Smart Authentication, Identification and Digital Signatures as Foundation for the Next Generation of Eco Systems

80

Markus Hertlein, Pascal Manaras, and Norbert Pohlmann

Abstract

Nowadays the daily live relies on digital identities, mainly in the context of the Internet. These identities are used for opening a bank account, for online shopping, to access company resources in the business environment and in many more situations. Therefor it is necessary to have strong identification and authentication of the identities owner and to create legally binding electronic signatures. Today password- and TAN-based authentication is still the most prevalent form of authentication. But with new requirements emerging from new scenarios like the Internet-of-Things (IoT) password-based authentication mechanisms become outdated. A new approach for identification, authentication and electronic signature creation is the use of the user's smartphone, equipped with cryptographic material in combination with protocol-based authentication instead of transmission of secrets. Furthermore this setup enables the use of one system in different scenarios and ECO-Systems. Interoperability and federation with existing authentication and identification systems is the key for a wide spread acceptance by service providers. From the users point of view the use of its own smartphone is more comfortable than handling passwords and usernames. That leads to a high level of acceptance by potential users. The idea is to provide an adaptive multifactor authen-

M. Hertlein (✉) · P. Manaras
XignSys GmbH
Gelsenkirchen, Germany
e-mail: hertlein@xignsys.com

P. Manaras
e-mail: manaras@xignsys.com

N. Pohlmann
Institute for Internet-Security
Gelsenkirchen, Germany
e-mail: pohlmann@internet-sicherheit.de

C. Linnhoff-Popien et al. (eds.), *Digital Marketplaces Unleashed*,
https://doi.org/10.1007/978-3-662-49275-8_80

tication that can be used flexibly in many different use cases from business or IoT-platforms to the use in the urban environment of smart-cities. For an easy integration and a high degree of usability different entry points for authentication and electronic signature creation are used. As example for a modern and smart identification, authentication and electronic signature system the XignQR system [1] will be described in the following chapters.

80.1 Introduction

20 years ago only a few people would have thought, that the rise of the Internet would affect our lifestyles in such a fundamental way, as it's the case today. The handling of transactions, the opening of a bank account and even shopping are only the beginning of internet-based applications. As a whole, all provided services gain sensibility in the face of its users' data, which is a part of their digital identities and thus needs to be stored in a secure manner. The access to and the use of a digital identity need to be restricted to the user, which it represents. To check if a user is the user he claims to be and if he is allowed to use a certain digital identity, different service providers use different forms of user authentication. On one hand this authentication chaos leads to many different trust levels of the provided digital identities. On the other hand the user has to manage all these different authentication forms (s. Fig. 80.1). The effect is that the usability and the security of the system are limited.

