Bring Your Own Device For Authentication (BYOD4A) – The Xign–System

Norbert Pohlmann · Markus Hertlein · Pascal Manaras

Institute for Internet-Security
Westphalian University of Applied Sciences
{pohlmann | hertlein | manaras}@internet-sicherheit.de

Abstract

The paper proposes an innovative authentication-system called Xign that is very easy to use, easily integrated in existing infrastructure, while offering strong multifactor-authentication for different domains of application, like web applications and physical access control. A QR code is all that is needed to provide an entry point of authentication to the user. The system comprises a smartphone application (Xign App), a server-component (Xign Authentication Manager) and a smartcard-applet (Xign SC). A NFC token contains a special smartcard-applet and a keypair which is protected through a user-selected PIN. To use this token for authentication, it must be paired with the users smartphone. To achieve that, the smartphone is also equipped with corresponding certificates. The Xign-system is backed by a Public Key Infrastructure (PKI). As trust-anchor the PKI depends on the attributes of the new German identity card or similar identity verification systems, which are used to generate a derived identity, that is subsequently stored into token. As a consequence the Xign-System also takes steps to ensure anonymity of the user, while preventing tracing over multiple authentications.

1 Authentication in Organisations

This chapter focuses on problems during authentication in organisations and shows two improvements and its limitations.

1.1 Problems

Mobile devices, such as tablets and smartphones, are on the rise to an extent, that they are used in nearly every situation in our daily lives. They are used personally, but also during work, resulting in a need to establish some form BYOD-Policy for the use in corporate networks containing sensitive data. Compromised personal devices, thus endanger the security of every network, which grants access to them.

In this context secure authentication and authorization of a user are as crucial as the use of strong cryptography to protect the user's personal information and in the end the security of the whole infrastructure involved.

Today authentication is primarily done via passwords. Password authentication is vulnerable to many attacks like Phishing or Bruteforce attacks and thus considered as insecure. The main problem is that the chosen passwords are often too easy to guess. Additionally a password is often used for more than one user account, adding to the insecurity of password protected user accounts.

There are not only problems regarding authentication and authorization, but also social problems regarding the privacy of every user in general:

In recent years IT security gained relevance, as there were several high-profile security breaches, such as the attack on Lockheed Martin in 2013. The secret operations of intelligence agencies have never before reached such a high level of intrusion into the personal lives of citizens, as shown by the documents revealed by Edward Snowden.

In general the trust in IT security, especially in IT security solutions provided by US businesses, is heavily shaken. Reports of NSA-backdoors, the deliberate use of weak cryptography and the tampering with hardware of Internet service providers to spy on users, are the most prominent reasons for this kind of distrust.

1.2 Approaches

Over the past years, there were many attempts to solve the security problems in connection with password authentication. As a result, several security solutions have found their way into the market.

Mainly there are two types of approaches: The field of One-Time-Passwords (OTP) and the field of X.509-Tokens and smart cards.

OTPs, as generated by the RSA SecurID Token, rely on a shared secret and can be used as single or second factor. OTPs especially improve the security if used as second factor. If, however, the secret is stolen, an attacker can easily generate his own OTPs, as shown in the hack of Lockheed Martin in 2013.

X.509 Token or smart cards use certificates and public key pairs. Because of the tamper proof design of smart cards, the private key is never exposed or transferred. As a result authentication is only possible, if the user has control over two factors: knowledge (PIN) and possession (smart card; the token itself). The X.509 Token has an advantage over OTPs: Because of contained digital certificates it is also possible to enable authentication across different organisations (bridging).

As shown, both approaches can be used for improving security during authentication in different realms. Since both approaches often require to align existing infrastructures appropriately, they are not easy to integrate. As a consequence the proposed system supports multiple protocols as well as direct integration, while maintaining usability.

2 Base Technologies

This chapter explains both established technologies, QR-Code and PKI, and how they are used to build an easy to use and modern authentication system.

2.1 QR Code

Quick Response codes (QR codes) are crucial for the Xign-System. They offer an easy way to contain information in a machine-readable fashion and are used to transfer the necessary information to start the authentication process, from the server to the smartphone application. The QR codes, as issued by the Xign Authentication Manager, contain compressed JSON-objects structuring the information. These codes are subsequently read by the smartphone's camera and processed by the smartphone application. A QR code's payload can be described as follows:

```
QRCode{
        String url;
```

```
                String signature;
                String id;
            }
```

The ***url*** property points to the corresponding endpoint at the authentication manager, the application needs to communicate with. The ***id*** property is required to match the client-session and the corresponding authentication-session. The ***signature*** property is used to ensure the legitimacy of the QR code and is verified by the application before starting the authentication process.

