust to all the other stakeholders in the other zones. The zone-based conceptual architecture of CPS systems captures huge variety in the CPS value networks in a very simple structure relying on a horizontal approach [12]. The contribution of this article, called *trustworthy communication hub for cyber-physical systems*, is depicted in the middle and right side of the Figure 2, and overviewed in the following.

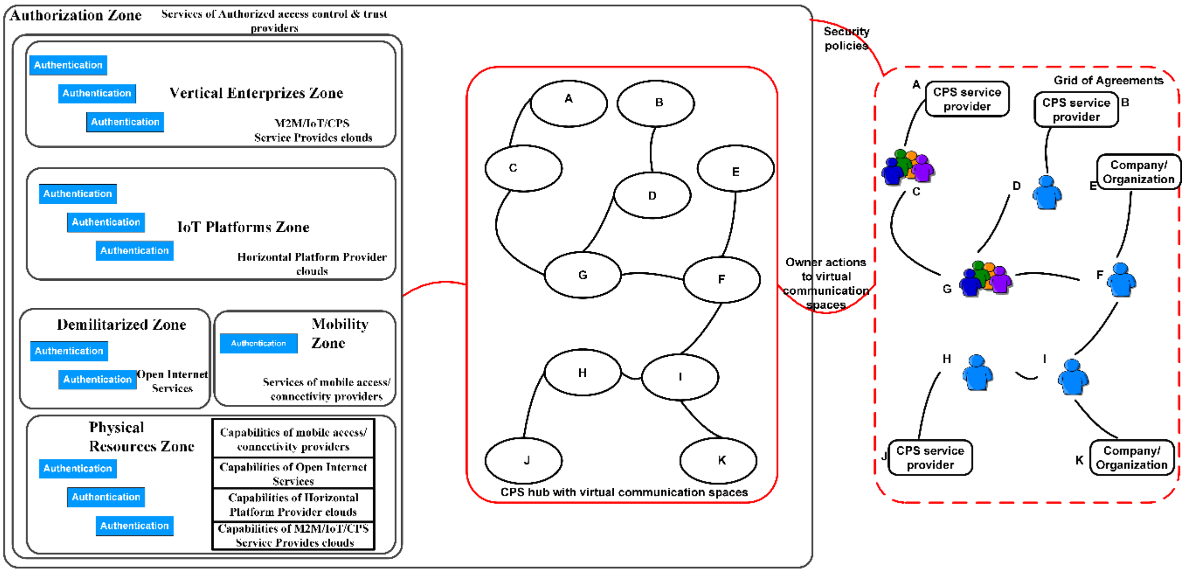

Authorization Zone
Services of Authorized access control & trust providers
Authentication
Authentication
Vertical Enterprizes Zone
Authentication
M2M/IoT/CPS Service Provides clouds
Authentication
Authentication
IoT Platforms Zone
Authentication
Horizontal Platform Provider clouds
Demilitarized Zone
Authentication
Authentication
Open Internet Services
Authentication
Mobility Zone
Services of mobile access/ connectivity providers
Physical Resources Zone
Authentication
Authentication
Authentication
Capabilities of mobile access/ connectivity providers
Capabilities of Open Internet Services
Capabilities of Horizontal Platform Provider clouds
Capabilities of M2M/IoT/CPS Service Provides clouds
A
B
C
D
E
G
F
H
I
J
K
CPS hub with virtual communication spaces
Security policies
Owner actions to virtual communication spaces
Grid of Agreements
A
CPS service provider
CPS service provider
B
C
D
E
Company/ Organization
G
F
H
I
J
CPS service provider
K
Company/ Organization

Figure 2. Conceptual model of trustworthy communication hub for cyber-physical systems.

The right side of the Figure 2 represent an example view of the relationships between owners of physical CPS resources (devices). An owner can be an individual person, a group of people, or an organization, who may have agreements between each other. For example, person D has an agreement with CPS service provider B and with the group of people G, which can be, for example, family of person D. The natural needs of each owner are to control the *access*, *usage* of his/her/is own the *physical CPS resources (devices)*, and the *exposed information*. Today, there are multiple vertical CPS SPs providing services for the owners; however, there is no proper means for the owners to referred control process. The CPS hub has been developed to enable the referred control process for the owners. In the CPS hub solution, each owner is expected to have their own communication space, representing the owner in a virtual world. The communication space acts on behalf of the owner to link and represent the services, networks, contents, and physical CP resources (devices) of the owner in the virtual world. The security policies of the owner are used to define the rules for the *access*, *usage* of the resource, and *exposed information.* The referred security policies of a specific owner are inherently the same for all the stakeholders in all the zones; therefore, the horizontal services of authorization and trust zone are envisioned to be useful for all stakeholders in the CPS value chains.

3.2. Structure and Operation of CPS Communication Space

An example of the logical structure of a CPS communication hub is depicted in Figure 3. Each owner has a virtual communication space, represented as a colored oval in the dashed rounded rectangle in the middle of Figure 3. The dashed green lines represent the related ownership relations, for example, person X owns the blue virtual communication space. The physical CPS resources (e.g., devices, server) of a specific owner register their presence in the communication space (green lines). For example, the devices and server of company A can register in the white communication space. The red lines connecting virtual communication spaces represent agreements between the owners. The referred agreements are negotiated online between the resources of the owners via the communication spaces. The blue, black, and orange lines represent the example information flows. The main operation processes related to the referred information flows are *presence management of the physical CPS resources* (green lines), *information sharing* (black lines), and *data plane operation* (orange line). The operation of physical CPS resources and trust checking with CPS communication spaces represent the key enablers of the CPS hub, which are described in the following sections.

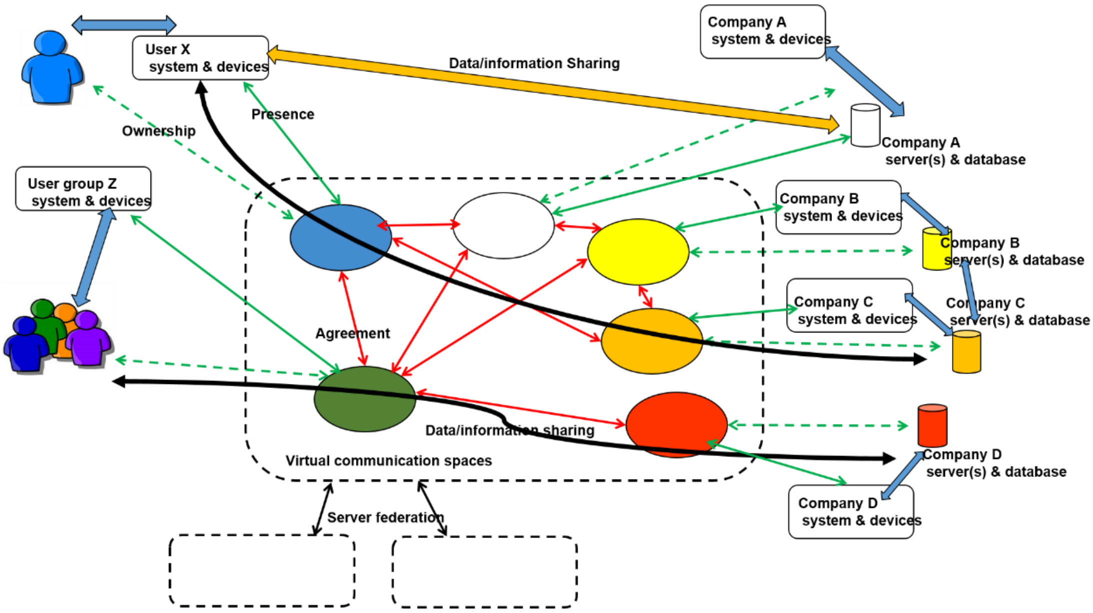


Figure 3. An example logical structure of a CPS communication hub.

3.3. Trust Checking with CPS Communication Spaces

The basic structure of the trust checking with CPS communication spaces is depicted in Figure 4. The CPS devices are usually tightly coupled with the service provider cloud systems, and each of them has their own allowed users (customer) base; see the upper part of the Figure 4. Accordingly, each user/owner makes a separate authentication with each SPs' service cloud system and related resources. This is usually the state-of-the-practice in the CPS/M2M service sector today in vertical enterprise zone. However, this is not enough, because there is a need for smart, trustable, secure, and interoperable communications across CPS systems for the owners of the resources. As the solution, it is proposed here that the CPS communication spaces establish the trustworthy grid of communicating stakeholders and entities; see the lower part of Figure 4.

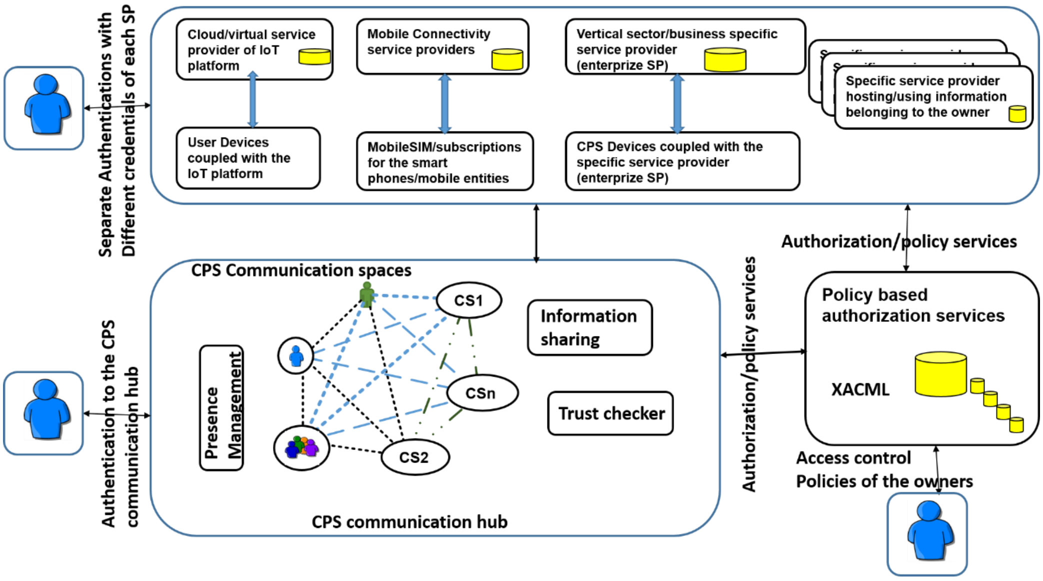

Separate Authentications with Different credentials of each SP
Cloud/virtual service provider of IoT platform
Mobile Connectivity service providers
Vertical sector/business specific service provider (enterprise SP)
Specific service provider hosting/using information belonging to the owner
User Devices coupled with the IoT platform
MobileSIM/subscriptions for the smart phones/mobile entities
CPS Devices coupled with the specific service provider (enterprise SP)
Authorization/policy services
CPS Communication spaces
CS1
CSn
CS2
Presence Management
Information sharing
Trust checker
CPS communication hub
Authentication to the CPS communication hub
Authorization/policy services
Policy based authorization services
XACML
Access control Policies of the owners

Figure 4. Trust checking with CPS communication spaces. IoT, Internet of Things; SP, service provider.

Each stakeholder needs to be authenticated with separate credentials to the CPS communication hub, and have a specific virtual communication space there. In addition, each stakeholder needs to describe their own security policies in the policy based authorization framework relying on, for example, XACM [22–25]. These security policies can then be applied by the SPs via authorization policy services, which enables consideration of the requirements of the owners. The authorization policy services need to be reliable and common for all the SPs, including CPS communication hub, in order to achieve smart cross domain/SP services for users/owners. The CPS communication hub takes care of the presence management, establishment and maintenance of the communication spaces with their trustworthy relationships, and information sharing with trust checking. The role of the trust checker is to ensure that the required information subscription is in line with the current relationship of the stakeholders and their authorized policies. The required information delivery can happen only if both the relationships and policies allow it.

3.4. Physical CPS Entities with CPS Communication Spaces

The operation of physical CPS entities (i.e., device systems, resources) is challenging today, because they usually need to interoperate with all the zones of the system when interacting with the information services of cyber world; Figure 2. For example, a mobile CPS device needs to get access over the radio access systems (mobility zone) into the Internet (demilitarized zone) to be able to interact with service platforms (IoT platforms zone) and/or specific SPs (vertical enterprises zone), so that the all authentications with the related stakeholders are successfull. This is particularly challenging because the physical CPS resources are very heterogeneous, ranging from big machines and vehicles to constrained wearable low power mobile devices, and sometimes a gateway structure is needed, like clarified in Figure 1.

The operation of physical CPS entities with CPS communication spaces has two options; Figure 5. A physical CPS entity can be attached to the CPS communication hub directly (option 1) or indirectly via the enterprise SP cloud (option 2). The direct attachment requires that the physical CPS entity can be programmed to contain the *connector of the CPS communication hub* with information of the owner of the device, address of the hosting CPS hub and required owner credentials for authentication with CPS hub. Let us assume that we classify the devices based on who chooses the set of tasks embedded in the device—the manufacturer (Class I), the service provider (Class II), or the user (Class III) [26]. When applying this classification, the direct attachment option looks most relevant for Class III devices or devices operating via the Class III gateway.

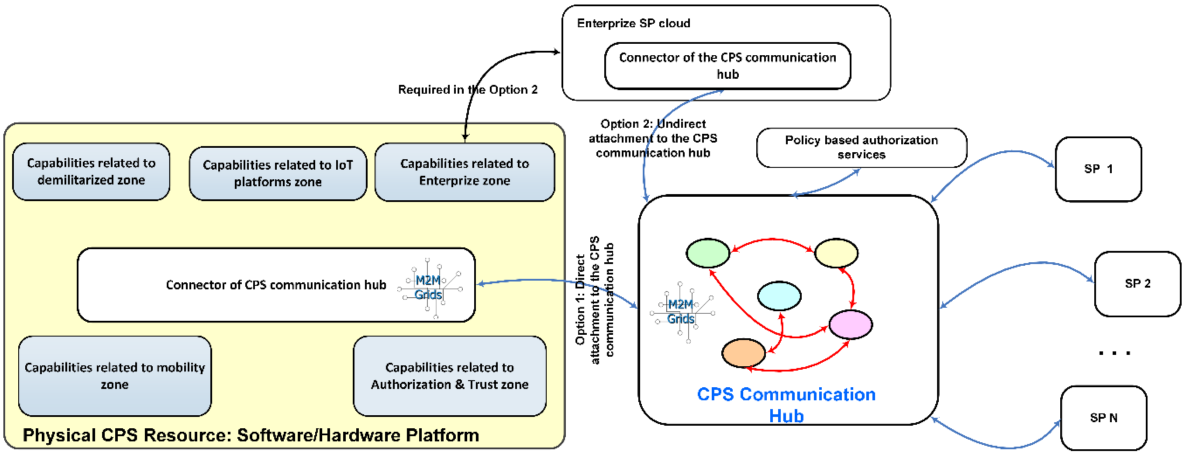

Enterprize SP cloud
Connector of the CPS communication hub
Required in the Option 2
Option 2: Undirect attachment to the CPS communication hub
Policy based authorization services
SP 1
SP 2
. . .
SP N
Capabilities related to demilitarized zone
Capabilities related to IoT platforms zone
Capabilities related to Enterprize zone
Connector of CPS communication hub
M2M Grids
Option 1: Direct attachment to the CPS communication hub
M2M Grids
Capabilities related to mobility zone
Capabilities related to Authorization & Trust zone
Physical CPS Resource: Software/Hardware Platform
CPS Communication Hub

Figure 5. Capabilities of physical CPS resources and options for operation with CPS communication spaces.

