# An Usable Application for Authentication, Communication and Access Management in the Internet Of Things

Matteo Cagnazzo[1] Markus Hertlein[2] and Norbert Pohlmann[1]

[1] Institute for Internet-Security, Gelsenkirchen, Germany
{lastname}@internet-sicherheit.de,
WWW: www.internet-sicherheit.de
[2] XignSys, Gelsenkirchen, Germany
hertlein@xignsys.com
WWW: www.xignsys.com

**Abstract.** The following paper introduces a secure and efficient application concept that is capable of authenticating and accessing smart objects. The concept is based on two already developed applications. It describes the used technologies and discusses the outcome and potential downfalls of the idea.

**Keywords:** Security, Authentication, Communication, Internet Of Things

## 1 Preliminaries

Modern components with connectivity mechanisms need authentication to offer services to the authenticating entity. Especially in the emerging Internet of Things as well as eMobility scenarios this becomes imperative. The requirements to authentication mechanisms are that it should be secure, easy to use and reasonable fast, so that there is no "waiting time" for the user. Nowadays the most common mechanism to authenticate against a service or an object is to use password-based approaches. These are prone to manifold attack-vectors:

- Brute-Force-Attack
- Dictionary-Attack
- Rainbow-Tables
- Keylogging

By choosing unsafe passwords or using the same password for multiple services attacks on the internet become more and more profitable. One alternative is multi-factor authentication which combinates knowledge (username/password), ownership (smartphone) and/or individual biological properties (biometry). Access to a system is therefore granted if and only if the combination of all these challenges return successful. A downfall is that a stolen "root-secret" corrupts

a whole system and therefore most problems of password-based authentication are persistent.
Generally identities have different security levels. Depending on the source which is used to verify ones identity, a level of trust can be determined [10].

- Level 1: Data is not verifiable
- Level 2: Verification via Mail
- Level 3: Verification via presence
- Level 4: Verification via official document

Official documents are for example identity cards. These are called primary identity offer the highest level of trust. From those secondary and tertiary-identities are derivable.
One way to depict these different trust levels is via Public-Key-Infrastructure. [4]

### 1.1 Authentication Systems

Todays authentication processes are more dynamic since the interaction of users and machines in the field of the Internet of Things. The classic approaches like password-based authentication or smartcard-based authentication are not able to answer the new challenges developing from the human-machine interaction. On the one hand it is not possible to use password-based authentication for the authentication against a radiator or a coffee brewer due to the need of extra hardware like keyboards or pin-pads. Also the time consuming aspect of using passwords and the user-unfriendly process of managing passwords are not acceptable for small use cases. For high security use cases like the access to production machines a weak one-factor authentication is not applicable. On the other hand strong two-factor authentication methods like smartcard authentication are expensive due to the need of smartcards readers and smartcards or security tokens.

The two examples, the authentication against a radiator and the access to production machines are showing two more demands emerging from the Internet of Things. Unlike authentication systems in the todays Internet, which are mainly working with a level of high or low security, authentication systems in the field of IoT should be able to adjust the security level based on the protection needs of the assets. This so called adaptive authentication is able to increase the usability where possible. Usability is a necessary feature in the field of authentication in IoT, due to the fact that the number of authentication processes will be a multiple of these a user has to perform nowadays. Furthermore the authentication systems have to confluence to an authentication eco-system that works with different technologies in different scenarios and use cases [7].

Summarizing a modern authentication and access management system has to fulfill the following requirements [8]:

- Interoperability
- Adaptive authentication between security and usability
- Reduced complexity and cost-efficient
- Operational in different scenarios and use cases

### 1.2 Communication Systems

An essential part that becomes even more relevant with further interconnectedness of humans and things is efficient communication. In a system where billion things and humans are interconnected there is no need for redundant and slow communication. Current standardization processes like 5G want to enable tactile user experience through real time communication. To realize that one needs short reaction time and latency (< 1ms) [1] [12]. Concepts like network-coding try to reduce redundancy in those networks [5].