2.2 Public Key Infrastructure

The PKI consists of a Certification Authority (CA) and a corresponding Registration Authority (RA), which represents a user interface for administration and user management. An administrator is able to enrol new, delete old or manage existing users. Furthermore certificates of existing users can be revoked, ultimately preventing successful authentication with the system, this way providing a mechanism for efficient risk-management.

The RA is able to communicate with the CA to enrol users and to retrieve user certificates needed for token personalization, while providing an interface for smartphones to securely personalize software tokens.

3 Xign

This chapter gives an overview of the Xign-System and its components comprising the four core actors (Fig.1) authentication server, smartphone app, security token and service provider.

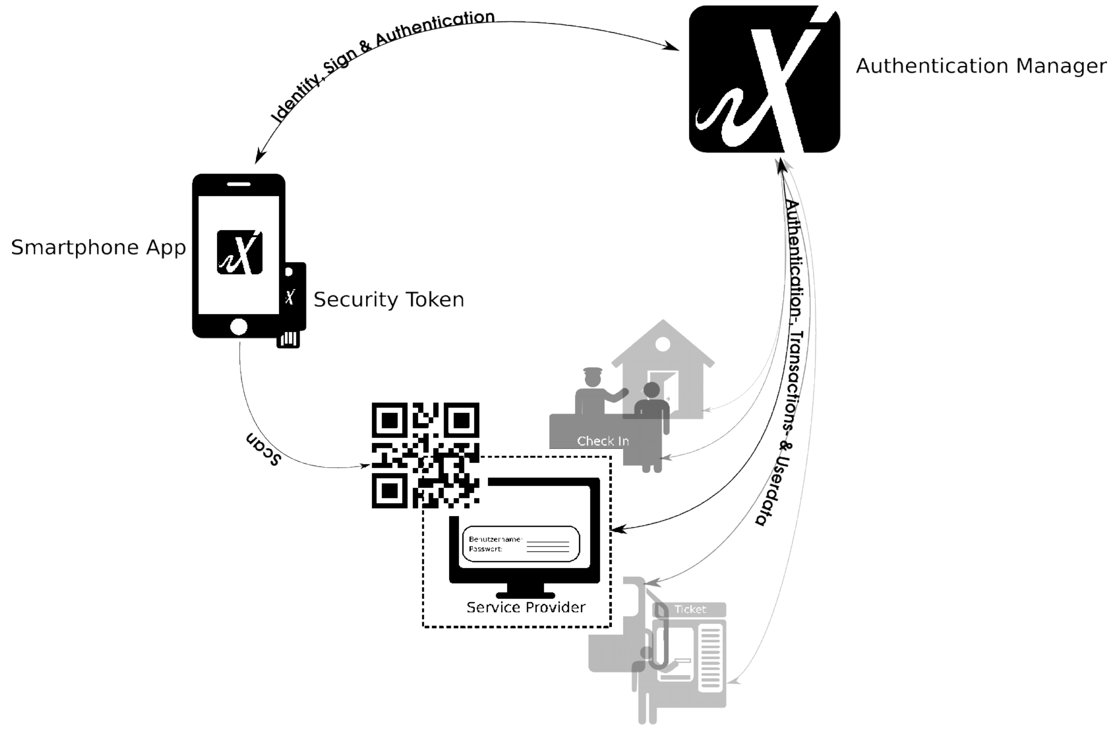


Fig. 1: Xign Overview

3.1 Concept

The Xign-System comprises of four actors: the smartphone application, optionally extended with a hardware token, the authentication server and the service provider. A service provider could be a Webshop and other Websites, an ERP system, a VPN server, the local workstation or a physical access control systems or any other system, that needs to grant access to its users.

The service provider represents a service the user wants to authenticate with. To enable the user to authenticate, the service provider retrieves a QR code from the authentication server and presents it to the user.

The user scans the QR code to start the authentication. The smartphone application processes the information contained and communicates with the authentication manager to authenticate the user.

The authentication manager mediates between smartphone application and service provider. It is responsible for delivering authentication events and QR codes to service providers and communicates with the corresponding smartphone clients to authenticate users. Authentication is done by using a PKI-backed challenge-response-protocol.

3.2 Components

Figure 2 shows the architecture of the Xign-System and their integration. It illustrates how the main components act together.