The indirect operation model looks better for the Class I devices, into which the manufacturer usually programs the address of the hosting SP (usually the manufacturer) parameters. The same is true for the Class II devices, where the service provider parameters have been programmed into the devices. In these cases, the indirect operating model requires that the enterprise SP cloud apply the connector of the CPS hub on behalf of the device and the owner.

Some of the CPS devices are constrained in terms of memory and power capabilities. Usually, they require special optimized operation capabilities to enable feasible collaboration with the related enterprise SP cloud. In these cases, the indirect operating model works better, because the manufacturer usually knows better how the referred optimization shall be done. However, when a separate programmable gateway capabilities/device can be applied, then the direct operating model could also be possible. In such a case, the connector of the CPS hub operating on behalf of the owner is needed in the gateway. In addition, some of the CPS devices could be programmable, for example, via application of virtualization/programmable operation capabilities. In that case, direct operating model could be also applied for Class I or Class II devices, if the manufacturer/enterprise SP allows such programmable operation.

4. Building Blocks of the CPS Communication Hub

4.1. Trust Process

An essential element related of the CPS hub from the owners' point of view is the trustworthiness. It refers here to all the capabilities required for ensuring trustability of the physical and logical resources, exposed information and their application under control of the owner. The basic trust enabling procedures in the CPS hub are shown in the Figure 6, and clarified in the following.

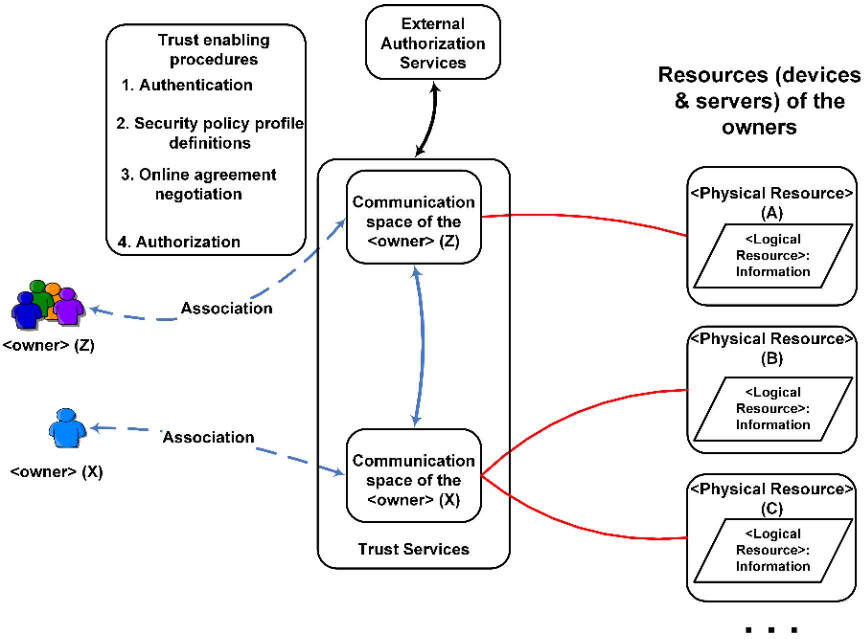

Trust enabling procedures
1. Authentication
2. Security policy profile definitions
3. Online agreement negotiation
4. Authorization
External Authorization Services
Resources (devices & servers) of the owners
Communication space of the <owner> (Z)
Communication space of the <owner> (X)
Trust Services
Association
Association
<owner> (Z)
<owner> (X)
<Physical Resource> (A)
<Logical Resource>: Information
<Physical Resource> (B)
<Logical Resource>: Information
<Physical Resource> (C)
<Logical Resource>: Information
. . .

Figure 6. Trust services of CPS hub.

Mutual *authentication* is required in order to identify and bind the owner with the related communication space in the CPS hub. Authentication is also required to bind the physical and logical resources (e.g., servers and device resources) of the owner into the communication space of the owner. When an SP is an owner, its back-office services system may be a resource in the SP communication space. Such a resource, the back-office service system of the SP, usually also has specific authentication relying on its own allowed user space. It is obvious that a separate authentication is required between the referred resource of the SP and the customers of the SP.

The *security policies (profiles)* of the owners related to the access, use of their physical and logical resources, and the exposed information need to be *defined* by the owner. The policy definitions may include, for example, rules according to which the access to the resources of the owner may be allowed for the other parties. Such rules may include conditions related to, for example, situation, time, environment, and level of trustworthiness, among others.

The capabilities for creation and maintenance of online trust and value exchange relationships between the owners are required for keeping the grid of agreements in "real-time" according to the dynamic relationship situation (*online agreement negotiation).*

Authorization refers to the process for formally ensuring the identity of the owner/user access control rights for the stakeholder in the authentication, security policy profile definition, online agreement negotiation, and in the use of physical/logical resources.

The physical resources (A–C ...) shown in Figure 6 can be any physical resource, embedded device/product and, for example, a server, which is owned by a single company ("owner"), CPS service provider (SP). Such a server of the SP usually has its own authentication and authorization services to ensure that only their customers have access to the services that their server provides. A specific owner may be a customer of many SPs and, therefore, multiple authentication and authorization processes are required for enabling trustworthiness.

4.2. Presence Management

The need for presence management arises from the inherent characteristics of physical CPS asset devices and services (resources) to be online or offline at any given time. The reasons for being offline may be related, for example, to power sources, unreliable communication links, mobility, or the user/owner needs. When such a resource needs to be reachable via communication networks, it should register its presence into a known place. According to our approach, such a place is the virtual communication space of the resource owner.

When speaking about resources, an essential problem to be solved is related to identities and addressing. There are several solutions for identities in different levels of the systems. For example, medium access control (MAC) addresses are in use in the radio access level, Internet protocol (IP) addresses, and Uniform Resource Locator URLin Internet/Web contexts, service provider specific addresses in enterprise systems, and e.g., Universally unique identifier (UUID) to identify resources have been proposed, among others. Here, identities and addressing refer to the ones used at the communication level, more specifically in the communication overlay level and especially related to the concept of virtual communication space.

The problems for the identities and addressing in the communication overlay level arise from the mobility, use of local identities, dynamic presence, and topics of shared information. Local identities and addressing, such as IP and physical level addresses, may be temporal; therefore, more reliable ways for identifying resource owners and the resources themselves are needed. Basically, the generally applied "scheme:[//host[:port]][/path]" could be applied; however, it lacks references to the ownership of resources. Therefore, identities and addressing for virtual communication spaces at the communication overlay level are specified using the following notation:

<owner>@<domain.server>/<physical resource>/<logical resource> (1)

where

- <*owner*> denotes the resource owner;
- The home domain of the owner is <*domain.server*>;
- <*physical resource*> refers to a physical resource, which can typically be, for example, embedded devices, gateways, or servers;
- The optional part <*logical resource*> can refer to any specific information content, or to logical resource tree of the information or, for example, a semantic Web type of resource.

4.3. Trustworthy Information Sharing Process

The information sharing process requires preceding creation of trust relationship/agreements between owners of the physical resources, the presence of the resources in the communication spaces of the owners, and enabling basis for trustworthiness. The information sharing of the CPS hub relies on the publish/subscribe paradigm, because in the CPS system, there are typically multiple and a variety of numbers of potential consumers for a single source of information [7].

The sharing of information contains the following phases; Figure 7. The first phase connects the owner to the CPS communication hub, authentication of the owner, and registration of the presence of the physical resources of the owner into the home domain of the owner. As the result of this step, the presences of the physical resources are registered in the communication spaces of the owner in the CPS communication hub. The referred resources can be identified by <owner>@<domain>/<resource> notation.

In the second phase, some resource may subscribe to receive information published by some other resources. The publish/subscribe service requires a separate authentication done using the same owner identity to the CPS information sharing service as that applied in step 1. The published/subscribed information is identified by notation <owner>@<domain>/<resource>/<topic>. Any resource can publish information according to its own strategy, if the authentication has been done in a successful manner. However, when a resource subscribes for information published by other owners/resources, then the trust service checks whether it is allowed or not.

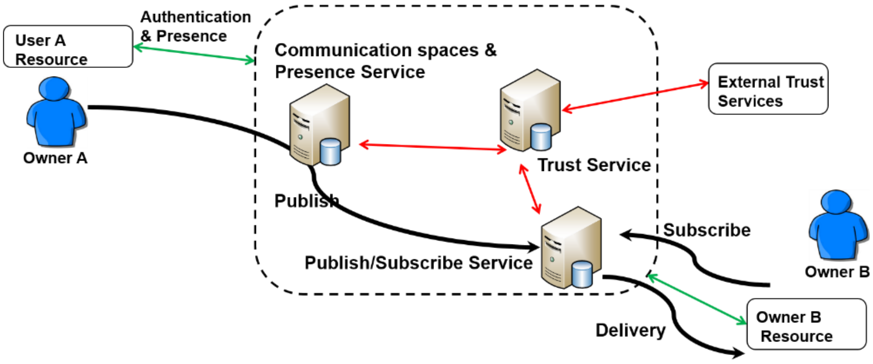


Figure 7. Information sharing of CPS communication hub.

In the third phase, the CPS trust service checks the status related to the agreements between the owner (A), which is publishing the information, and the other owner (B), which wants to subscribe to the information published by A. If there is an agreement between A and B, then the subscribed information may be delivered to the subscriber B. However, before the delivery, the security policies of the owner are checked by the CPS trust service using an external policy-based authorization service.

Let us assume that the <owner> (Z) has a <physical resource> (B), which wants to subscribe the <logical resource> information that is published by the <physical resource> (A), which belongs to the <owner> (X), Figure 8. The respective information-sharing algorithm is represented in Figure 9.

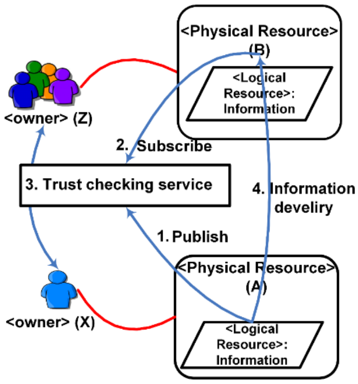


Figure 8. Information sharing process.

1. *The <physical resource> (A) may be publishing the <logical resource> (information of A) every now and then. The identity of the published information is X@<domain>/A/information-of-A.*
2. *The <physical resource> (B) (Z@<domain>/B) send subscribe request related to the referred X@<domain>/A/information-of-A.*
3. *The trust checking services checks the following issues*

a) *Mutual agreement situation between the <owners> of resources (A and B) i.e. X (X@<domain>) and Z (Z@ <domain>).*
b) *Access control policy defined by the <owner> (X) related to the publishing of the X@<domain>/A/information-of-A to the Z@<domain>/B in the current situation.*
c) *If the checks 3. (a) or 3. (b) do not allow the publishing, then the subscribe of <physical resource > (B) of the <owner> (Z) i.e. (Z@<domain>/B) is rejected, and any information delivery cannot happen.*
d) *If the checks 3. (a) or 3. (b) allows the publishing, then the subscribe of Z@<domain>/B is approved.*

4. *If 3. (d) matches, then the delivery of <logical resource> (information from the <physical resource> (A) to <physical resource> (B) can be executed, i.e. X@<domain>/A/information-of-A can be delivered to Z@<domain>/B according to the subscription.*

Figure 9. Information sharing algorithm.

4.4. *Data Plane Operation Process*

The sharing of information using data plane negotiation capability is clarified in this section (see also the orange arrow in Figure 10). The basic operation is divided to control plane and data plane functions. It is expected that the physical resources first execute the registration of their presence into the virtual communication space of the owner as a control plane function. After that, the owners need to execute the trust checking process including mutual agreement and checking of the access control policies, otherwise no interaction can happen between the physical resources of the referred owners. These are also a control plane function. After such an agreement has been created, then any resource of the owners can interact/exchange messages between each other, as clarified earlier.

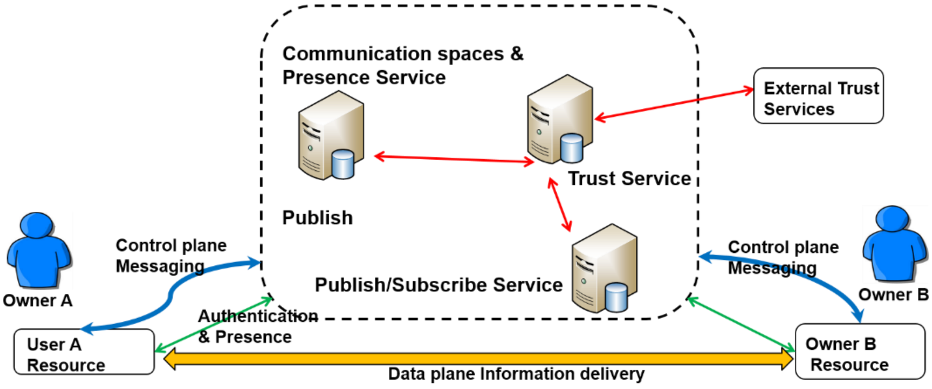


Figure 10. Data plane of CPS communication hub.

If the information exchange via the CPS communication spaces is not enough efficient, for example, in the case of multimedia delivery or enterprise specific means is required to be used, then data plane operation can be a possibility. The data plane operation can be activated by executing so-called "M2MGrids negotiation", where the applied data plane communication channel is negotiated as the control plane action first. This negotiation can happen between any two individual physical resources that have passed all the control plane actions clarified earlier. On the basis of the "M2MGrids negotiation", the used end-to-end data plane format/protocol can be defined by the resources themselves. After the "M2MGrids negotiation" has happened, the interaction between referred physical resources can happen, as the data plane functions directly without any involvement of the communication spaces related network/control plane processing using the agreed data plane means.

4.5. Attachment of Physical CPS Resources

The attachment of physical resources to the CPS hub can be either direct or indirect, as clarified in Section 3.4. Let us have a look at some physical resources of the traffic accident case; Figure 11. In the experimental case, the direct attachment of the Polar smart watch was applied using a smart phone as a gateway. The embedded CPS hub connector enabled the communication with the virtual spaces of Polar in the CPS hub; green oval in Figure 11. While, for example, the Tracker dog collar applied the indirect method for communication with the CPS hub. The reason for this was the specialized optimized communication between the collars and the Tracker router and service cloud. A specialized gateway with the CPS hub connector was applied to register the presence of collars to the CPS hub. In this way, the presence of all the online collars in the Tracker service cloud could be registered in the CPS hub. However, the scalability of the experimental CPS hub services was found to be a challenge in this case. The indirect attachment methodology was also applied with the Bittium medical Electroencephalography (EEG) sensor, IMEC CO_2 sensor, and Valopaa street illuminator in the traffic accident case.