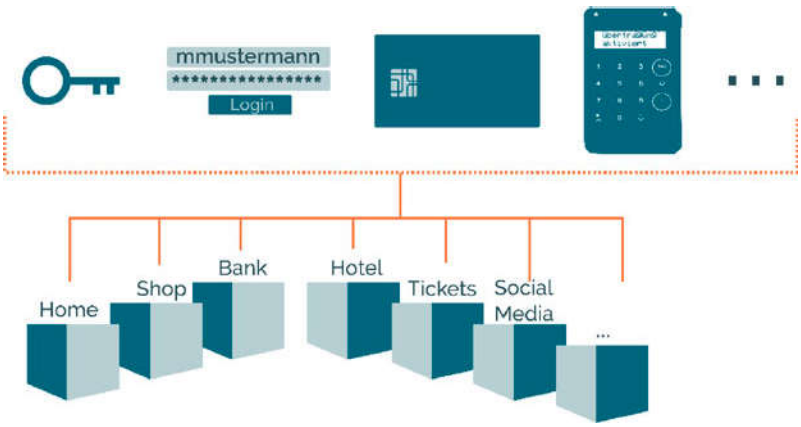

Fig. 80.1 Overview of the different authentication forms

80.1.1 Trust Is Everything

Passwords & The Hack of TV Monde

The most prevalent form of authentication is the combination of an username and a corresponding password. This form is considered as insecure and longwinded [2]. To counteract these problems, XignSys developed a concept for a modern authentication and digital signature system called XignQR, that doesn't rely on passwords, but on strong cryptography. Relying on a challenge response mechanism and backed by a PKI [3], XignQR eliminates the need for passwords completely. As passwords are the most prevalent form of authentication today, they have to be very secure, to prevent fraud or identity theft. Secure passwords have certain properties, such as a minimal length or special characters that must be contained, that add to the complexity of the use of passwords. As a result the password will be written down or stored in an insecure manner by most users.

The consequences of handling passwords that way were demonstrated by the hack of TV Monde a French TV broadcaster. The passwords needed for authentication were written down on piece of paper that was visible during a live news broadcast and were subsequently exploited by hackers.

Validity of Data

Since more and more commercial Internet services emerge, a service provider needs to have confidence in the data that is provided by its users. Therefore he must ensure that the data provided is valid, to prevent identity fraud and to protect its business. In this context XignQR offers two very trustworthy identification mechanisms that rely on the new German identity card. Besides being able to electronically read the information stored on the id card, XignQR supports a new mechanism called VideoIdent, with which the user is identified via a video chat application while presenting the id card and certain built in security features.

Several service providers depend on the personal data of users in order to deliver their services accordingly. Besides that, most users are registered with more than one of them (e. g. EBay and Amazon). That means, that their data is spread over all services they registered with. With XignQR the spread of personal user data can be reduced.

The whole system is designed to store and deliver information of different kinds in many different formats. Relying on standard technologies and protocols, the system can be integrated into a variety of services. Using the XignQR system the user has total control over the flow of his personal data, as he can also prevent the transmission of his data to the service provider.

80.1.2 Achieving Trust in the User's Identity

Besides user identification, authentication is a main task for using a digital identity. The XignQR system uses the user's personalized smartphone as a personal authentication de-

vice (PAD) and a QR Code for the identification of a service provider (e. g. Website, Terminal, Shop System, . . .). The authentication process can be described as: 1. Scan QR Code 2. Check the required and optional attributes 3. Confirm the process.

Due to the use of the QR Code, the XignQR System can be used everywhere a QR Code can be displayed or printed. Using smartphone as PAD results in to two main benefits: On one hand a personal digital identity could be used in a variety of use cases beginning from the login at webpages at home or at work to the authentication at terminals in urban areas. On the other hand it is possible to provide a very secure solution that is still easy to use.

Strong Adaptive Multi-Factor-Authentication
XignQR introduces a smart mechanism for authentication – called adaptive multi-factor authentication (A-MFA) – that makes use of the user's and the service provider's preferences. The authentication factor can be dynamically negotiated during the authentication process. It is possible that a login into a website can be done by scanning the QR Code without any further interaction, only exposing a unique user-pseudonym for that service. But if a user wants to unlock a car-sharing vehicle, he can be forced to enter a PIN or to use a biometric factor or even a combination of several factors.

Authentication as a Service
Add to that, the infrastructure of the XignQR system cannot only be used to authenticate users, but also to authenticate any system against another. That means XignQR can also be applied in the context of the Internet of Things and Industry 4.0.

80.1.3 Affected Markets

National borders do not limit today's markets. Trading has developed to a globally interacting eco system. As part of the digital transformation the EU released the eIDAS regulation [4]. The eIDAS regulation enables the digitalization of all paper-based processes for national and international trading. XignQR relying on digital signatures and smartphone based A-MFA in combination with eIDAS, enables usable mobile digital signatures for legally signing documents, transaction, bills and other data in the cloud. That leads to a completely new set of use cases, simplifying our private and business lives.