By analyzing communication behavior of adolescents, one can derive that they are able to pack a lot of information in just a few signs by combining literals, graphics and emoticons. For example the phrase "See you" is reduced to just "cu". The information that is being transmitted is the same but the quantity of used literals is 66 % lower. That is a significant decrease and a lot of behaviors like this are observable in modern lingo. Another example for modern linguistics is the evolution of the "hashtag" or comparable mechanisms to operate as a marker referencing a specific target. Through this tagging, language becomes searchable and it is possible to affiliate values to words by counting mentions or weighing these mentions. One already implemented and tested approach to this is called "TechnoWeb 2.0" but unlike the proposed approach it focuses on "microblogging" of the users and is only focused on user to user interaction [11]. Finally electronic communication is moving from asymmetrical towards symmetrical communication whereby the communicating peers can exchange their information in real-time and see the collaboration of the other peer which increases efficiency and promotes the exchange of information[14].

Modern collaboration tools simplify the mechanism to address someone by just mentioning them in a document and send a notification to them. Efficiency is essential concerning communicating in a business environment, since employees in every level of hierarchy spent a lot of their time communicating. From this stake a lot of time is consumed by e-mails which are inefficient since there is the need for a salutation and valediction in every e-mail alongside arbitrary and reciprocal information until there is unique information being exchanged. Tools that support symmetrical information exchange though make it easier to share unique information, insights, experiences and knowledge in the blink of an eye with colleagues, friends or any other entity. Global communication is a complex system that can be uni- or multi directional, independent of social status, secure or insecure, private or public but in summary it is mostly dependent on protocol-specific human and technical components.

Taking into account the emerging Internet of things it is clearly distinguishable that current communication solutions are not capable of dealing with the increasing number of participants. Not a single platform provides support for communicating with things or has an interface to connect with smart objects. Efficient, smart and secure chat-based communication is the key for the ongoing digitalization.

These key-features are introduced by a novel platform called "Quvert" [3]. This approach will be expanded in this paper to support communication with

smart objects in the Internet of things by combining Quvert with XignQR. The support of secure authentication and communication will be adressed and explored in this paper.

## 2 Used Technologies

Chapter 2 describes the technologies XignQR and Quvert that will be used to create the proposed architecture.

### 2.1 XignQR

XignQR [9] is an authentication and signature system that fits into a modern authentication eco system. The concept behind XignQR addresses all the requirements mentioned in chapter 1.1. Therefor the XignQR-System comprises of four actors, shown in figure 1:


**Fig. 1.** Interaction of the four Actors

1. Authentication Manager
   The authentication manager is the identity provider and broker. It is the main part in the authentication process between an user and a service provider/relying party (3.).
   It mediates the authentication result from the user authentication to the service provider. It also enforces the security and trust level of the used digital identity requested by a service provider on server-side. At the beginning of an

authentication process the security policy of a service provider and the users self-defined security policy is compared. The policy information are combined and enforced. During an authentication process the authentication manager receives user-behavior from the users personal authentication device (2.) and analyses these data. If anomalies are detected a new factor for authentication is requested through the personal authentication device.

From the users view the authentication manager helps to prevent the loss of privacy. It only delivers the users information to the service provider that are granted through the user.

Another function of the authentication manager is the connection to the public key infrastructure (PKI). Thereby it is responsible for the provisioning of the PKI functionality and its user-management, containing digital certificate enrollment and user pseudonymity.

The PKI, digital certificates and cryptographic protocols are playing a key role in reference of interoperability, adaptive authentication and multi-functional deployment in a variety of use cases.

Besides the PKI a modular protocol stack is necessary for an easy integration. Therefor multiple ID-Protocols like SAML or OpenIDConnect are supported to enable federation between different identity and service providers to build an authentication eco system.

To ensure integrity, authenticity and privacy the whole communication is signed with the users and components elliptic curve private keys and symmetrically encrypted with derived session keys.