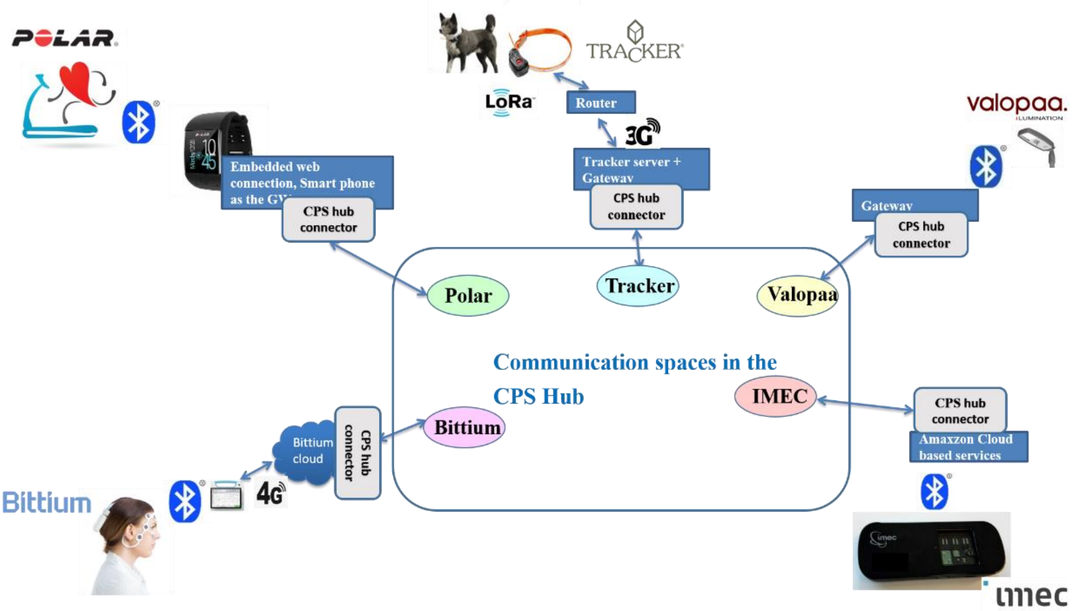


Figure 11. Example attachments of physical CPS resources to the CPS hub.

5. Solutions of the CPS Communication Hub

5.1. Services of the CPS Hub

An experimental realization of the CPS communication hub services are communication spaces and presence services, information services, and trust services; Figure 12. The realization of communication spaces and presence services relies on the application of presence and contact list management related features of extensible messaging and presence protocol (XMPP) technology [8,9]. The information sharing services relies on the application of publish/subscribe capabilities of message queue based telemetry transport (MQTT) protocol [13,14]. The trust services rely on the contact list management related features of XMPP, capabilities to define access control policies with eXtensible access control markup language (XACML) [22], and external authorization services; Safax [23]. The experimental realization of the referred services is clarified in the following sections.

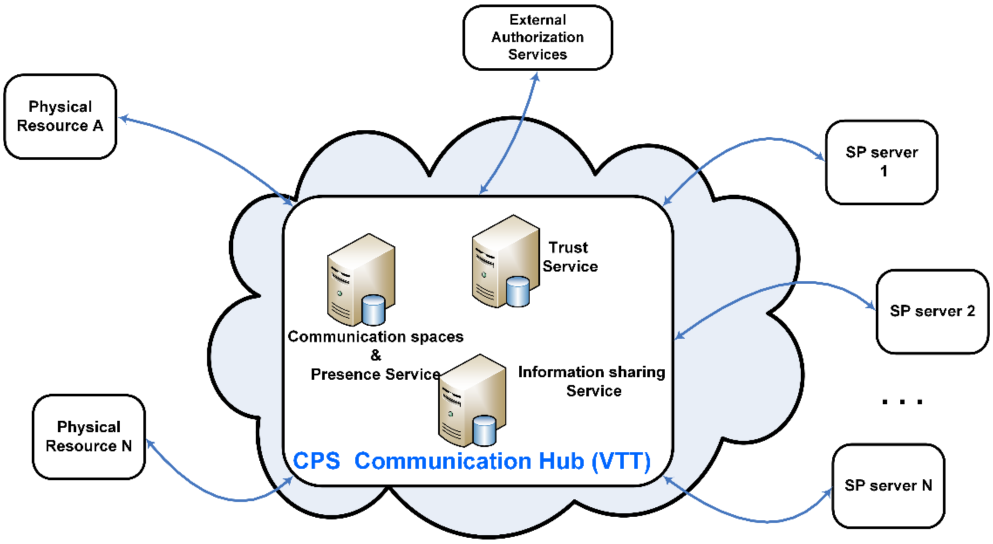

External Authorization Services
Physical Resource A
SP server 1
Trust Service
SP server 2
Communication spaces & Presence Service
Information sharing Service
Physical Resource N
. . .
CPS Communication Hub (VTT)
SP server N

Figure 12. Services of the CPS hub.

5.2. Communication Spaces and Presence Services

The realization of communication spaces and presence services relies on the distributed hybrid peer-to-peer (P2P) architecture model enabled by XMPP technology. At the architecture level, it enables client to server communication, server-to-server communication called server federation, and client-to-client communication. The main supported services include, for example, support for presence management, secure messaging (TLS), overlaid communication over IP, near real-time messaging, authentication, contact list management, and service discovery. The key applied capabilities from the XMPP technology in the CPS hub are physical presence, access, contact lists, and server federation.

Initially, the administrator of the CPS hub makes the communication spaces for the users/owners of the physical resources (devices/servers) by making them accounts with the CPS hub server. After this step, each of the owners has a communication space in which the physical resources owned by the user can be registered. The communication spaces and presence services of the CPS hub assume that there is an XMPP client embedded in the physical resources. Such a client connects the physical resource to the server who is hosting the virtual communication space of the owner. The procedure, clarifying how a client in a physical resource connects into the communication spaces server, is visualized in the Figure 13.

First, the server address is discovered by a domain part as a server address or discovering server address with Service record (SRV) lookup from Domain Name Service (DNS). The XMPP client embedded in the physical resource must establish a XMPP session with the XMPP server that is hosting the virtual communication space of the owner. The minimum parameter set for the session establishment contains a valid XMPP account identified by XMPP ID (JID) and a password, which are used for the authentication between the resource (client) and CPS hub (server). JID consists of a username, server, and resource parts, that is, part of the notation 1 clarified in Section 4.2, *<owner>@<domain.server>/<physical resource>*. Every client connects to his or her home domain server specified by his or her JID.

The connections are established over TCP and optionally encrypted by the transport layer security (TLS) layer (recommended). An administrator of a domain may specify that encryption is mandatory and it is up to administrator or designer to choose whether or not TLS certificates shall be checked. Most client libraries accept self-signed certificates in client-to-server connections. The authentication can be carried out relying on a simple authentication and security layer (SASL) [27,28], relying on the use of TLS.

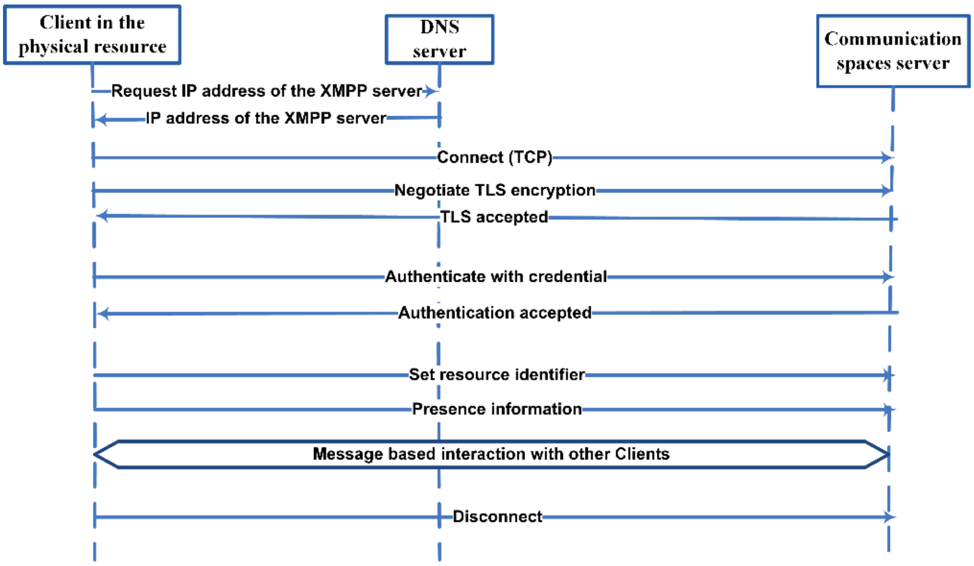

Client in the physical resource
DNS server
Communication spaces server
Request IP address of the XMPP server
IP address of the XMPP server
Connect (TCP)
Negotiate TLS encryption
TLS accepted
Authenticate with credential
Authentication accepted
Set resource identifier
Presence information
Message based interaction with other Clients
Disconnect

Figure 13. Connecting and presence registration of the physical resources. XMPP, extensible messaging and presence protocol; TLS, transport layer security.

XMPP supports per-hop channel encryption using transport layer security (TLS) through a STARTTLS upgrade mechanism [10]. Per-hop encryption using TLS can be used to protect only messages transmitted between the client and the server, or messages transmitted between servers, but not inside servers that do the routing. TLS has been used mainly in client-to-server communication, and server-to-server communications are usually not encrypted. Mechanisms such as OpenPGP, off-the-record (OTR), TLS, Secure/Multipurpose Internet Mail Extensions (S/MIME), SIGMA, XML encryption, and Cryptographic Message Syntax (CMS) with JOSE to enable end-to-end encryption between two clients exist, but none of them has been deployed widely [10].

Just after an XMPP session is established, the XMPP client of physical resource should also send the information of its presence to the XMPP server. The presence information will be stored in the roster of the owner, and used by the other physical resources of the same owner. However, when another owner wants to use the presence information of the owner, it is required that the owners need to first have a mutual agreement (“trust” relationship), before the presence information of their physical resources can be shared.

5.3. Trust Services—Mutual Agreement Negotiation

The negotiation of the mutual trust relationship, *agreement*, between the owners, was realized by application of the XMPP contact “buddy” list management capability in the CPS hub. Using the “buddy subscription” means, each owner can decide which other users/owners are accepted to be included into the “buddy list” of the owner. When the owners have approved each other into their buddy lists, their identifiers are stored into the rosters of the owners in the CPS hub. Then, we can say that the mutual trust relationship, *agreement*, between the owners has been established. The owners of the physical resources can control the contact list management dynamically, which enables realization of the grid of agreements concept.

After such an agreement has been created, any resource of the owners can interact/exchange presence information between each other. For example, if company A and company B agree to such trust relationship between their communication spaces, then, for example, companyB@<domain>/server can get information about the presence of companyA@<domain>/deviceA, and vice versa. Otherwise, any information about the presence of the physical resources of the referred owners cannot be shared.

The related XMPP buddy subscription procedure is visualized in Figure 14. First, the XMPP connect, authentication, and presence registration process is executed.

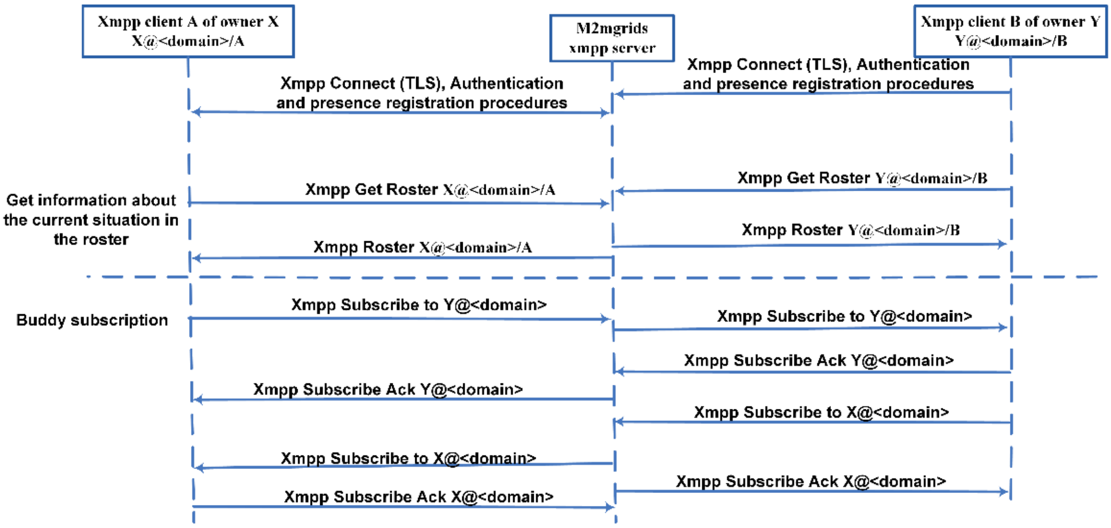

Xmpp client A of owner X
X@<domain>/A
M2mgrids
xmpp server
Xmpp client B of owner Y
Y@<domain>/B
Xmpp Connect (TLS), Authentication
and presence registration procedures
Xmpp Connect (TLS), Authentication
and presence registration procedures
Get information about
the current situation in
the roster
Xmpp Get Roster X@<domain>/A
Xmpp Get Roster Y@<domain>/B
Xmpp Roster X@<domain>/A
Xmpp Roster Y@<domain>/B
Buddy subscription
Xmpp Subscribe to Y@<domain>
Xmpp Subscribe to Y@<domain>
Xmpp Subscribe Ack Y@<domain>
Xmpp Subscribe Ack Y@<domain>
Xmpp Subscribe to X@<domain>
Xmpp Subscribe to X@<domain>
Xmpp Subscribe Ack X@<domain>
Xmpp Subscribe Ack X@<domain>

Figure 14. XMPP buddy subscription.

During that process, the availability of the clients' (resources) in their owners' rosters are registered. Afterwards, an XMPP client can ask the roster for its content from the server, and get information on the currently accepted other users stored in the roster of the owner (buddy list of the owner). If the required communication party is not yet in the buddy list, an XMPP client can activate the buddy subscription procedure to get acceptance from the other party for the communication. Thus, in the buddy subscription, the XMPP client that wants to communicate with resources owned by some other user subscribes to the access from the other user (XMPP subscribe message). If the other user wants to give access to the requestor, it accepts the subscription (XMPP subscription Ack message). The same procedure can be executed in both directions. After that, the related owners (X and Y in Figure 14) have made a kind of agreement so that they can communicate with each others' resources. The resources themselves may also have additional security-related procedures required to enable the use of the referred resources.

5.4. Information Sharing Services

The CPS/M2M system needs to deliver information from one to one (1–1), but also from one to many (1–N). Therefore, the CPS hub relies on the publish/subscribe paradigm in the information sharing. For example, XMPP technology has such a publish/subscribe mechanism, which is based on the concept of specific entity called "pubsub" node [10–12]. Such a "pubsub" node acts in a way as the publish/subscribe service established to work in the XMPP server. After that, the publisher can publish information into the "pubsub" node and a subscriber can subscribe to information from it. A subscriber can subscribe to information and receive notifications, if the subscriber is authorized to access the published information. However, the referred XMPP-based publish/subscribe means have proved to be quite complicated. Therefore, the information sharing service of the CPS hub relies on slightly more simple solutions for the publish/subscribe capabilities of MQTT [8,9].

It is essential to have some common identities for the information, so that the entities know what information the other entities are publishing. MQTT provides a possible way for such an identification by defining the concept of "topic" name, which could be applied as the name for the shared information. However, MQTT seems not to have the proper capabilities to define the owners and their physical resources in a simple way. Therefore, the CPS hub applies XMPP and its identities (JID) approach for this purpose. The selected parameters for the MQTT-based publish/subscribe services are clarified as follows:

$$\text{Username: } < \text{owner}>@<\text{home.domain}> \tag{2}$$

$$\text{Topic name of MQTT: <Username>/<physical resource>/<logical resource>/<sub logical resource>/} \ldots \quad (3)$$

where

- Username, < *owner*>@<*home.domain*> is the same as the XMPP identifier, JID;
- <*physical resource*> refers to a physical resource, which can typically be, for example, an embedded device, gateway, or server;
- <*logical resource*> refers to specific information content "topic", or logical resource tree of the information;
- <*sub logical resource*> refers to the child information elements of the logical resource.

The basic operation of the MQTT-based publish/subscribe services is visualized in Figure 15. First, the MQTT clients of the resources need to connect to the MQTT broker of the CPS hub using the defined username and password for authentication. After that, a MQTT client can subscribe to the selected topic, which is published by another MQTT client.