80.2 Concepts

This chapter focuses on some of the core concepts of the XignQR system, which enables the development of new markets, such as mobile shopping but also secures existing markets such as Online-Banking, Online-Shopping and authentication in general. The main idea behind XignQR is the separation from the user data that is necessary to fulfill a service, the identification of the service and the authentication process itself. The general

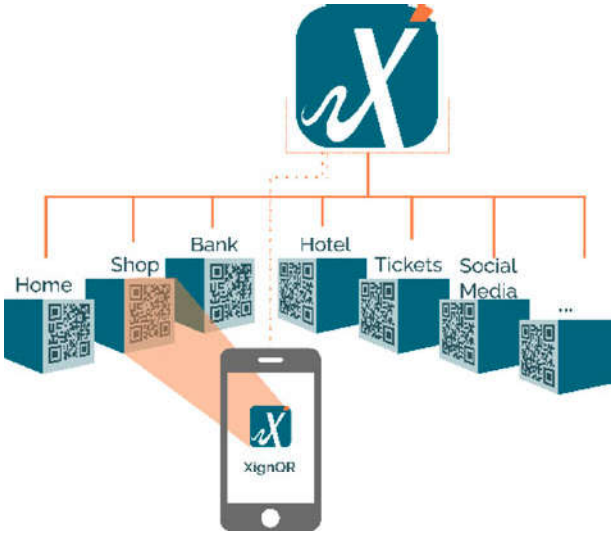

Fig. 80.2 Concept of the components interaction

idea is to have a QR Code to dynamically a service, the users personalized smartphone to authenticate the user and the trusted third party as trust anchor s. Fig. 80.2.

80.2.1 Requirements

A modern and secure authentication system, must fulfill several requirements to be widely accepted. Since acceptance is a requirement for the use of the system itself, we'll list the most important requirements:

- High Level of Security and low complexity
- Balance between security and usability
- Simple integration in existing systems
- Interoperability, flexibility and maintainability
- Protection of data and data thrift
- No additional hardware requirement (such as card readers)
- Transparency and informational self-determination
- Simple to manage

XignQR addresses these requirements through the use existing technologies. The wide spread of smart devices and the XignApp, as a part of the XignQR system, enables the use of the QR code as an entry point for authentication and thus the elimination of passwords in lots of different scenarios.

80.2.2 Registration & Identification

Digital identities build the foundation of authentication in the digital world. These identities are generated when the user registers with a service provider and consists of parts of the users real identity. Since the validity of data is essential to the service provider, the collection of data in a trustworthy manner is crucial. The trustworthy collection of data can be referred to as identification and is one of the most important features provided by the XignQR system. XignQR supports four Levels of identification, the trust levels. Each level distinguishes itself from the others by the trustworthiness of the collected data.

Level 1 – Not Verified
The user types in his personal data manually. The data has no trust anchor and is not verified. As a trusted third party does not verify the data, Level 1 is the lowest trust level supported by XignQR.

Level 2 – E-Mail Verification
The user verifies his identity via e-mail. During registration the user has to provide his e-mail address to which the system sends an e-mail containing a special link. Following this link verifies the possession of the provided address and thus the identity of the user. Since the only verified data is the e-mail address itself, this level is suitable for authentication at blogs or social networks, but not at e-business websites.

Level 3 – VideoIdent
The user proves his identity via video chat. A trained staff member that is connected to the user through the video chat application checks the user's identity. The German Federal Financial Supervisory Authority (BaFin) approved this form identification in 2014 and today several businesses emerged, providing or using such mechanism to identify their users at registration. The identification via VideoIdent is used especially in Germany, since on one hand the eID-functionality of the new German ID card, which enables the id card's ability to be electronically read, is not activated in most of the issued cards. On the other hand many service providers do not support eID as the required security infrastructure is very expensive. The use of VideoIdent only results in level 3 trust because the person checking the identity of the user can make a mistake at some point, which results in accepting false data or manipulated id cards.