2. Personal authentication device (PAD)

   The PAD is represented in form of a smartphone and the personalized XignAPP. It acts as user interface, as QR-Code scanner and as token reader for the optional Security Token.

   During the personalization process the app is equipped with user specific cryptographic material that is used for the challenge response authentication protocol.

   Since there are no passwords or shared secrets transmitted, all the mentioned attacks in 1 will not succeed.

   While authenticating, the smartphone collects user behavior and contextual information. These information are analyzed by the authentication manager (1.) to enforce the policies and initiate multiple authentication factors on-demand.

   The use of the smartphone as PAD enables the use of many different authentication factors, from classical PIN entries over biometrie and security tokens to new mechanism like photo-authentication or video-chat based authentication.

3. Service Provider/Relying Party

   The service provider is the component the user want to get access to. For example a website or a production machine. The integration is done by one of the many supported ID-protocols. As an entry point for the authentication a QR Code is used. The QR Code contains an ID, static or session-based,

representing the service provider, an URL to the authentication manager and a digital signature.
The authentication process starts with the scan of the QR Code with personalized XignAPP.

4. Security Token (optional)
A security token can optionally be added to the PAD to increase the security level while increasing the usability through enabling new kinds of multi-factor authentication without interaction.

**Authentication flow**

The authentication process consists of the following parts:

1. Service Provider requests the QR Code and the user attributes, e. .g. username
2. User scans QR Code with PAD
3. PAD verifies the embedded signature of the QR Code and connects to the authentication manager
4. PKI based mutual authentication between PAD and authentication manager will be executed and the requested attributes will be transmitted encrypted of the established secure channel
5. User sees the information and requested attributes in her app
6. User confirms the authentication by fulfilling the request security level, e. g. PIN or biometry
7. A PKI based challenge response mechanism is executed.
8. Authentication manager transmits the authentication results and user-attributes to the service provider.

### 2.2 Quvert

Quvert enables fast, reliable, usable and secure business communication based on a chat-system. It introduces mechanisms to conduct legally watertight agreements. It enables a visualizable and configurable knowledge management and other features to develop an internal knowledge big data: Quvert.Knowledge. The foundation of Quvert is a secure, distributed and reliable server based on XMPP and Erlang with various database-schemes (eg. Postgres or CouchDB) availabe to ensure up to 99,999999999 % service uptime [2]. The mobile and desktop applications have a composed user interface and are easily usable by technological unaffine users. They also provide security in terms that user input can be concealed and all messages are encrypted on transport and application layer before they are being transmitted to the server. The encryption scheme is a modified version of the Axolotl protocol that has already proven that it is capable of securing connections efficiently [6]. The platform is designed in a modular way so every client can specify their needs and Quvert can adapt it to their needs. The whole platform is designed by these principles:

1. Business by design: Inclusion of business processes into a communication platform

2. Compliance by design: Data autonomy and legally watertight archiving
3. Security by design: Usable and economic security from the start of development
4. Privacy by design: Privacy is dealt with during the development process to preserve it
5. Usability by design: Easy and usable for users, low training periods

## 3 Proposed Architecture

To be able to communicate with a Smart Object one needs to authenticate against it. This authentication can be done with a smartphone that scans a QR-code attached to a smart object. After this the schematic authentication process looks like the one in figure 2. Every arrow in figure 2 is a channel secured with TLS between the endpoints. Furthermore an end-to-end encryption is deployed to verify and establish trustworthy communication over insecure channels. The current mechanism is a Challenge-Response Authentication Mechanism (CRAM). XignQR offers all the functionality to grant access to a smart object,