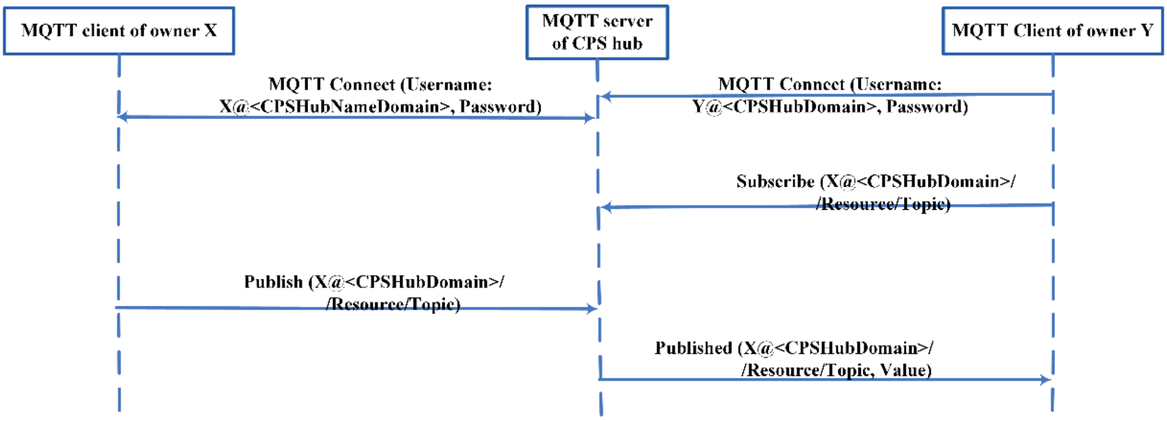

MQTT client of owner X
MQTT server of CPS hub
MQTT Client of owner Y
MQTT Connect (Username: X@<CPSHubNameDomain>, Password)
MQTT Connect (Username: Y@<CPSHubDomain>, Password)
Subscribe (X@<CPSHubDomain>/ /Resource/Topic)
Publish (X@<CPSHubDomain>/ /Resource/Topic)
Published (X@<CPSHubDomain>/ /Resource/Topic, Value)

Figure 15. Information sharing using the publish/subscribe service of the CPS hub.

However, the delivery of the information ("Published" in Figure 15) cannot happen like in the basic operation. This is because it is not known whether the owner allows delivery of the information to the subscriber in the current situation with the agreements and security policy of the owner. Instead, the trust checking services need to be executed at the latest before the delivery of the information to the subscriber.

5.5. Trust Checking Services for the Information-Based Interaction

The trust checking service is required in order to ensure that information and use of resources are allowed only for the authorized parties, and nobody else. The trust checking procedure of the CPS hub is visualized in Figure 16, and shortly clarified in the following.

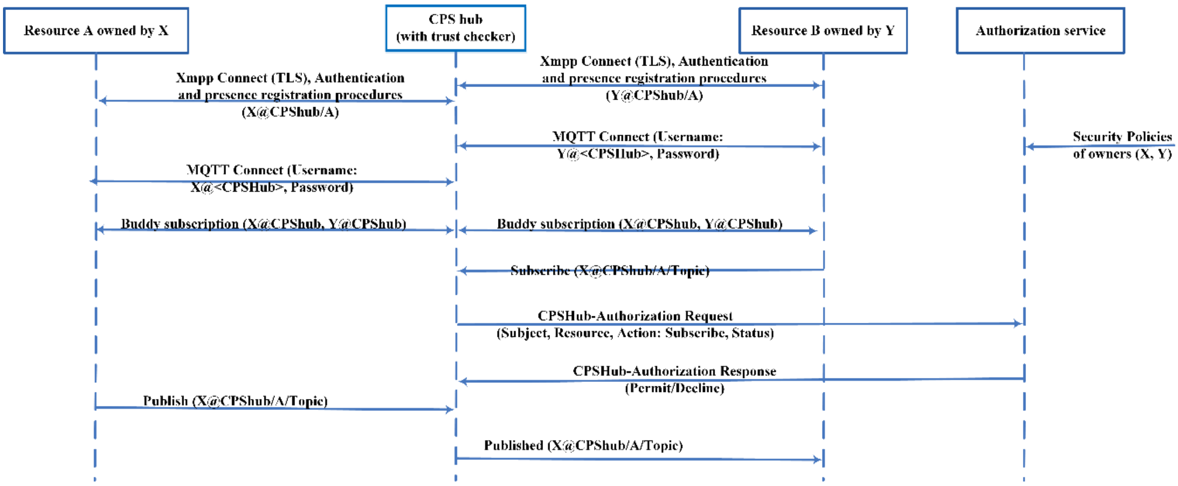

Resource A owned by X
CPS hub (with trust checker)
Resource B owned by Y
Authorization service
Xmpp Connect (TLS), Authentication and presence registration procedures (X@CPShub/A)
Xmpp Connect (TLS), Authentication and presence registration procedures (Y@CPShub/A)
MQTT Connect (Username: Y@<CPSHub>, Password)
Security Policies of owners (X, Y)
MQTT Connect (Username: X@<CPSHub>, Password)
Buddy subscription (X@CPShub, Y@CPShub)
Buddy subscription (X@CPShub, Y@CPShub)
Subscribe (X@CPShub/A/Topic)
CPSHub-Authorization Request (Subject, Resource, Action: Subscribe, Status)
CPSHub-Authorization Response (Permit/Decline)
Publish (X@CPShub/A/Topic)
Published (X@CPShub/A/Topic)

Figure 16. Trust checking procedure of the CPS hub.

The first step connects the owners to the CPS hub, authentication of the owner, and registration of the presence of the physical resources of the owners. These procedures shall happen as clarified in the Section 5.2 and Figure 13 (XMPP connect), and Section 5.4 and Figure 15 (MQTT connect). After this step, the presence of the physical resources (X@CPShub/A, Y@CPShub/B) is registered as resources of the communication spaces of the owners (X@CPShub and Y@CPShub) in the CPS hub. As a result, the trust checker of the CPS hub knows the identities and presence of the referred resources.

In the second step, the trust relationship between the owners (X@CPShub and Y@CPShub) is created using the "buddy subscription" procedure; see Section 3.3 and Figure 14. In the case of Figure 16, a resource of the party (X@CPShub/A) subscribes to the acceptance from the other party for the communication with its resource (Y@CPShub/B). If the acceptance agreement is approved by Y, then the procedure is also executed in the other direction. After successful execution of the referred buddy subscription, the related owners (X and Y in Figure 16) have made an agreement that they can interact with each others' resources. As the result, the trust checker of CPS hub has real-time information on the status of agreements between parties, the *grid of agreements.*

In the third step, a resource (Y@CPShub/B in the case of Figure 16) subscribes to the information published by some other resource (X@CPShub/A/topic, in this example case). The resource needs to know in one way or another that X is publishing the referred kind of information ("topic") in order to enable its subscription. In addition, any resource (like X@CPShub/A, in this example case) can publish information at any time. However, when a resource subscribes to the specific information topic (X@CPShub/A/topic, in this example case), the trust checker will check whether or not the delivery of the information content is allowed for the subscriber. The trust checker of the CPS hub will perform the check based on all the information that it has from the preceeding steps, that is, the identities and presence of the referred resources, grid of agreements, and the level of trust-related issues. In addition, the security/access control policies of the owners (X and Y, in this case) may be checked using an external authorization service such as, for example, SAFAX [23]. For example, an owner may define that a specific information topic can be delivered to other defined owners only in specific situations, like, for example, in an alarm caused by traffic accident or so on. The access control rules defined by the owner can be quite complex, consisting of information about, for example, situation, time, information, and subscriber. As the results, the trust checker of the CPS hub is able to make a decision of whether or not the delivery of the information content is allowed for the subscriber. If the conclusion is that it is allowed, then the information (X@CPShub/A/topic, in this case) is delivered to the subscriber (Y@CPShub/B, in this case).

After the trust checking has been executed in an acceptable manner, then the resources may interact and agree separately in the applied data plane, which will be used for end-to-end interaction between the referred resources. After the data plane negotiation, the CPS hub may be bypassed from the communication chain for optimization reasons. In addition, the resources themselves usually have specific security related procedures and authorization required to enable the use of the referred resources.

5.6. Solutions for Data Plane Negotiation

The data plane negotiation is performed utilizing the XMPP protocol and services. This implies that the physical resource that is going to participate in the data plane negotiation must deploy the CPS hub connector with the XMPP client that implements the required tasks. In the following sections, the description of data plane negotiation is divided into three parts, of which the two first are preliminary steps and prerequisite for successful data plane negotiation.

5.6.1. Prerequisite Steps

Before data plane negotiation can occur, the XMPP client embedded in the physical resource must establish an XMPP session with the XMPP server that is hosting the virtual communication space of the owner. The minimum parameter set for the session establishment contains a valid XMPP account identified by the XMPP ID (JID) and a password. JID consists of a username, server, and resource parts. In the context of data plane negotiation, all three are considered mandatory, as they are needed to uniquely identify different physical devices of the M2Mgrids system.

Just after an XMPP session is established, the XMPP client of the physical resource should also send the initial presence to the XMPP server in order to express its willingness to communicate with someone else. A trust relationship is required to be created between the owners. Creation is based on XMPP's fundamental feature, called presence subscription. It is executed between two XMPP clients of physical resources belonging to different owners. Within the same owner, the trust relationship is considered to exist inherently and the presence subscription procedure need not be conducted.

Presence subscription is a two-way procedure. Both involved XMPP clients should initialize it by sending "subscribe" request to the other endpoint. The recipient of the "subscribe" request should accept the subscription by sending a "subscribed" response to the sender. If, for any reason, the subscription cannot be accepted, the recipient should send an "unsubscribed" response. In that case, the trust relationship creation fails and data plane negotiation is cancelled.

The status of the presence subscription between the two owners is maintained in the XMPP server. Actually, there are several states in which status can depend on which phases the two presence subscription procedures are in. Status "both" means the state in which both endpoints have accepted the presence subscription made by the other endpoint. In this case, the "trust" relationship has been entirely created. Any other status indicates that the "trust" relationship is not established.

The status of the presence subscription is preserved in the XMPP server even if the XMPP client of the owner disconnects from the XMPP server. The XMPP client can also check the status. If the trust relationship exists, it need not be created again. Accordingly, if two endpoints have established a trust relationship between two owners, subsequent data plane negotiations between those owners can skip this phase.

Accepting or declining the presence subscription request is based on the list of trusted JIDs. The list contains all XMPP JIDs that are trusted by the owner of the physical resource. The list contains bare JIDs, that is JIDs are in the format that contain the username and server, but does not include the resource field.

5.6.2. Data Plane Negotiation

The purpose of the actual data plane negotiation is to share information on communication-related parameters of the specific data plane protocol to be used between the physical resources. The basic operation of the data plane negotiation is depicted in Figure 17. The endpoint willing to communicate with the other endpoint, and knowing other endpoint's XMPP JID, sends a specific Data Plane Protocol request (DPP-req) to that JID. The recipient of the request then creates the response message (DPP-resp) that contains the requested information. The recipient of the request can consult trusted JID lists in verifying that the endpoint sending the request is acceptable. The request coming from an endpoint not found in the list should be discarded. Trusted list usage is recommended because, although "trust" relationship creation is required before negotiation, an endpoint can still send the DPP-req request to any JID without earlier "trust" relationship creation. Below, the endpoint sending the DPP-req is called the DPP-client, whereas the recipient is called the DPP-server. As data plane protocols may vary a lot, only the most common and generic parameters can be shared using this approach. IP address or hostname, port number, and identification of data plane protocol belong to the set that could be shared.

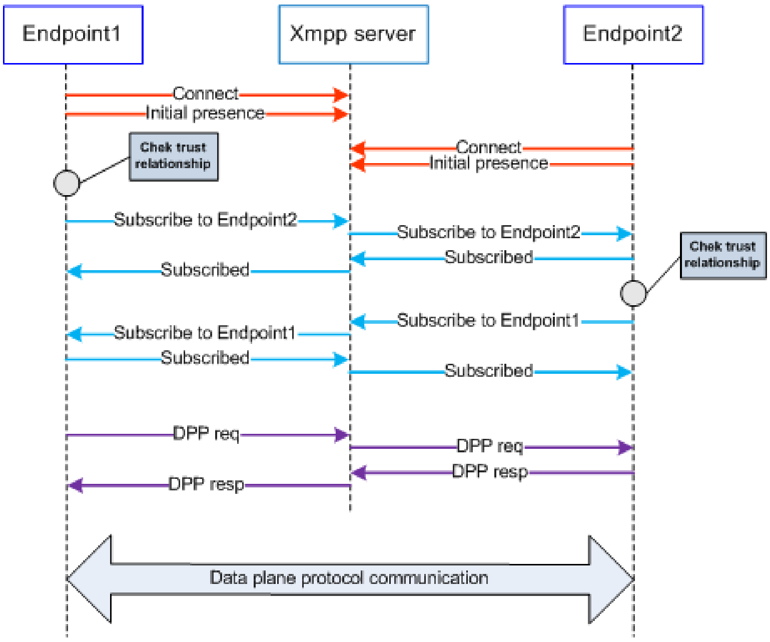


Figure 17. Data plane negotiation procedure.

Request/response implementation is utilizing XMPP message stanza and "Data Form" XMPP extension [29]. That extension is identified by XML namespace called "jabber:x:data". Fields with example values of the request message are expressed here in plain text.

msg-name DPP-req

suggested-protocol-type MQTT
Request message example described in XML format:

```
<x xmlns=’jabber:x:data’ type=’submit’>
<field type=’text-single’ var=’msg-name’><value>DPP-req</value></field>
<field type=’text-single’ var=’suggested-protocol-type’><value>MQTT</value></field>
</x>
```

By the "suggested-protocol-type" field, a DPP-client can express which protocol it is supporting and willing to use. Fields with example values of the response message are in plain text.

msg-name	*DPP-resp*
protocol-type	*MQTT*
server-ip	*130.244.94.172*
port	*1883*
status	*ACK/NACK*

The response message described in XML format is as follows:

```
<x xmlns='jabber:x:data' type='result'>
 <field type='text-single' var='msg-name'><value>DPP-resp</value></field>
 <field type='text-single' var='protocol-type'><value>MQTT</value></field>
 <field type='text-single' var='server-ip'><value>130.188.94.172</value></field>
 <field type='text-single' var='port'><value>1883</value></field>
 <field type='text-single' var='status'><value>ACK</value></field>
</x>
```

where the "protocol-type" field states which protocol shall be used, while the "Status" field is used to inform the DPP-client whether data plane protocol negotiation was successful.

5.7. Interaction between Physical CPS Resources

Let us take an example of the CPS hub deployment case showing interaction between physical CPS resources in the traffic accident case. The prerequisite steps of the case, attachments of related physical CPS resources to the CPS hub are described in Section 3.4 and Figure 11. In the example interaction, Figure 18, a smart watch of Polar, is interacting via the CPS hub with a remotely located air quality sensor of IMEC.

The solution applies bluetooth low energy (BLE) technology for interaction locally with the devices and gateways/infrastructure. The Polar smart watch is maintaining a BLE network for sensors in the BLE host role, and simultaneously acts as BLE client to the smart phone controlled BLE network. The smart phone operates as a gateway to the CPS hub. Depending on the smart watch capabilities, a gateway can act as a protocol translator, allowing the passing of messages directly to the Internet, like in this case. The gateway allows simpler and more power-efficient smart watches by reusing the existing mobile Internet connections. In this way, there is no need for additional ISP licenses/security devices/fees/maintaining.