Level 4 – eID
The user proves his identity via the eID-functionality of his id card. Since the data read from the card is sovereign information and the process of collecting the data cannot be prone to human error, it is very trustworthy [5]. Registration via the ID card results in the highest trust level supported by the system, because the design of the ID card guarantees confidence in the data read. At this point we have to add, that the security of and the con-

fidence in the data is achieved through a trade-off in usability, because every workstation must have a NFC card reader and an eID-client installed.

The data that is collected during the registration and identification process is converted into a distinct ID, the so-called derived identity. The derived identity can be represented in different formats, one of which is a representation as a digital certificate, which is used by XignQR. The digital certificate (i. e. the derived identity) is installed on the user's device during the personalization process and is subsequently used to authenticate against the system.

Personalization
The personalization process takes place right after the registration is completed. It consists of several stages involving the generation of digital certificates by a Public Key Infrastructure (PKI), binding the certificates and cryptographic keys to the device and storing necessary information in the system and on the device.

80.2.3 Strong Adaptive Multi-Factor-Authentication (A-MFA)

Authentication is achieved through interaction of all components of XignQR. This way XignQR offers strong and usable MFA providing several features such as pseudonymity to prevent tracking of users across multiple domains or services.

New Factors for Multi-Factor-Authentication
Additionally to the known factors possession, knowledge and inherence, XignQR realizes new combinations of factors. Through the cryptographically bound hardware token (XignSC) a new scheme called multiple possession is introduced by which the requirement for input of a PIN is eliminated. Authentication via PIN and VideoIdent can be requested for access management in high security environments or for critical processes. During authentication the user must then present his ID card and type in his PIN to accomplish the process.

Multi-Layered Security
Since the system counts on smart devices as a personal authentication device, the sensors of the device can add to the security of the authentication process. In general the information used, is called contextual information and consists of GPS data, network information and data of other sensors such as the gyroscope or the acceleration sensor. The information is processed and analyzed by the system to increase the trust in the authentication process. The processed information can be used to detect fraudulent behavior and forms the base for the request of additional authentication factors during authentication.

Choose the Required Authentication Factors

The user can choose the authentication factors, which are required for the use of the XignApp. For non-critical applications he can for example forgo the use of PIN and is thus able to use the XignApp without further interaction. That means the user can set its own personal security level. While this might be beneficial for the user, the security of a service provider can also be jeopardized through this mechanism. As a result the use of the right authentication factors depends on both parties, the user and service provider. If a user's personal security level is too low, the service provider is able to enforce a certain security level for the authentication.

Smartphone as a Secure Display

While using password based authentication mechanisms the user has no insurance that the display shows correct data. XignQR provides a secure display using the smartphone and the XignApp. The XignApp shows information about the service provider. Additionally the user can choose which personal information is transferred to the service provider. If the authentication takes place in the process of carrying out a transaction, the XignApp also shows the transaction data, which will be processed by the server. s. Fig. 80.3. The user can verify the validity of the shown data. Any tampering can thus be recognized and the void transaction can be cancelled.

Fig. 80.3 XignAPP with data to be verified before signing. Example payment transaction

80.2.4 Beyond Authentication

For the process of digitalization it is necessary to have trusted and legally bound processes. The foundation for legal digital processes is electronic signatures. As mentioned the European Union has released the eIDAS regulation. The eIDAS regulation allows two new kinds of electronic signatures. The first on one is the creation of electronic seals. Electronic seals are signatures bound to legal instead of natural persons. The second innovation is the possibility to create legal electronic signatures in the cloud, the Remote Qualified Electronic Signatures (rQES).

Remote Qualified Electronic Signatures With rQES the user has the possibility to digitally sign contracts and documents and to checkout shopping carts of online shops while on the go. Due to that fact many new use cases are emerging. The creation of legal electronic signatures needs a very high level of trust and confidence. Therefor strong identification and authentication is mandatory. XignQR with its smartphone-based A-MFA offers an authentication form that allows creation of rQES. Furthermore the QR code initiated authentication process matches the flexibility and usability that is necessary to reach many users and service providers.