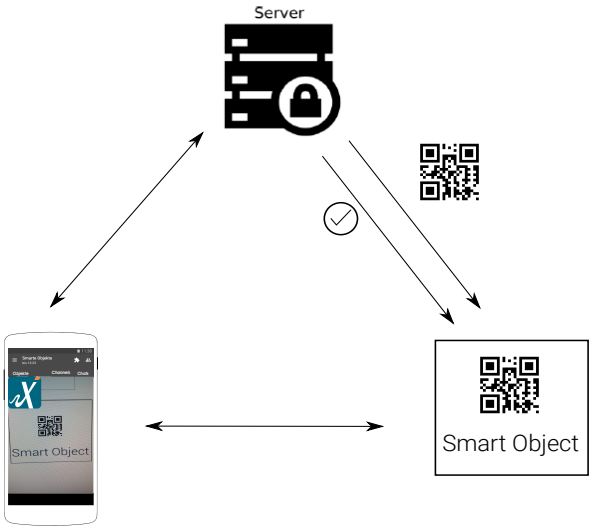


**Fig. 2.** Schematic view of an authentication

for example strong authentication and the public key infrastructure that is being used. Quvert serves as the user friendly interface in which XignQR is being embedded. In Figure 2 XignQR has been personalized to a user in advance by a defined process. Through this personalization XignQR gets meta information and challenges this against the QR-Code. If the challenge-response is successful the user gets access in Quvert to the controls of a smart object. The QR-Code

only serves as a trigger for the authentication process and can be replaced by another mechanism for example NFC or indoor geo location.

The QR Code only stores necessary information to identify the Smart Object on the server and a digital signature. After the QR Code is scanned the XignAPP validates the QR Codes signature and requests the information from the Server of the Smart Object. All information are transmitted through the use of attribute certificates. The benefits of the use of attributes certificates is that the information of the Smart Object can be verified towards integrity and authenticity [10]. Now the adaptive authentication mechanism of XignQR will be used. If the authentication point is a non-critical component, like a radiator, the possession of the personalized smartphone suffices to fulfill the authentication process. At critical authentication points like the physical access to industrial facilities or access to production machines the smartphone will prompt the user to enter a pin, use his fingerprint, capture a photo of the user to use biometric authentication mechanisms or a combination of two or more factors. The use of the smartphone as PAD for Smart Objects in the Internet of Things will gain a high level of usability and security. For example a user picture can not only be used for authentication, but also be added to process confirmations as one part of a signature to dedicate the process to the person that is responsible.

XignQR offers bidirectional communication channels through websockets so the smart objects do not have to poll the server. This saves resources in terms of energy which is an essential feature for resource constrained devices.

After a successful authentication process all necessary information are transmitted to the Smart Object. That can be done on a high level with PKI-based attribute certificates or on a low level with a small uni-directional protocol.

On the app-side after a successful authentication the smart object is shown in the user interface Quvert and the user can control it from a mobile device or workstation. A possible control view for a radiator is shown in figure 3. This view is an interactive element through which a user can interact with smart objects and communicate with it in a secure way. The control elements in figure 3 are only

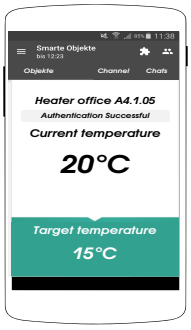


**Fig. 3.** View of userinteraction with a smart object

exemplary and can be expanded if Quvert is openend as a desktop application. Most objects with a low trust level will be easily accessible with the smartphone while more complex objects for example production machines will be visualized on a desktop application.

## 4 Discussion, Outlook and Conclusion

By using this architecture it is possible to authenticate a user with his smartphone against different smart objects by scanning a QR-code attached to it. The platforms that are used for this architecture preconceive data security and privacy so that the possibility of manipulation is still possible but it is very hard to break or fraud the application and it's backend. The scanning of a QR-code is easily feasible by all kinds of users, since it is a intuitive technique. The chat like interface makes the control of smart objects intuitive and flexible as well. A lot of application scenarios are possible for example secure remote maintenance, monitoring, eMobility or distributed testbeds.