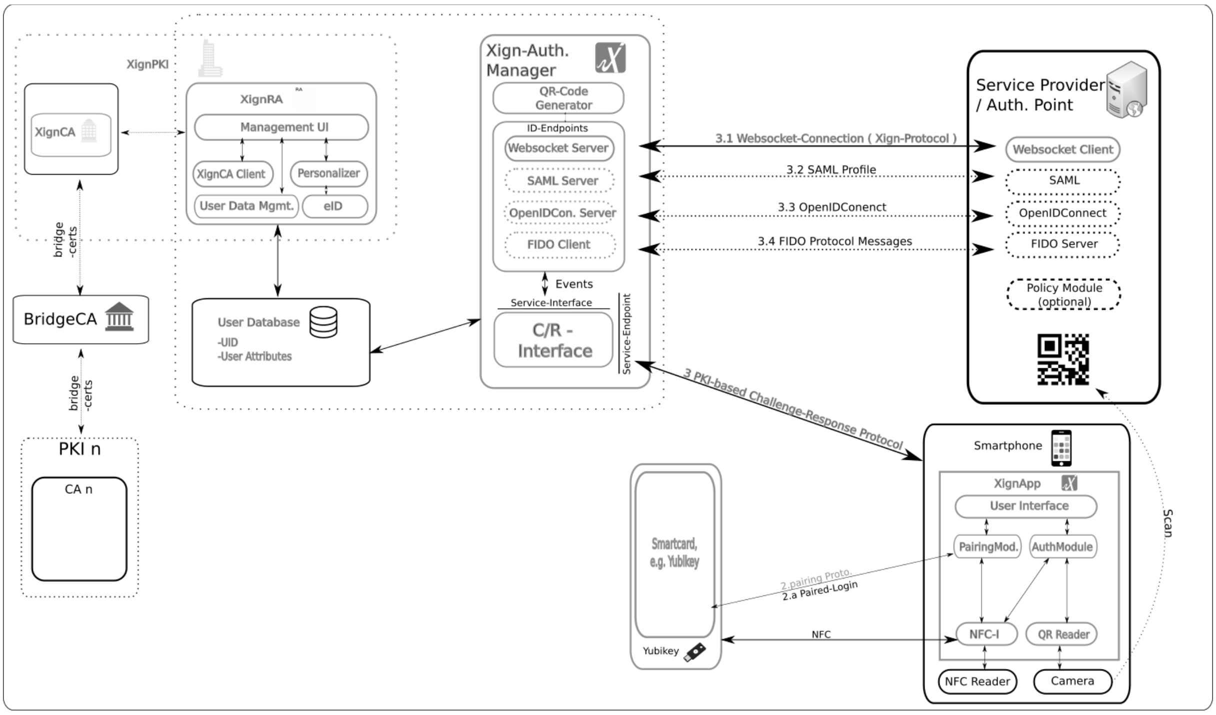


Fig. 2: Xign Components

3.2.1 Authentication Manager

ID-Protocols for Integration

Since existing solutions often require to align existing infrastructures appropriately, they are not easy to integrate. As a consequence the proposed system supports multiple protocols as well as direct integration.

As cloud computing becomes more prevalent, authentication with cloud services is crucial for every service provider. As a result it is important to support cloud based protocols:

- SAML

  The Security Assertion Markup Language (SAML), developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application [Adva].

- OpenID Connect

  OpenID Connect 1.0 is a simple identity layer on top of the OAuth 2.0 protocol. It allows Clients to verify the identity of the End-User based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the End-User in an interoperable and REST-like manner.

  OpenID Connect allows clients of all types, including Web-based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users. The specification suite is extensible, allowing participants to use optional features such as encryption of identity data, discovery of OpenID Providers, and session management, when it makes sense for them [Open].

- Xign-Protocol

  The Xign-Protocol is the proprietary protocol used by the Xign-System. It relies on the websocket-protocol for transport and uses JSON-Messages as payload. This protocol is also used by service providers to directly integrate Xign into their systems.

- FIDO

  The FIDO Alliance has two sets of specifications, U2F and UAF. The FIDO UAF strong authentication framework enables online services and websites, whether on the open Internet or within enterprises, to transparently leverage native security features of end-user computing devices for strong user authentication and to reduce the problems associated with creating and remembering many online credentials. The FIDO UAF Reference Architecture describes the components, protocols, and interfaces that make up the FIDO UAF strong authentication ecosystem [PhSS14].