For the user and for the service provider the sequence for creating a rQES is very similar to the authentication process. The service provider sends the data that should be signed to the XignQR signing service and receives a QR code. The user scans the QR code with his XignAPP. To be able to validate the data, the XignApp displays the corresponding information to the user before signing. s. Fig. 80.3. If the user accepts the data and initiates the signing process the strong authentication process will be started. On success the data will be signed on the server-side and transmitted to the service. For the user the whole process is as easy as the authentication process.

80.3 The Use Cases

This section focuses on the use cases that are covered by the XignQR system. The use cases are categorized and distinguished by different sectors.

80.3.1 Governance

Over the years governments started offering certain governmental services to their citizens to relieve the corresponding agencies of their workload, which in turn means a reduction of costs. The provided services range from the reservation of license plates to the notification of a change of one's residential address. To fulfill their services these institutions have to identify the user. Since in Germany the majority of citizens refused to activate the eID functionality of their id cards only a few citizens are able to use the governmental services, because the agencies don't support any other authentication mechanism.

With XignQR agencies are able to provide services all users alike, as the data collected in level 3 and 4 is sovereign and thus trusted.

80.3.2 Enterprise

In an enterprise there are lots of tasks that require authentication. Employees must authenticate to gain physical access to the premises of their workplace, typically realized via a smartcard-based employee ID cards. The employee then has to log into his workstation using his password and username, which were generated by the IT department of their employer.

Besides recovering lost and replacing stolen passwords, the IT department also has to enforce change of these regularly which adds to the complexity of IT management. The larger the enterprise the larger complexity dealing with passwords. Since XignQR can be delivered as on-premise solution, these complexities can be dealt with easily, because XignQR does not rely on passwords, but on a Public Key Infrastructure. Lost or stolen credentials can be revoked and replaced easily with a single click.

Alongside authentication, signatures also play a major role in larger enterprises. There are contracts, transactions or vacation requests that have to be authorized by a superior. Problems occur if one or more superiors are not available, due to illness or external meetings.

These problems are conquered using XignQR. Relying on asymmetric cryptography the concept of digital signatures is used throughout the whole XignQR system. Using the smartphone enables superiors to easily sign, which has to be signed. Additionally the amount of paper used, can also be drastically reduced, hence enabling digital transformation.

80.3.3 Financial Sector

In the financial sector every single process needs a high level of confidence. Starting from the access to the online banking portal over stock trading to all kinds of direct trading from B2C, C2C, and B2B.

In particular the security level and the usability level can vary in a very broad range in the financial sector. One the one-side there are high-value transactions that have to be confirmed by more than one person and must strictly bound to a user and on the other-side there are low-value transaction, where the user wants the transaction to happen seamlessly.

XignQR with its ability to manage the level of trust between security and usability, is able to answer this challenge.

For example, a transaction that transfers a high value could be secured with the combination of three factors. Therefor the signature will only be created if the user is in

possession of the XignAPP, knows the corresponding PIN and a face-recognition algorithm has verified the user's identity by the use of the smartphone camera.

A low value transaction could be signed using the XignAPP in combination with a PIN omitting the confirmation display.

80.3.4 xCommerce

Commerce and shopping use cases are depending on transaction and user attraction. In the online environment a shop must be very easy to use. In the best case the user is able to purchase products without the need of long registration processes. If the user has to authenticate itself against the shop, the authentication failure rate must be as small as possible. If that criteria are not matched the shop will miss spontaneous purchases.