Physical and digital restrictions must be considered when combining an Identity Service with a communication platform. Especially if control authentication is granted a holistic contemplation must be done. Every transmission and every endpoint becomes a critical point where security and integrity has to be assured. All of this has to be done in a secure manner without losing the usability of the system. This will soon be a challenging task for the involved researchers. In the future machine-to-machine communication will become the most important topic for digitalized businesses and factories. XignQR is capable of authenticating a machine against another machine and Quvert could operate as a bus system where machines can communicate and push or pull data to specific channels while an administrator has the ability to overview all the machine communication for maintenance or analysis purposes in a tidy and clear interface.

Since XignQR is an authentication and signature system that is able to keep track of the digital processes ensuring integrity and authenticity, the described system is not only able to authenticate and to communicate with and between machines. In combination with the emerging possibilities to create server-side qualified signatures and digital seals, because of the European law eIDAS. Therefore the system can attest the results of digital process or decisions.

Both applications have been tested separately and are currently in the starting phase of a pilot project. Future work will focus on implementation of the proposed framework as well as simulation and testing. Thus the proposed application can be evaluated and further drafted.

All in all the described application could serve as a visionary tool for communicating with smart objects in an efficient and secured way but there is still a lot of research and work to do.

## References

1. Andrews, JG, Buzzi, S, Choi, W, Hanly, SV, Lozano, A, Soong, ACK, Zhang, JC (2014): What will 5G be? Selected Areas in Communications, IEEE Journal on,

32(6):10651082.
2. Armstrong, J., Virding, R., Wikstrm, C., Williams, M. (1993). Concurrent programming in ERLANG.
3. Barchnicki, S (2016): Eine Antwort auf die Frage nach effizienter Kommunikation von Morgen, IT-Sicherheit.
4. Beutelspacher, A (2005): Kryptologie. Eine Einfhrung in die Wissenschaft vom Verschlsseln, Verbergen und Verheimlichen ; ohne alle Geheimniskrmerei, aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergtzen des allgemeinen Publikums. 7. Auflage. Vieweg, Wiesbaden.
5. Chou, P. A., Wu, Y., Jain, K. (2003): Practical network coding.
6. Frosch, T., Mainka, C., Bader, C., Bergsma, F., Holz, T. (2014). How Secure is TextSecure?.
7. Hertlein, M., Manaras, P., Pohlmann, N.(2016): Die Zeit nach dem Passwort Handhabbare Multifaktor-Authentifizierung fr ein gesundes Eco-System, DuD Datenschutz und Datensicherheit Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag.
8. Hertlein, M., Manaras, P., Pohlmann, N.(2015): Abschied vom Passwort Authentifikation fr ein gereiftes Internet, IT-Sicherheit Management und Praxis, DATAKONTEXT-Fachverlag.
9. Hertlein, M., Manaras, P., Pohlmann, N.(2015): Bring Your Own Device For Authentication (BYOD4A) The XignSystem. In Proceedings of the ISSE 2015 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe 2015 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag.
10. Manaras, P(2016): "Konzeption und Implementierung eines Identity Providers auf Basis von FIDO UAF und OpenID Connect Verifikation der Identitt mit der Xign-Technologie", Master-Thesis.
11. Mörl, Susanne; Heiss, Michael; Richter, Alexander (2011): Siemens: Wissensvernetzung mit TechnoWeb 2.0,Schriftenreihe zu Enterprise 2.0-Fallstudien Nr. 09,Andrea Back, Michael Koch,Petra Schubert,Stefan Smolnik (Hrsg.) München/St.Gallen/Koblenz/Frankfurt: Enterprise 2.0 Fallstudien-Netzwerk, 02/2011, ISSN 1869-0297
12. Rappaport, TS, Sun, S, Mayzus, R, Zhao, H, Azar, Y, Wang, K, Wong, GN, Schulz, JK, Samimi, M, Gutierrez, F (2013): Millimeter wave mobile communications for 5G cellular: It will work! Access, IEEE, 1:335349.
13. WhatsApp-Security-Whitepaper(2016).
14. Zappavigna, M. (2011). Ambient affiliation: A linguistic perspective on Twitter. New media & society, 13(5), 788-806.