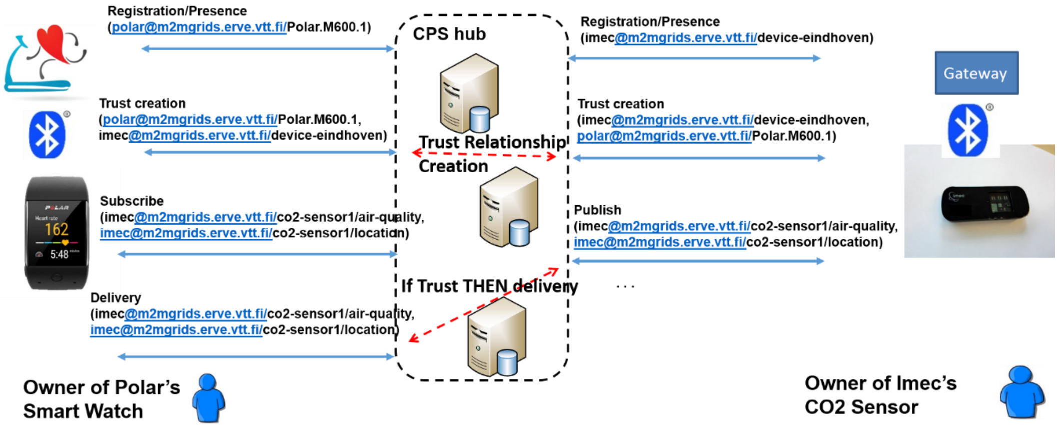

Registration/Presence
(polar@m2mgrids.erve.vtt.fi/Polar.M600.1)
Trust creation
(polar@m2mgrids.erve.vtt.fi/Polar.M600.1,
imec@m2mgrids.erve.vtt.fi/device-eindhoven)
Subscribe
(imec@m2mgrids.erve.vtt.fi/co2-sensor1/air-quality,
imec@m2mgrids.erve.vtt.fi/co2-sensor1/location)
Delivery
(imec@m2mgrids.erve.vtt.fi/co2-sensor1/air-quality,
imec@m2mgrids.erve.vtt.fi/co2-sensor1/location)
CPS hub
Trust Relationship
Creation
If Trust THEN delivery
Registration/Presence
(imec@m2mgrids.erve.vtt.fi/device-eindhoven)
Gateway
Trust creation
(imec@m2mgrids.erve.vtt.fi/device-eindhoven,
polar@m2mgrids.erve.vtt.fi/Polar.M600.1)
Publish
(imec@m2mgrids.erve.vtt.fi/co2-sensor1/air-quality,
imec@m2mgrids.erve.vtt.fi/co2-sensor1/location)
. . .
Owner of Polar's
Smart Watch
Owner of Imec's
CO2 Sensor

Figure 18. Interaction process of smart watch via the CPS hub with remotely located air quality sensor.

The IMEC air quality sensor applies bluetooth LE and a gateway for communication with the related Amazon cloud-based services. The CPS hub connector is applied in the gateway for registration and publishing CO_2 measurements to the CPS hub. The CPS hub acts as the communication intermediary realizing the communication spaces for the owners, Polar and IMEC in this example case; Figure 11.

The interaction process of the smart watch via the CPS hub with remotely located air quality sensor is shown in the Figure 18. First, registration of the presences of the devices to the CPS hub is required. The smart watch registers its presence to the Polar communication space (polar@m2mgrids.erve.vtt.fi/Polar.M600.1) and CO_2 (imea@m2mgrids.erve.vtt.fi/cp2-sensor1), respectively. Then, the trust creation process between the referred owners/resources needs to be done.

After this, the IMEC air quality sensor can start publishing the measured CO_2 level and location of the sensor. The Polar smart watch subscribes to the CO_2 level and location information of the sensor. When the information is available and the trust relationship between Polar and IMEC is present, the delivery of the CO_2 level and location information of the sensor can happen. After the information delivery, the CO_2 level can be shown on the screen of the smart watch.

6. Evaluation

6.1. Evaluation Process

The evaluation of the trustworthy CPS communication hub was carried out in several steps in a laboratory environment targeting towards the final demonstration of energy flexibility and traffic accident cases of the M2MGrids project [24]. The applied evaluation steps are shortly overviewed in the following, and a more detailed view is provided in the sections of this chapter.

- *CPS hub with physical CPS asset devices*: Evaluation of the basic capabilities of the CPS hub, such as registering and operation of physical CPS asset devices with the virtual communication spaces. Increasing, step by step, the amount of owners and physical resources such as smart watches (Polar), hunting dog collars and specific servers (Tracker), street lamps and specific servers (Valopaa), and EEG measurement devices and specific servers (Bittium). Establishing trust relationship between owners, and increasing their amount. Application of publish/subscribe information sharing between physical resources owned by different stakeholders.
- *CPS hub with services of automated dynamic microgrids:* Registration of the presence of the distributed resource components in the CPS hub: simulated electric vehicles simulated charging spots, charging manager, simulation model of the local distribution grid, user interface tool, visualizer tool, and energy market platform (Empower EMSP). Establishing a simple trust relationship between energy market platform and all the other components controlled by VTT. Enabling the resources to communicate with each other to collaborate to reach negotiated energy consumption/production flexibility in the day ahead/intraday energy market case.
- *CPS hub with heterogeneous data planes:* Development and evaluation of the capabilities of the CPS hub to operate with heterogeneous data planes according to the needs of physical assets, the IoT platform, and/or enterprise zones. The evaluation considered application of MQTT, HTTP/CoAP, and OneM2M/ETSI M2M [30–33], in order to evaluate the generic nature of the data plane negotiation capabilities of the CPS hub.
- *CPS hub with streams-based M2M service platform in the energy flexibility case*: The capabilities of the CPS hub to operate in the energy flexibility case were evaluated in this evaluation step. The system included a new small scale external aggregator of VTT (FlexEntities), which aggregated a set of simulated distributed energy resources: electric vehicles and charging stations, as well as some buildings. These simulated DERs were controlled via the stream bridge of Nokia WWS by the higher-level aggregator service/local market. The evaluation included establishing the required streams towards the streams-based M2M service platform (Nokia WWS) for reaching the topic names for communication with the local market entity of Nokia WWS for the CPS hub via VTT stream proxy. Creation of the trust relationship with Nokia WWS system by applying a VTT stream proxy to simplify the test case. Evaluation of the interoperability of the CPS hub with Nokia WWS. In addition, evaluation of the scalability of the CPS hub by execution of multiple instances of the ADM simulation system owned by different stakeholders.
- *CPS hub with external authorization service in the traffic accident case:* The capabilities of CPS hub to operate with several heterogeneous stakeholders' systems and resources of multiple owners so that the security policies of the owners are considered in this evaluation step. The evaluation included such aspects as the scalability of the CPS hub to support presence management of larger set of resources owned by different stakeholders, trust checker of CPS hub for taking care of the dynamic grid of agreements dynamically negotiated between the parties/resources, trust checker

negotiation with policy based authorization, extensible authorization framework as a service (SAFAX), in a simple security policies case dealing with an alarm type of event, and trusted publish/subscribe type of information sharing between resources so that the delivery of subscribed content happens only if it is allowed.

6.2. CPS Hub with Physical CPS Assets

The evaluation step focused on testing the basic capabilities of the CPS hub related to the registering and operation of physical CPS asset devices with the virtual communication spaces. Establishing trust relationship between owners. Application of publish/subscribe information sharing between physical resources owned by different stakeholders. The demonstration (the laboratory environment was represented for a wider audience in the ITEA M2MGrids (m2mgrids.erve.vtt.fi) booth in the digital innovation forum (DIF) event, see https://dif2017.org/ as well as https://itea3.org/publication/download/itea-magazine-november-2017-28.pdf), included the following steps:

- Configuring the communication spaces for the owners (Polar, Bittium, Tracker, and Valopaa) in the CPS hub, see also Figure 11.
- Connecting and authenticating the physical resources of the owners with the CPS hub/XMPP server over TLS connections.
- Presence registration of the physical resources, smart watch of Polar, EEG measurement device of Bittium, dog collar of Tracker, and street illuminator of Valopaa into the CPS hub.
- Visualizing the dynamic presence situation of physical resources in the CPS hub using the visualizer tool.
- Negotiation of the trusted relationship (agreement) between Polar and Valopaa resources: smart watch and street illuminator.
- Connecting and authenticating the physical resources of the owners, according to the trusted relationship for information sharing, with the CPS hub/MQTT broker.
- Application of bluetooth LE low-power technology for delivery of heart rate information from low-power sensor to the Polar smart watch. Publishing the heart rate information measured and delivered via the Polar smart watch to the CPS hub using the CPS hub connector in the direct attachment method.
- Subscribing the heart rate information of the Polar smart watch by street illuminator/intelligent lightning gateway of Valopaa in the CPS hub.
- Checking the conditions for allowing the delivery of the subscribed heart rate information of Polar smart watch to the street lamp of Valopaa by the trust checker of the CPS hub.
- Delivery of the heart rate information of the Polar smart watch to the street illuminator of Valopaa.
- Adjusting the light intensity of street illuminator of Valopaa according to the measured heart rate information via the Polar smart watch. Application of the 868 MHz ISM radio technology for controlling intensity of light fixtures of the street illuminator by intelligent lightning gateway.

The devices of the Valopaa and Polar of the demonstration (the laboratory environment was represented for a wider audience in the ITEA M2MGrids booth in the digital innovation forum event) are shown in Figure 19. The lightning fixture (left) and the gray gateway box in the middle control the lightning according to the heart rate information published by Polar smart watches. The heart rates were simulated (white box, hand on the adjusting knob), so that it was possible to adjust the rates rapidly. A Polar M600 smart watch (white and black in the Figure 19) was applied for the exposing of heart rate information from the heart rate simulator and publishing it to the CPS hub via the gateway.

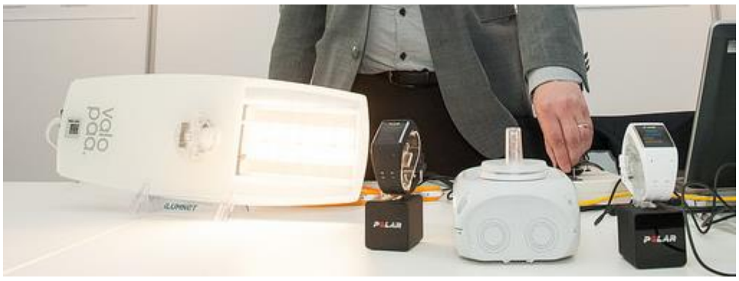
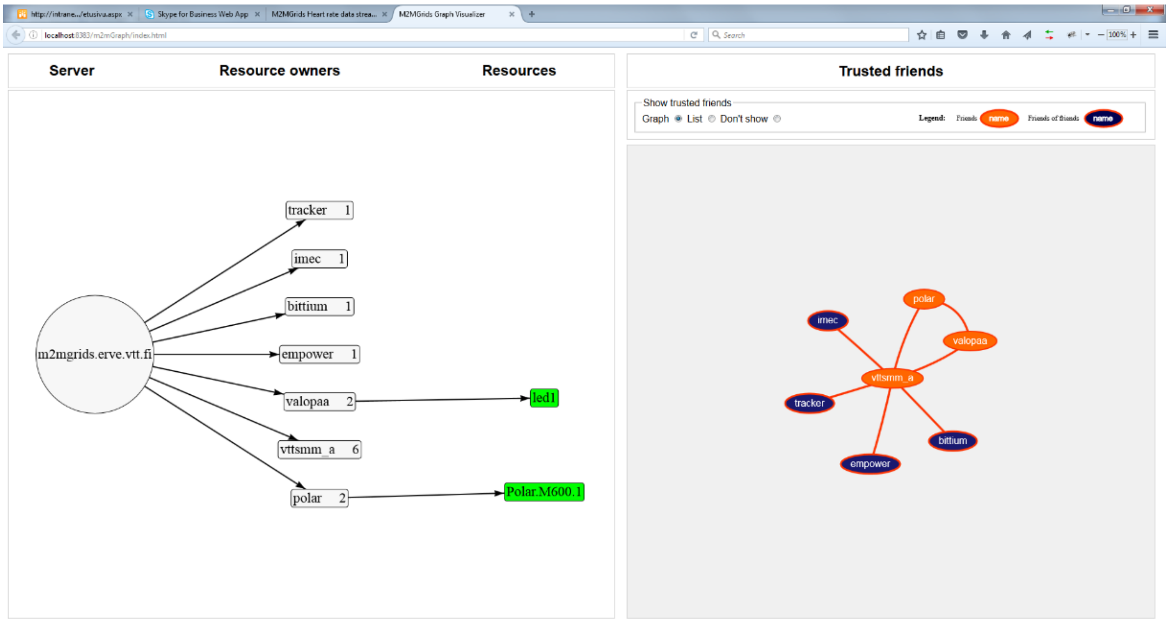


Figure 19. Polar and Valopaa devices of the smart mobile M2M demonstration in the digital innovation forum (DIF) event.

A snapshot into the visualization of presence of physical resources and the trust relationships in the CPS hub is shown in Figure 20. The presence of the street illuminator and smart watch can be seen as green rectangles in the left side, and trust relationships of the owners in the right side of Figure 20.

The evaluation indicates that the publish/subscribe type of information sharing seems to fit quite well for CPS/M2M type messaging, because in the experiment, there were few information elements in use. However, when sharing a larger set of content such as multimedia, domain, or even vendor specific information content/protocols, then some more advanced methods, such as data plane negotiation, are maybe needed (see Section 5.4).

For the realizations of the publish/subscribe method, we had two options: XMPP pub-sub nodes or MQTT-based solution. The MQTT-based publish/subscribe method proved to be more simple and usable than XMPP pub-sub node, and thus it was selected. However, it does not have any support for trust-based conditional delivery of content, nor presence management of physical resources. Therefore, presence and buddy subscription means of XMPP were selected and applied for enabling dynamic support for presence management and negotiation of trust relationships. In addition, the concept of the Jabber identifier (JID), that is, notation <*owner*>@<*domain.server*>/<*physical resource*>, applied in the XMPP proved to be very practically usable, see Sections 3.2 and 4.2. However, we enhanced it a step forward in this research, see (1) in Section 4.2, and also applied it for the MQTT-based publish/subscribe and identities of the trust checking service.


http://intrane.../etusivu.aspx × Skype for Business Web App × M2MGrids Heart rate data strea... × M2MGrids Graph Visualizer ×

localhost:8383/m2mGraph/index.html

Server Resource owners Resources

Trusted friends

Show trusted friends

Graph ● List ○ Don't show ○

Legend: Friends name Friends of friends name

Figure 20. Visualization of the presence and trust relationship in the CPS hub.

The realization of the trust checking services proved to be the most challenging part in this step. We were capable for taking the dynamic presence of resources, their identities, owner identities, and grid of agreements into concern in the DIF demonstrator. However, it proved during the work that aspects such as, for example, situation (alarm and so on), time, information, and subscriber require more capabilities in order to enable their definition in the owner specific way. Therefore, application of external authorization service relying on SAFAX and XACML technology [22,23] was included in the trust checking services of the CPS hub.

6.3. CPS Hub with Services of Automated Dynamic Microgrids

The evaluation step related to the automated dynamic microgrids (ADMs) is shown in Figure 21. The system considered the energy market service platform (EMSP) of Empower, the simulation-based system of the distributed energy resources, and the CPS hub. The simulation-based approach was selected to enable studying the concepts, algorithms, and real SW systems of automated dynamic microgrids without complex and expensive distributed energy resources (DERs), distribution grid, embedded products HW systems, and a large number of stakeholders and service systems [1].