XignQR enables an online shop owner to focus on its products, instead of the user-management processes. A XignQR user can fill his shopping cart and start the direct checkout by scanning the displayed QR Code. The items of the shopping cart will be concatenated with the users personal data and will be signed using the user's personal cryptographic material. The shop owner is now able to invoice. With XignQR e- and mCommerce and retail trade can be easily connected. The QR Code cannot only be generated dynamically. A static QR code can be used to identify items instead of service providers. An example in which retail trading and online commerce get in touch is the window shopping scenario. s. Fig. 80.4.

Fig. 80.4 QR Codes as bridge between retail trading and online commerce

80.3.5 Online – X

Most users will use XignQR for their daily online life that consists of logging into blogs, social networks or other platforms, that don't need much of user information. Most sites operate on a single verified information, i. e. the email address. Though these sites pose little to no harm to the user if credentials are lost or stolen (financial loss or endangerment of personal health), no one wants attackers to harm one's online reputation. XignQR helps service providers such as blogs, platforms or other websites to prevent the taking over of accounts by attackers. XignQR is designed to be easily integrated into websites via several protocols SAML or OpenID Connect and facilitates the protection of user accounts.

80.3.6 Internet of Things and Industry 4.0

It is predicted that until 2020 there will be up to 30 billion devices [6] connected to the Internet. To ensure a minimum level of security every device has to be authenticated to be able to automatically access data and resources. Beside the authentication of the device to a network and other devices, the authentication by a user against IoT devices will be one of the most authentication scenarios in the near future. Because of the amount of authentications it will be necessary that the authentication process is easy, fast and secure.

Since IoT connects the real and digital world IT security and thereby strong authentication becomes an important part to ensure safety.

The DDOS attacks with the "Mirai botnet" [7] in October 2016 shows, that the use of password-based authentication is insufficient.

To solve the IoT password problem the devices can be equipped with digital certificates and digital attribute certificates. With that combination the IoT devices can be connected to the XignQR infrastructure. The devices are now able to authenticate them self against other devices connected to the XignQR infrastructure in the same way a user will authenticate its self by using the smartphone. The authentication process is completely the same, only the smartphone is replaces by the IoT device. The entry point for the devices authentication can be a QR Code, like it is in the users authentication process, but also other authentication trigger can be included, for example an alert of an temperature sensor.

The identification of a device with a QR Code or NFC trigger helps to gain maximum flexibility. If a user wants to interact with an IoT device, it can use XignQR to authenticate itself in the same way the user authenticates itself against a website. On the one hand XignQR implements a high level of security by the substitution of the insecure password based authentication, for example the mentioned "Mirai Botnet" attack could not be realized with the use of XignQR. And on the other hand a user can easily interact with the IoT devices [8], also in an environment where the implementation of keyboards or other hardware is expensive or no possible, for example in the urban environment of "smart cities".

The digitalization of the production industry leads to many different and complex scenarios. It starts with the connection of different departments within a company and ends with the interconnection of production machines and the automation of production and business processes, based on decisions invoked by a machine signal. Therefor it is inalienable that process and data is authenticated.

But even the existing problems in the industry environment can be solved with XignQR. For example a massive problem is the access to production machines for maintaining.

Today the physical access to production machines is still done with a mechanical key and lock. To access the terminal at a production machine a strong password up to twenty and more characters is needed.

This combination is highly insecure and needs a lot of administration. For example, a maintenance worker needs to get the key to gain physical access and the strong password. The passwords are usually written down, because nobody is able to remember these types of passwords. Sometimes the passwords are directly noted at the terminal of the production machine.

The use of strong and flexible certificate based authentication is a solution the addresses all the mentioned problems.

Using XignQR improves the user experience for the administration and for the maintenance worker. An administrator can grant physical access for a defined timeframe to an explicit user or user group. And at the terminal there is no need for passwords, thereby no passwords can be written down at the terminal. Since the system can be remotely managed, also authorization processes can be implemented due to the substitution of the password.