Larger businesses typically manage their users using LDAP, RADIUS or other protocols. Because of that, it is mandatory to provide appropriate interfaces for these kinds of services, eliminating the need for duplication or transformation of existing user data.

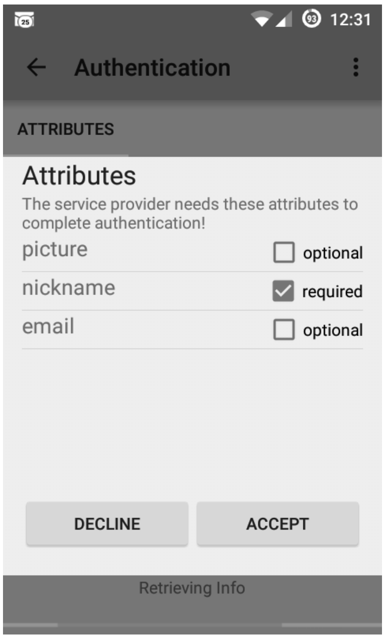
Service Protocols – Authentication

The challenge-response protocol is used between smartphone/token and authentication manager to authenticate the user with the authentication manager, while taking account of Phishing and MIT-attacks. Since there are no passwords, the whole system is secure from Phishing attacks. Furthermore the system is even secure against Man-In-The-Middle Attacks due to its PKI. Another benefit in using the PKI lies in the capability to authenticate with other Xign Authentication Managers through a process called bridging. The whole protocol consists of a set of JSON messages and thus is independent of its underlying transport-protocol.

3.2.2 Smartphone Application

The smartphone app acts as user interface, as QR-Code scanner and as token reader for the NFC Security Token. It is equipped with a public-private key pair and corresponding certificate. Because of the key pair and the need for a PIN, the smartphone can be used as soft-token providing two-factor authentication. If the smartphone is used as Security Token reader the key pair is used for pairing.

While authenticating, the smartphone provides contextual information, like location data. This information helps the user and the Authentication Manager to proof the validity of the authentication process.



Attributes

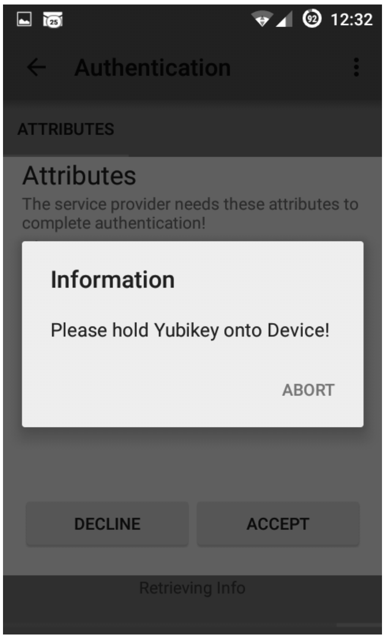
The service provider needs these attributes to complete authentication!

picture □ optional

nickname ☑ required

email □ optional

Fig. 3: Smarthpone Application Screenshot 1



12:32
Authentication
ATTRIBUTES
Attributes
The service provider needs these attributes to complete authentication!

Information

Please hold Yubikey onto Device!

Fig. 4: Smarthpone Application Screenshot 2

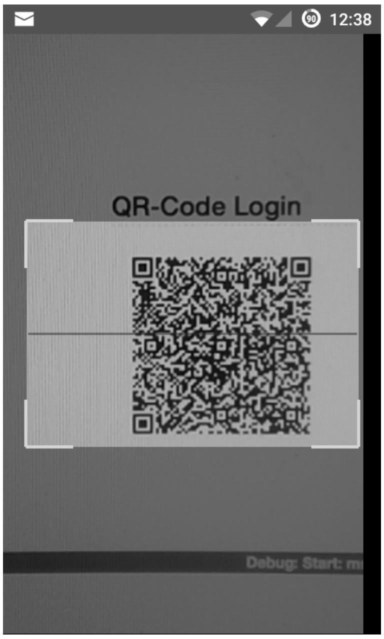


Fig. 5: Smarthpone Application Screenshot 3

3.2.3 Security Token

The system supports hardware tokens as well as software tokens. These tokens are so called X.509 tokens, containing a distinct key pair for each user.

At first the tokens need to be personalized. While hardware tokens can be personalized by authorized personnel, using the capabilities of the Registration Authority (RA), the software tokens need to be personalized with the help of the smartphone application, since software tokens are stored on the user device itself.