The demonstration included the following steps related to setting up the CPS hub operation capabilities for the automated dynamic microgrids:

- Configuration of communication spaces for Empower and VTT resource owners;
- Connecting and authenticating the physical resources of the owners with the CPS hub/XMPP server over TLS connections;
- Presence registration of the real and simulated resources, and visualizing the dynamic presence situation of physical resources. The green rectangles upper right corner of Figure 21 shows that "Emp" (Empower EMSP), "simev*" (simulated electric vehicles 1–3), "simevse*" (simulated charging stations 1–3), "CMSim" (simulated charging manager), "Apros" (simulation of the local distribution grid), and "simui" (simulation user interface, also shown in the lower right corner of Figure 21) are available in the system;
- Negotiation of the trusted relationship (agreement) between Empower and VTT resources;
- Checking the trust for enabling the delivery of the energy domain/ADM-related specific information-based interaction via XMPP.

After these steps, the CPS hub was set up for messaging between the resources. In this case, all the referred ADM specific messaging was exchanged using two methods: first XMPP and then MQTT in the enhanced version in energy flexibility demonstrator. The ADM specific messaging consisted of the following steps:

- The control unit of the ADM simulation entity/charging manager reported the amount of combined capacities (estimations of the day ahead numbers) of the controllable DERs for both consumption and production to EMSP, which is allowed to be used by the EMSP;
- EMSP knows the day ahead situation in the larger distribution grid, energy market prizes, and gives control commands, guidelines for consumption/production, to the control unit of the ADM simulation entity accordingly for the next day (24 h);
- The control unit of the ADM simulation entity uses the control/guideline values according to the EMSP control commands and the results of the actions can be monitored via the simulation system;
- The control unit of the ADM simulation entity reports the measured consumption and production levels to EMSP on an intra-day basis;
- EMSP can send intra-day control commands to ADM simulation entity if there is need to do so.

The evaluation indicates that including the simulated entities as the resources in the CPS hub proved to be a very useful capability, because then the complex scenario can be executed without having all the real physical resources present in the system. In addition, the presence services of the CPS hub/XMPP server enabled dynamic changes in the availability of the distributed energy resources.

The application of virtual communication spaces to host the resources of each owner seems to be essential in resource identification, especially when speaking about mobile DERs such as Electric Vehicles (EVs.) The trust checking service of CPS seems to be essential in ensuring that ownership of resources, as well as the agreements and value sharing between owners, can be taken properly in concern. It is estimated that these capabilities are essential in enabling energy communities between a variable numbers of stakeholders with a dynamic set of DERs in various aggregator types of energy business set-ups.

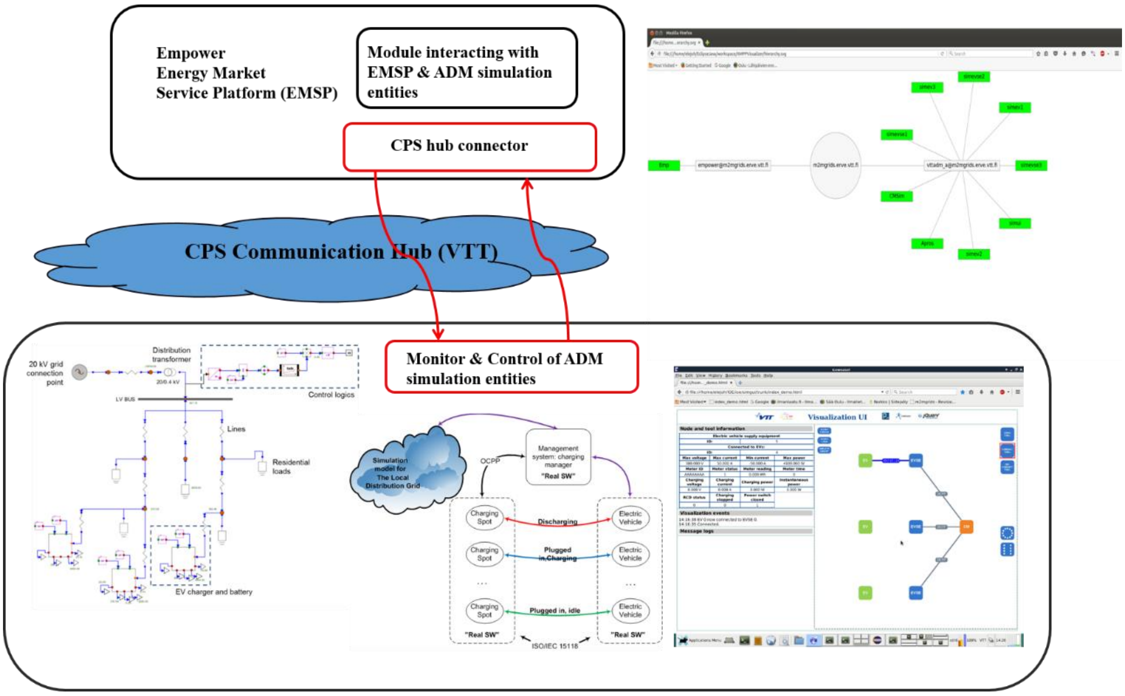


Figure 21. Experimental system of the automated dynamic microgrids. EMSP, energy market service platform; ADM, automated dynamic microgrid.

A challenging part of the ADM is related to the information-based interaction between distributed energy resources and EMSP. In the executed scenario, the information-based interaction was based on the proprietary—specifically defined for this case—messaging, which was exchanged between simulated entities and EMSP using XMPP means. However, the energy domain has several standards (defined, for example, in CEN, CENELEC, ISO, IEC, and ETSI) and industrial forums/specifications, for example [34–39], for its specific operations, like smart energy metering, energy market interaction, home automation, and charging electric vehicles. This implies heterogeneity of DERs and platforms of energy field stakeholders. One potential solution method can be data plane negotiation, the evaluation of which is clarified in the following section.

6.4. CPS Hub with Heterogeneous Data Planes

The operation capabilities of the CPS hub with heterogeneous data planes are clarified here using three environments realized for the validation of the data plane negotiation capability of the CPS hub. The first system includes the use of MQTT as the data plane protocol, whereas in the second system, HTTP/CoAP entities are used. The third evaluation system contains endpoints that use the OneM2M protocol as the data plane protocol.

6.4.1. MQTT as the Data Plane Protocol

The evaluation arrangements related to the MQTT case are shown in Figure 22. The system comprises three MQTT endpoints: one MQTT server and two MQTT clients. MQTT endpoints were equipped with XMPP clients that are capable of data plane negotiation. For XMPP services, there are two federated XMPP servers in the system, local and public. The public XMPP server also hosts the virtual communication spaces of the owners.

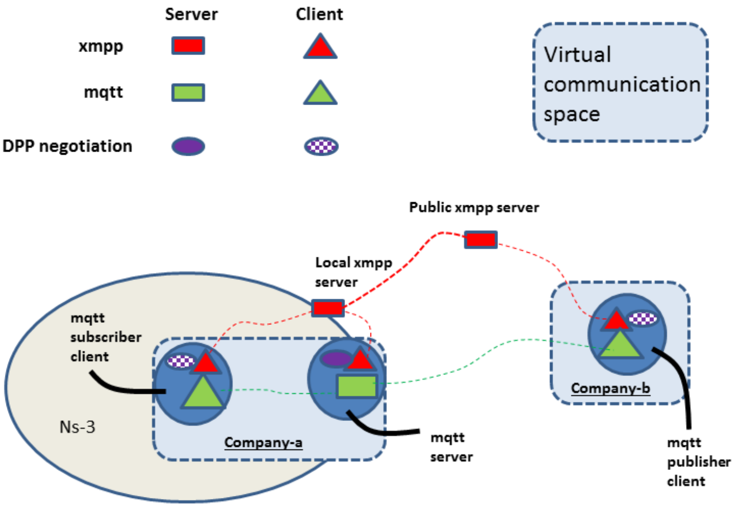


Figure 22. Data plane negotiation in the message queue based telemetry transport (MQTT) case.

The MQTT server and MQTT subscriber clients run in the NS-3 network simulator environment, being clients of the simulated lr-wpan/6lowpan network. The MQTT server also has a Local Area Network (LAN) interface to company intranet. The MQTT publisher client runs on company intranet. The XMPP clients running in the NS-3 simulator connect to the virtual communication server (public XMPP server) via the local XMPP server, whereas the MQTT publisher client running on company intranet can register directly to the virtual communication server.

There are two owners in the system, Company-a and Company-b. Company-a owns the MQTT server and MQTT subscriber client, while Company-b owns the MQTT publisher client. This means that there are two virtual communication spaces in the system. They can be expressed using XMPP JID as Company-a@m2mgrids.erve.vtt.fi and Company-b@m2mgrids.erve.vtt.fi, respectively.

Both MQTT clients are willing to communicate with the MQTT server. The MQTT subscriber client is under the same owner (under the same virtual communication space) as the MQTT server, so they inherently have a trust relationship. However, in order to obtain the MQTT server's IP address and other communication parameters, it needs still to execute data plane protocol negotiation. On the other hand, the MQTT publisher client needs to establish a trust relationship with the MQTT server, as they are under different owners. Naturally, it also needs to perform data plane protocol negotiation.

The MQTT server was configured to accept Company-b's trust relationship creation request and data plane negotiation request. This is done by adding Company-b's JID (Company-b@m2mgrids.erve.vtt.fi) into the trusted list.

After both MQTT client endpoints have successfully performed the data plane negotiation with the MQTT server, they can connect to MQTT server, as they now know the IP address and port to be applied. The evaluation case indicated the successful operation of the data plane negotiation when using MQTT as the data plane protocol.

6.4.2. HTTP/CoAP as the Data Plane Protocol

The testing arrangements for the data plane negotiation with HTTP/CoAP as the data plane protocol are depicted in the Figure 23. The system consists of two endpoints, the CoAP server and HTTP client, that are willing to communicate with each other. The CoAP server runs in the NS-3 simulator, whereas the HTTP client is located in company internet. They do not understand each other directly, and thus need the HTTP/CoAP proxy for interpreting purposes. The endpoints were embedded with data plane negotiation-capable XMPP clients. There are two XMPP servers working in federation to transfer XMPP traffic for data plane negotiation purposes.

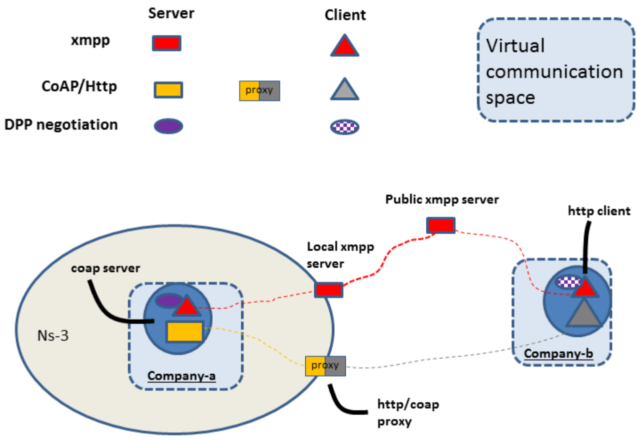


Figure 23. Data plane negotiation in the hypertext transfer protocol (HTTP)/constrained application protocol (CoAP) case.

Like in the MQTT case, there are two virtual communication spaces involved in the system, belonging to Company-a and Company-b. Hence, the data plane protocol negotiation is required. In this test arrangement, the HTTP/CoAP proxy was left out of the data plane negotiation for simplicity.

In this configuration, the DPP-client is deployed in the HTTP client, while the DPP-server locates in the CoAP server. When the HTTP client is ready to start reading data from the CoAP server, it first initiates data plane negotiation in order to get the required information for the HTTP connection. Company-a's trusted list contains Company-b, which means that a trust relationship can be established. As a result of the data plane negotiation, the HTTP client learns the IP address and other communication parameters of the CoAP server. The IP address of HTTP/CoAP proxy was hard-coded in the HTTP client. By combining these two IP addresses together with the port number, the HTTP client is able to constitute the HTTP URL to be used in the connection. The evaluation case indicated successful operation of the data plane negotiation when using HTTP/CoAP as the data plane (transport) protocol.

6.4.3. OneM2M as the Data Plane Protocol

Validation arrangements for experimenting data plane negotiation with OneM2M protocol are shown in Figure 24. The system comprises a server for virtual communication spaces (XMPP server) and two OneM2M/ETSI M2M components, Network Service Capability Layer (NSCL) and Gateway Service Capability Layer (GSCL). NSCL and GSCL run in the Open Service Gateway Initiative (OSGI) framework [30–33]. Embedded in GSCL, there is a bulb application status, which can be monitored via NSCL using the methods provided by the OneM2M framework.

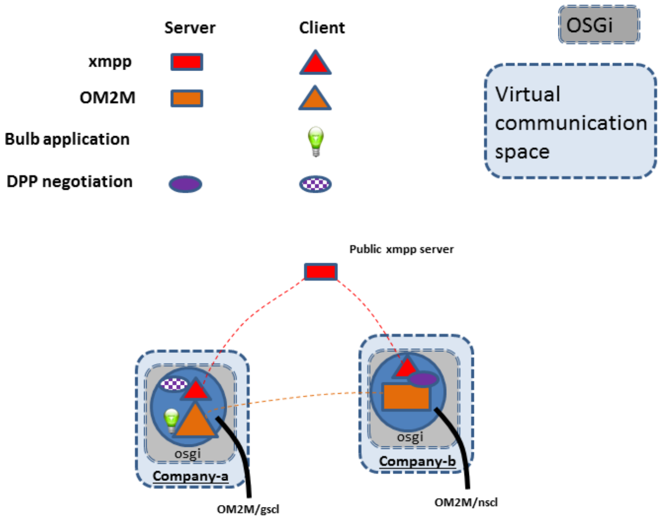


Figure 24. Data plane negotiation in the OneM2M case.

The system involves two virtual communication spaces, Company-a@m2mgrids.erve.vtt.fi and Company-b@m2mgrids.erve.vtt.fi. Consequently, the data plane negotiation is needed between those communication spaces.

NSCL hosts the DPP server and contains the trusted JID list for checking the data plane negotiation accesses. GSCL involves the DPP client that initiates data plane negotiation with JID associated to GSCL. As a result of the data plane negotiation, GSCL obtains the IP address and port number of NSCL and can initiate the normal OneM2M session. The evaluation case indicated the successful operation of the data plane negotiation when using OneM2M as the data plane protocol.

6.5. CPS Hub with Streams-Based M2M Service Platform in the Energy Flexibility Case

The energy flexibility case is described in the work of [24], and overviewed shortly in the following. There are a number of buildings, each of which have a specific set of energy sensitive resources (white goods, boilers, heating resources), and electric vehicles, which are controlled by multiple energy aggregator services, in turn acting on a local market; Figure 25. The status and load balance in the electrical grid is monitored and compared with the forecast in real time. A distribution service operator (DSO) detects a need for flexibility and asks for bids from the aggregators on the local market every 15 min in a 24 h forecast window. The aggregators make their bids, based on the flexibility capacity of the energy resources they control, considering energy market prizes and restrictions as set by the energy resource owners. The flexibility is related to possibility to shift the energy consumption or production to another timeslot in a controlled way. For example, the energy consumption of white goods, boilers, heaters, or electric vehicle charging can be moved to happen earlier or later, or, if possible, at a lower or higher pace, depending on the constraints the device user has set. The local market can mix and match the aggregator bids to the flexibility asked by the DSO. When a bid is awarded, the aggregator can fulfil the corresponding flexibility by instructing the individual devices. As such, the electrical grid power balance can be maintained better, with flattened, lowered differences between energy production and consumption, in effect having the finer-grain consumers/producers follow the fluctuations of (renewable) energy production. This is beneficial because DSOs can save on energy storage investments; new aggregator businesses can conduct sound, revenue-generating business cases; and households and vehicle owners get energy bill rebates for their flexibility contribution. The experimental case enabled automatic and real-time energy flexibility, which addressed real needs of the energy sector, which is challenged by the introduction of ever more renewable, but intermittent energy sources, and the ever more distributed nature of both production and consumption [24].