80.4 The Authentication Process

The Fig. 80.5 shows the process of authentication with XignQR. Authentication is achieved through the interaction of the three main components of the system, the Xign Manager, the XignApp on the user's smartphone and the service provider. The Xign Manager builds the core of the system. It mediates between the XignApp and the service provider to authenticate users. Users are authenticated using the Xign App, while the Xign Manager delivers QR codes, authentication events and user information to the service provider, who then grants or denies access to his services on behalf of the received information. An authentication is initiated by the service provider that sends an authentication request to the Xign Manager. The Xign Manager responds with a QR code that has to be displayed to the user. The user scans the QR code using his Xign App to authenticate against the Xign Manager leveraging a cryptographic challenge-response-mechanism. The result of the challenge-response scheme is transferred back to the service provider afterwards. The result message contains the status of the corresponding authentication process and a token that is used to request the user information from the Xign Manager.

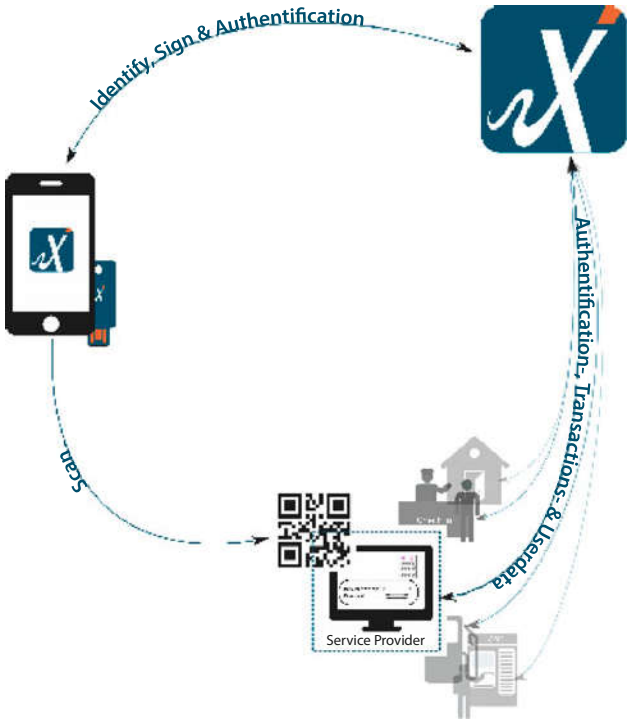

Fig. 80.5 Authentication process

References

1. M. Hertlein, P. Manaras und N. Pohlmann, "Bring Your Own Devide For Authentication (BYOD4A)," in *In Proceedings of the ISSE 2015 – Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 20151 Conference*, Wiesbaden, Springer Vieweg Verlag, 2015.
2. C. Okyle, "Password Statistics: The Bad, the Worse and the Ugly (Infographic)," [Online]. Available: http://www.entrepreneur.com/article/246902 [Accessed 17 August 2016].
3. S. Goswami, S. Misra und M. Mukesh, "A replay attack resilient system for PKI based authentication in challenge-response mode for online application," *3rd International Conference on Eco-friendly Computation and Communication Systems,* 2014.
4. E. Union, "REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/HTML/?uri=CELEX:32014R0910 [Accessed 17 August 2016].
5. M. Schröder und M. Morgner, "eID mit abgeleiteten Idenititäten," in *DuD Datenschutz und Datensicherheit 8-2013*, Heidelberg, Springer, 2006.
6. H. Bauer, M. Patel und J. Veira, "The Internet of Things: Sizing up the opportunity," [Online]. Available: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity. [Accessed 28 October 2016].
7. S. Cobb, "10 things to know about the October 21 IoT DDos attacks," [Online]. Available: http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/. [Accessed 28 October 2016].

8. M. Cagnazzo, M. Hertlein und N. Pohlmann, “Information and Software Technologies: An Usable Application of Authentication, Communication and Access Management in the Internet of Things,” in *22nd International Conference, ICIST 2016*, Druskininkai, Lithuania, Springer International Publishing, 2016, pp. 722–731.