In this evaluation step, the capabilities of *CPS* hub to operate with streams based M2M service platform in the energy flexibility case was evaluated. The system included a new small scale external aggregator of VTT (FlexEntities), which aggregated a set of simulated distributed energy resources: electric vehicles and charging stations, as well as some buildings. These simulated DERs were controlled via the stream bridge of Nokia WWS by the higher-level aggregator service/local market. The evaluation focused especially on the operation of the CPS hub with the specific streams-based M2M service platform (Nokia WWS), and simulated distributed energy resources; Figure 26.

The M2M service platform (Nokia WWS) has a local market entity in the energy flexibility case, which is capable of streams-based interaction with external entities via a specific entity called the stream bridge. The VTT stream proxy was created to establish the required streams, with the sink/source related topic names of the local market entity, towards the stream bridge, and acting as the connector of the CPS hub on behalf of the owner "Nokia". After that, the trust relationship with the resources of Nokia and "vttadm_a" was established. Finally, the energy flexibility related interaction (FlexRequest, FlexResponse, FlexAllocate, FlexAllocate Response) between the local market and the local VTT aggregator of the simulated distributed energy resources was tested. The limited trial in which the charging/discharging level of a simulated electric vehicle was used to lower the energy consumption according to the flexibility needs of the local market. The executed test case was very limited in the energy flexibility case; however, it was very essential in the architecture concept point of view. This is because the evaluation step showed interoperability of the streams-based M2M service platform and the CPS communication hub.

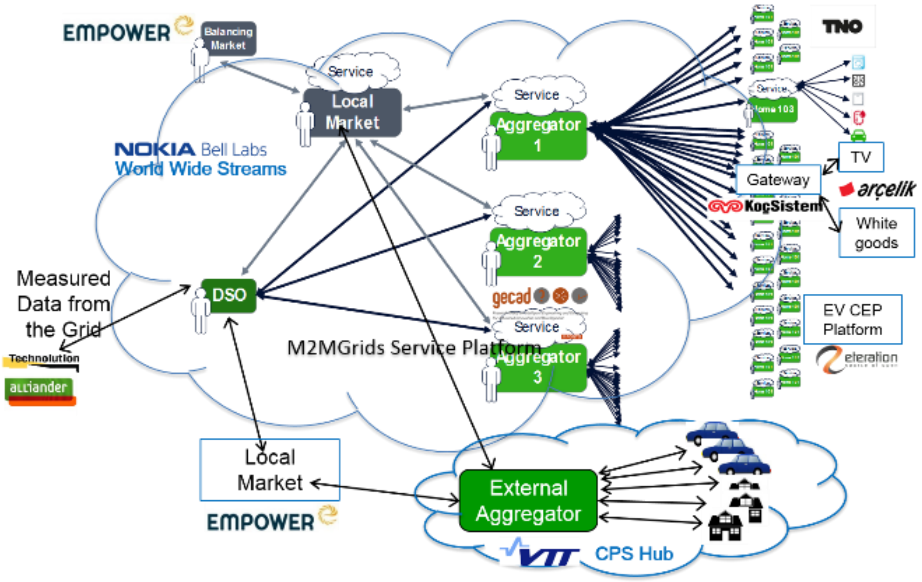


Figure 25. Structure of the energy flexibility case. DSO, distribution service operator. EV CEP, complex event processing in the electric vehicle.

In addition, the evaluation step included preliminary estimation of the scalability properties of the CPS hub by execution of multiple instances of the ADM simulation system owned by different stakeholders. During this step, duplicated distributed energy resource sets were established using different owners, and their control under the energy market service platform of Empower was emulated.

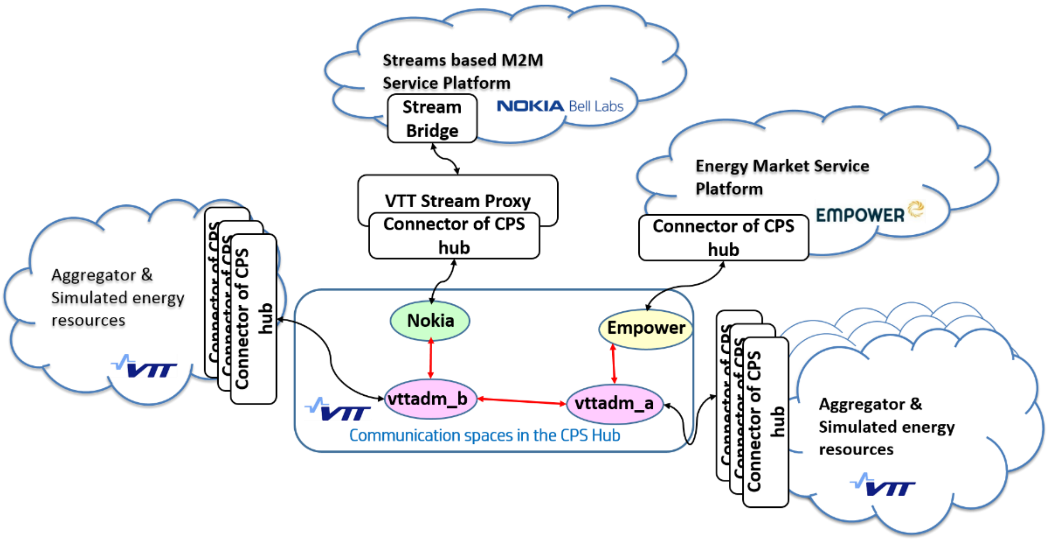

Streams based M2M Service Platform
Stream Bridge
NOKIA Bell Labs
VTT Stream Proxy
Connector of CPS hub
Energy Market Service Platform
EMPOWER
Connector of CPS hub
Aggregator & Simulated energy resources
VTT
Connector of CPS hub
Nokia
Empower
vttadm_b
vttadm_a
VTT
Communication spaces in the CPS Hub
Connector of CPS hub
Aggregator & Simulated energy resources
VTT

Figure 26. The CPS hub with streams based M2M service platform.

6.6. CPS Hub with External Authorization Service in the Traffic Accident Case

The traffic accident case is described in the work of [24], and overviewed shortly in the following (Figure 27). A person does his exercise on the road, and monitors the performance via the smart watch. The smart watch is able to receive warnings from environmental conditions such as CO_2 level, because the owner of the CO_2 measurements has allowed delivering the measurement reports directly to him. Simultaneously, another person is hunting in the nearby forest with his dog. The dog has a tracker that makes it possible to follow the dog on a map. If the dog runs too near the road, the location of the dog is detected by the nearby street lamp, which thus increases the intensity of lightning and starts blinking. However, a vehicle collides with the hunting dog, causing an accident. A person sees the accident and calls the alarm center. The alarm results in authorized changes in the information delivery process according to the profiles of the persons and stakeholders on the road. For example, authorities such as the police and medics are able to receive information from multiple devices and stakeholders according to their alarm-related profiles and see the situation online.

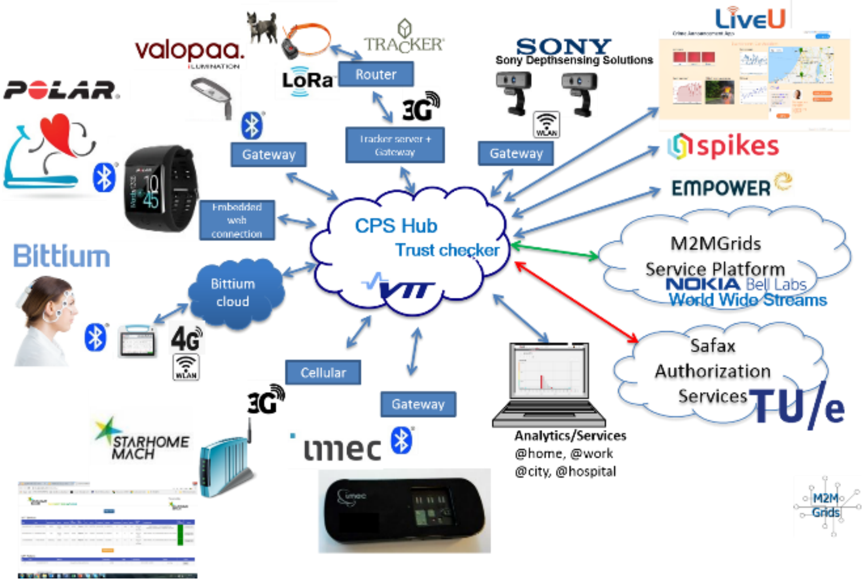


Figure 27. Structure of the smart mobility in the emergency case.

The capabilities of the CPS hub to operate with several heterogeneous stakeholders' systems and resources of multiple owners so that the security policies of the owners can be taken into concern were tested in this evaluation step. This considered the evaluation of the scalability of the CPS hub to support presence management of a larger set of resources owned by different stakeholders; evaluation of the trust checker of CPS hub for taking care of the dynamic grid of agreements dynamically negotiated between the parties/resources; evaluation of the trust checker negotiation with SAFAX in a simple security policies case dealing with alarm type of event; and evaluation of the trusted publish/subscribe type of information sharing between resources, so that the delivery of subscribed content happens only if it is allowed.

The operation capabilities of the trust checker of the CPS hub to collaborate with policy based authorization, extensible authorization framework as a service (SAFAX), were especially focused on in this evaluation step. In addition, the capabilities of trust checker to take into concern the policies of the owners in the information delivery process were tested as the part of the traffic accident case.

First, a simple security policy for the owner "IMEC" and "Polar" was done so that they allow delivery of the CO_2 measurement information between each other. In addition, a special system status information to a specific location area was defined to indicate the "alarm" type of condition. It was seen that only an authorized stakeholder, which was simulated in this case, can define such an "alarm". Then, the security policies for the owners "Polar", "Imec", "Starhome", and "Bittium" were defined so that the information from their resources can be delivered to authorized stakeholder, "LiveU", if an alarm happens.

After these actions, the alarm situation was executed together with the physical resources attached to the CPS hub. The trust relationship between the owners before the alarm event, the traffic accident, has happened is visualized in Figure 28. The respective situation after the accident has happened is shown in Figure 29.

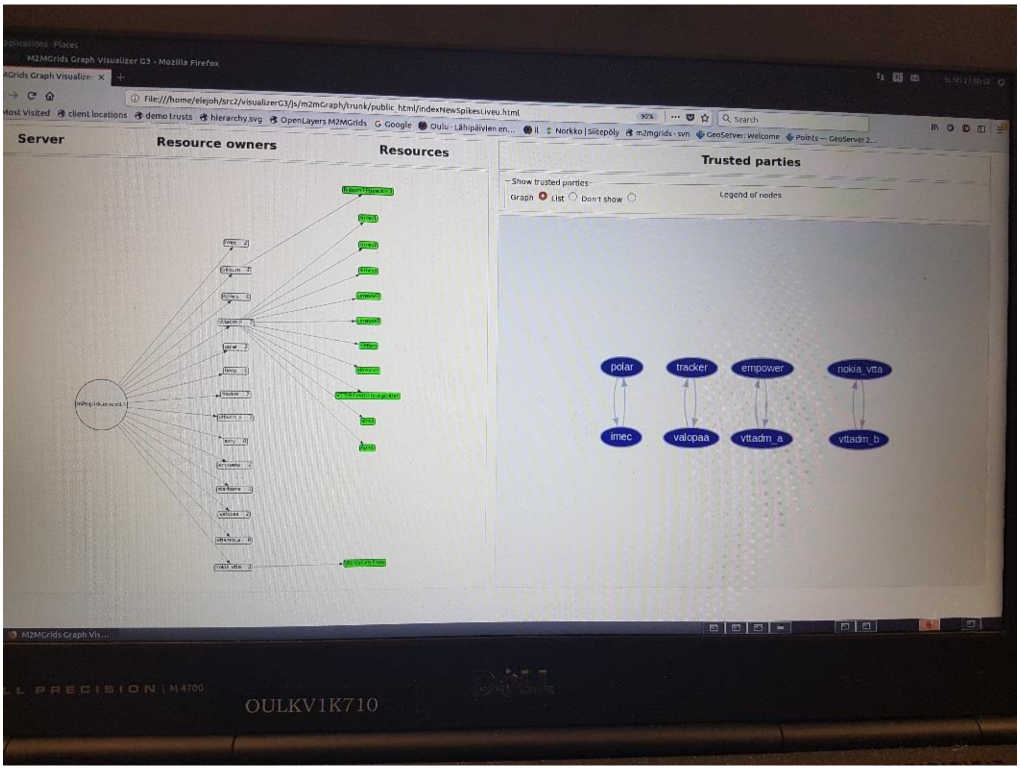


Figure 28. Trust relationship between owners before the alarm event, the traffic accident, has happened.

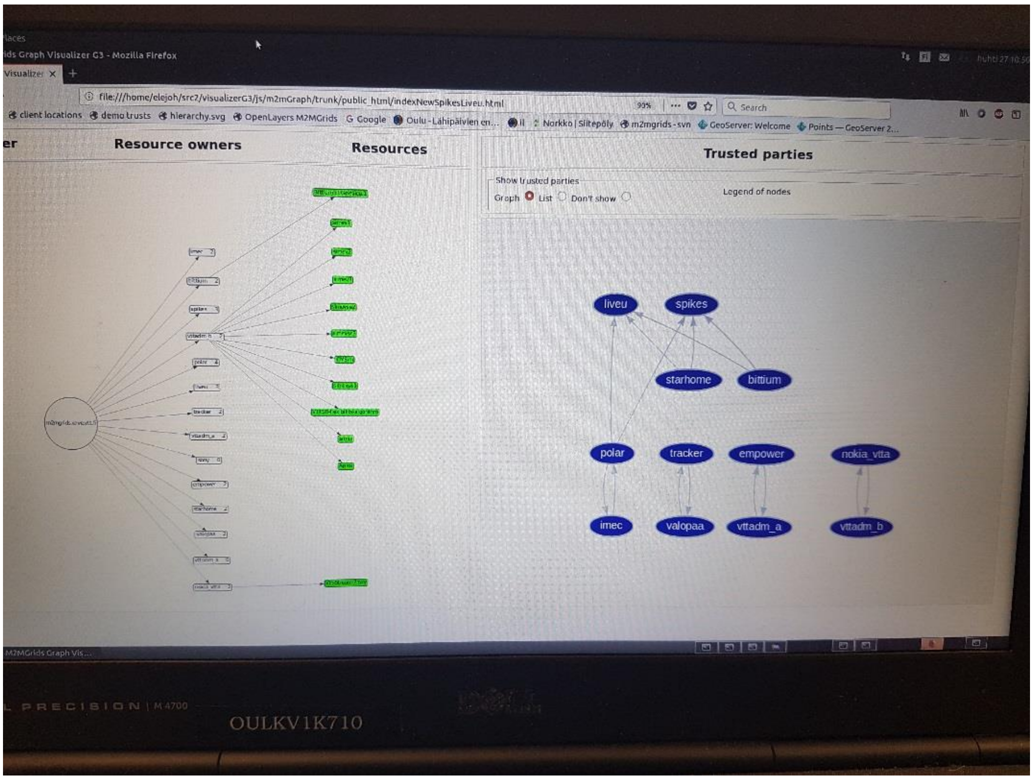
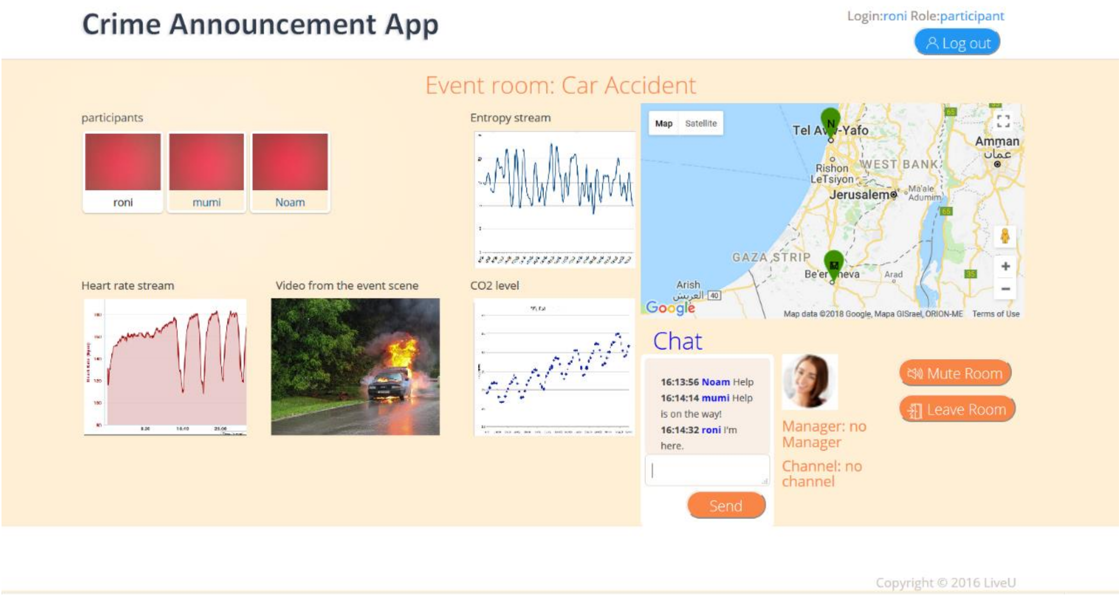


Figure 29. Trust relationship between the owners after the alarm event, the traffic accident, has happened.

The visualization screenshot shows that after the alarm event has happened, the trust relationships between the owners are updated according to their policies. Finally, the information from the heart rate measured via the Polar smart watch, the video picture captured by Starhome camera, the CO_2 level measured by IMEC sensor, and the entropy stream extracted relying on the information published by Ekg/Egg sensor of Bittium can be seen in the screen provided for the authorities from the traffic accident area after the alarm has happened; Figure 30.



16:13:56 **Noam** Help
16:14:14 **mumi** Help is on the way!
16:14:32 **roni** I'm here.

Figure 30. A view of the screen of the authorities of the traffic accident area after the alarm event.

6.7. Discussion

The development of the CPS hub and evaluations were done in a systematic step-by-step manner, which has proven to be a very powerful approach. The evaluations indicate that the capabilities of the CPS hub to manage presence, trust process, and publish/subscribe type of information sharing between heterogeneous resources/services of multiple stakeholders are functionally sufficient to operate in the considered evaluation cases. The CPS hub enabled interactions of very heterogeneous physical resources, such as, for example, smart watches (Polar), hunting dog collars (Tracker), street lamps (Valopaa), EEG measurement device (Bittium), electric vehicles (simulated), charging stations (simulated), buildings (simulated), simulation models, and multiple servers of companies, so that ownership was taken into concern. However, the evaluation related to energy flexibility case was limited in the sense that only simulated physical resources were used in a limited scenario. Especially the scalability, real-time and streams-based operation, application of physical DERs, aggregation, virtual power plants, and interaction within day ahead/intraday energy markets are seen to be issues for future research. In addition, the evaluations of the CPS hub demonstrated potential methods for including the policies of the owners for trustable interactions between CPS resources. However, combining the policies of the owners, service providers, and OEMs in the physical resources, communications and information levels in dynamic contexts requires future research actions. On the basis of the evaluations, it is envisioned that the constructed CPS hub contributes a set of very essential technical enablers for future smart CPS systems and creates a strong basis for such future research.

7. Conclusions

As the results of this research, we provide a trustworthy communication hub for cyber-physical systems and contribute towards solving the challenges related to trustworthy communications between physical resources owned by different stakeholders. The CPS hub realizes the communication spaces concept, and enables the combined trust and communications process when dynamic resources owned by different stakeholders are exchanging information. The solutions contribute towards solving the introduced grand challenge related to trustworthy communications of cyber-physical systems, especially in the energy flexibility and emergency mobile cases.

The evaluation shows that the provided CPS hub enables information exchanges between distributed energy resources of different stakeholders, so that they can join the aggregation process for more flexible and efficient resource usage in the energy markets. However, the evaluation was limited in the sense that only simulated energy resources were used in a specific test scenario. In the emergency mobile case, the CPS hub enables interaction between heterogeneous physical devices of multiple stakeholders to exchange information, so that, for example, authorities can see the situation in the emergency area and, simultaneously, the policies of the owners can be taken into concern. However, the evaluation was limited in the sense that only very simple security policies of the owners were involved in the test scenario.

Despite these limitations, the evaluation cases showed that consideration of the ownership issues in the communication for information exchanges between heterogeneous physical resources (devices) is possible and feasible. The evaluations of the CPS hub demonstrated potential methods for including the policies of the owners for the creation of trustable interactions between CPS resources. However, for example, scalability, real-time and streams-based operation, application of physical DERs, aggregation, virtual power plants, and interaction with in day ahead/intraday energy markets are seen to be issues for future research. In addition, consideration of the security, privacy, trust, and safety challenges with a larger set of service providers, OEMs, and owners, as well as more constrained physical CPS resources, ad hoc wireless communications, and information semantic levels in dynamic contexts, is an open area for future research. However, it is envisioned based on evaluations that the constructed CPS hub contributes a set of very essential technical enablers for future smart CPS systems and creates a strong basis for such future research towards a future smart society.

Author Contributions: J.L. wrote and authored all the chapters of this article. J.H. contributed to the realization and evaluation of the CPS hub, and some pictures and part of texts in Sections 5 and 6.

Funding: This article is based on the research actions executed within ITEA 2 call 8 project 13011 M2MGrids, Smart M2MGrids - M2M Internet for dynamic M2M information business ecosystem. The M2MGrids project was made possible by ITEA framework and was funded by public authorities in Belgium, Finland, Netherlands, Portugal, Turkey, and Israel.

Acknowledgments: Acknowledgments are offerred for all ITEA M2MGrids project partners for their active contributions and discussions during the project. Especially, acknowledgements are offered to Juha Kemppainen, Jari Jauhiainen, and Taavi Hirvonen from Bittium; Marko Tilvis, Pertti Puolakanaho, and Niclas Granqvist from Polar; Hannu Lohi from Tracker; Kari Kananen and Toivo Vilmi from Valopaa; Olli Kilkki and Jan Segerstam from Empower IM; and Hannu Nurmi from Business Finland.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Latvakoski, J.; Mäki, K.; Ronkainen, J.; Julku, J.; Koivusaari, J. Simulation-Based Approach for Studying the Balancing of Local Smart Grids with Electric Vehicle. *Batter. Syst.* **2015**, *3*, 81–108. [CrossRef]
2. Latvakoski, J. *Small World for Dynamic Wireless Cyber-Physical Systems*. Academic Dissertation publication University of Oulu/VTT Science 142. Teknologian Tutkimuskeskus VTT Oy, Finland. December 2016. Available online: http://www.vtt.fi/inf/pdf/science/2016/S142.pdf (accessed on 24 August 2019).
3. Roussaki, I.; Chantzara, M.; Xynogalas, S.; Anagnostou, M. The virtual home environment roaming perspective. In Proceedings of the IEEE International Conference on Communications, Anchorage, AK, USA, 11–15 May 2003; pp. 774–778.
4. Familiar, M.S.; Martínez, J.F.; Corredor, I.; García-Rubio, C. Building service-oriented Smart Infrastructures over Wireless Ad Hoc Sensor Networks: A middleware perspective. *Comput. Netw.* **2012**, *56*, 1303–1328. [CrossRef]
5. Zhang, X.; Law, C.; Wang, C.; Lau, F.C.M. Towards pervasive instant messaging and presence awareness. *Int. J. Pervasive Comp. Commun.* **2009**, *5*, 42–60. [CrossRef]
6. Latvakoski, J.; Iivari, A.; Vitic, P.; Jubeh, B.; Alaya, M.B.; Monteil, T.; Lopez, Y.; Talavera, G.; Gonzalez, J.; Granqvist, N.; et al. A Survey on M2M Service Networks. *Computers* **2014**, *3*, 130–173. [CrossRef]
7. Eugster, P.T.; Felber, P.A.; Guerraoui, R.; Kermarrec, A.-M. The many faces of publish/subscribe. *ACM Comput. Surv.* **2003**, *35*, 114–131. [CrossRef]
8. Saint-Andre, P. (Ed.) Extensible Messaging and Presence Protocol (XMPP) Core. IETF RFC3920. October 2004. Available online: https://www.ietf.org/rfc/rfc3920.txt (accessed on 2 January 2018).
9. Saint-Andre, P. (Ed.) Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. IETF RFC3921. October 2004. Available online: https://www.ietf.org/rfc/rfc3921.txt (accessed on 2 January 2018).
10. Iivari, A.; Väisänen, T.; Alaya, M.B.; Riipinen, T.; Monteil, T. Harnessing XMPP for Machine-to-Machine Communications & Pervasive Applications. *J. Commun. Soft. Syst.* **2014**, *10*, 163–178.
11. Millard, P.; Saint-Andre, P.; Meijer, R. *XEP-0060: Publish-Subscribe*, XMPP Standards Foundation. Draft Standard, version 1.16; 11 September 2019. Available online: https://xmpp.org/extensions/xep-0060.html (accessed on 24 August 2019).
12. Latvakoski, J.; Alaya, M.B.; Ganem, H.; Jubeh, B.; Iivari, A.; Leguay, J.; Bosch, J.M.; Granqvist, N.T. Horizontal Architecture for Autonomic M2M Service Networks. *Future Internet* **2014**, *6*, 261–301. [CrossRef]
13. ISO/IEC 20922: 2016. *Information technology Message Queuing Telemetry Transport (MQTT) v3.1.1*; Springer: Cham, Germany, 2016.
14. OASIS. MQTT 3.1.1 Specification. 10 December 2015. Available online: http://mqtt.org,andhttp://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html (accessed on 24 August 2019).
15. Sensor over XMPP. Available online: http://xmpp.org/extensions/inbox/sensors.html (accessed on 30 November 2015).
16. Rosenberg, J.; Schulzrinne, E.; Camarillo, G.; Johnston, A.; Peterson, J.; Spark, S.R.; Handley, M.; Schooler, E. June 2002. SIP: Session Initiation Protocol, IETF RFC 3261. Available online: https://www.ietf.org/rfc/rfc3261.txt (accessed on 30 November 2015).
17. Fielding, R.; Reschke, J. Hypertext Transfer Protocol (THHP/1.1): Semantocs and Content. June 2014. Available online: https://tools.ietf.org/html/rfc7231 (accessed on 2 November 2015).

18. Zhelby, Z.; Hartke, K.; Bormann, C. The Constrained Application Protocol (CoAP). IETF RFC 7252. June 2014. Available online: https://tools.ietf.org/html/rfc7252 (accessed on 11 November 2015).
19. Roman, R.; Zhou, J.; Lopez, J. On the features and challenges of security and privacy in distributed Internet of Things. *Comput. Netw.* **2013**, *57*, 2266–2279. [CrossRef]
20. Ouaddah, A.; Mousannif, H.; Elkalam, A.A.; Ouahman, A.A. Access control in The Internet of Things: Big challenges and new opportunities. *Comput. Netw.* **2017**, *112*, 237–262. [CrossRef]
21. Alonso, Á.; Fernández, F.; Marco, L.; Salvachúa, J. IAACaaS: IoT Application-Scoped Access Control as a Service. *Future Internet* **2017**, *9*, 64. [CrossRef]
22. Simon Blackwell. *Extensible Access Control Markup Language (XACML)*; Version 3.0; Oasis Standard: Burlington, MA, USA, 2013.
23. Samuel, P.; Kaluvuri, A.; Ionut, E.; den Jerry, H.; Zannone, N. SAFAX—An Extensible Authorization Service for Cloud, Environments. *Front. ICT* **2015**, *2*, 9.
24. Latvakoski, J.; Roelands, M.; Tilvis, M.; Genga, L.; Santos, G.; Marrieros, G.; Vale, Z.; Hoste, L.; van Raemdonck, W.; Zannone, N. Conceptual Architecture for Cyber-Physical Systems. *Systems* **2019**. submitted.
25. Takabi, H.; Joshi, J.; Ahn, G.J. Security and privacy challenges in cloud computing environments. *IEEE Secur. Priv.* **2010**, *8*, 24–31. [CrossRef]
26. Gillet, S.H.; Lehr, H.; Wroclawski, J.T.; Clark, D.D. Do Appliances threaten internet innovation? *IEEE Commun. Mag.* **2001**, *39*, 46–51. [CrossRef]
27. Myers, J. Simple Authentication and Security Layer (SASL). IETF RFC. 1997. Available online: https://www.ietf.org/rfc/rfc2222.txt (accessed on 15 May 2019).
28. Melnikov, A.; Zeilenga, K. Simple Authentication and Security Layer (SASL). IETF RFC 4422 (Obsoletes ITEF RFC 2222). 2006. Available online: https://tools.ietf.org/rfc/rfc4422.txt (accessed on 15 May 2019).
29. Eatmon, R.; Hildebrand, J.; Miller, J.; Muldowney, T.; Saint-Andre, P. Data Forms. XMPP XEP-0004 2007. Available online: https://xmpp.org/extensions/xep-0004.pdf (accessed on 15 May 2019).
30. ETSI M2M/Smart M2M. Available online: http://www.etsi.org/ (accessed on 21 February 2019).
31. ETSI M2M. ETSI Technical Specification 102 690 v1.1.1 Machine-to-Machine Communications (M2M); Functional Architecture. 2011/10. Available online: https://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf (accessed on 24 August 2019).
32. One M2M Forum. Available online: http://www.onem2m.org/ (accessed on 21 February 2019).
33. OneM2M. Technical Specification Functional Architecture TS-0001-V3.15.1. 2019-05-07. Available online: http://www.onem2m.org/images/files/deliverables/Release3/TS-0001-Functional_Architecture-V3_15_1.pdf (accessed on 24 August 2019).
34. OSGP Alliance & ETSI. Open Smart Grid Protocol. ETSI TS 104 001 V2.2.1 (2019-01). Available online: https://www.etsi.org/deliver/etsi_ts/104000_104099/104001/02.02.01_60/ts_104001v020201p.pdf (accessed on 24 September 2019).
35. Flexiblepower Alliance Network (FAN), Energy Flexibility Platform & Interface (EF-Pi). Available online: http://flexible-energy.eu/ef-pi/ (accessed on 24 August 2019).
36. Flexiblepower Alliance Network (FAN), Energy Flexibility Interface. Available online: https://flexible-energy.eu/efi/ (accessed on 24 September 2019).
37. European forum for energy business information exchange (ebIX). Available online: https://www.ebix.org/ (accessed on 24 September 2019).
38. European forum for energy business information exchange (ebIX). Introduction to Business Requirements and Information Models, V1.0 Oct/2015. Available online: https://mwgstorage1.blob.core.windows.net/public/Ebix/Introduction_to_ebIX_Models_1r0B_20151101.pdf (accessed on 24 September 2019).
39. European Network of Transmission System Operators for Electricity (ENTSO-E). Common Information Model (CIM). Available online: https://www.entsoe.eu/digital/cim/ (accessed on 24 September 2019).