Additionally the hardware tokens can be paired with the user device to further enhance security. By pairing the hardware token with the device, the system ensures that authentication can only succeed, if the user uses both of these particular factors.

The keys stored in these tokens are used for signing the challenge, which is transmitted by the server. The Security Tokens are connected through Near Field Communication (NFC) or Bluetooth. NFC is the first choice on Android and Windows Phones, while Bluetooth is used on Apple's iPhone, since it lacks proper NFC-support.

3.2.4 Service Provider

There are different ways a service provider can integrate Xign into his systems. First of all Xign can be integrated directly, using the Xign Client Library. The Library offers a set of methods and objects to communicate with the corresponding authentication manager endpoint.

To facilitate integration in several scenarios and existing systems, Xign also supports several well-known protocols, such as OpenIDConnect, which is widely used even by large enterprises like Google and Facebook, as well as a set of SAML profiles. If the service provider already uses one of these technologies, integration is done by directing the authentication requests to the corresponding endpoint at the authentication manager.

3.3 Features

These are the main features of the Xign Authentication System:

3.3.1 Strong Authentication

End-2-End Encryption

Most protocols rely on SSL/TLS for encrypting the connection between two parties. Recent attacks and security issues showed that the dependence on SSL/TLS alone is not sufficient for establishing a secure encryption. Thus the proposed system implements an end-2-end encryption independent from the channel used.

To achieve that, the smartphone application, authentication server and service provider own a distinct keypair of its own. These key pairs are used to establish a session key between the communicating parties, based on a Diffie-Helman key exchange. The session key is used for encrypting each message. Additionally each message is also signed with the corresponding private key of the actor.

Pairing

Pairing is an extra feature provided by the smart card of the hardware token. During the pairing process the smart card and the smartphone are cryptographically bound together by calculating a secret, using its elliptic curve private key and the counterpart public certificate. The pairing protocol is based on the ECDH algorithm, AES encryption and mutual authentication.

A benefit of pairing the smartphone and the token is the realization of different security levels. Pairing results in a higher security level due the combination of two-times possession (personalized smartphone & paired hardware token) and one- or two-times knowledge (smartphone and/or token PIN) or in a higher usability level through two-times possession (personalized smartphone & paired hardware token) without any user input. The level of security can optionally be requested by the authentication point.

3.3.2 Multirealm Authentication

The authentication system relies on QR codes as triggers to start the authentication process. This design enables authentication without the need for extra peripheral devices, such as monitors or pin pads, resulting in a broader range of use cases.

The QR code can be displayed anywhere using stickers, monitors or even a sheet of paper, this way extending the domain of application beyond authentication with web applications. Imaginable use cases (Fig. 6) are ranging from physical access to premises to check-in systems in hotels, but also include claiming reservations in restaurants or at ticket terminals.

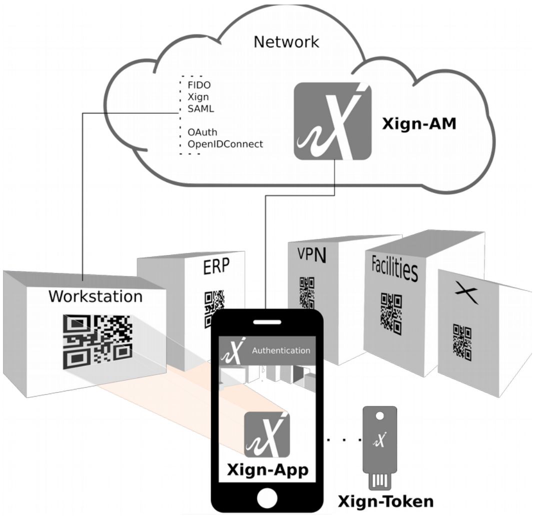


Fig. 6: Xign Multirealm Examples

3.3.3 Authentication Across Organisations

The fact that the whole authentication process is PKI backed not only leads to a quick and comfortable risk management, but also enables the feature of 'authentication across multiple organizations'. For this purpose the certificates of organizations offering authentication to one another are signed by a bridge CA. The certificate signed by the bridge CA becomes the new trust anchor for these organizations. Thereby the only requirement is to negotiate a policy between the organizations. There is no need for further software or hardware changes.

3.4 Functions

These are the current main functions of the Xign Authentication System:

3.4.1 Registration

Before users can be authenticated, they must be registered with the system. Registration can be done in different ways: For existing user data which is typically managed via LDAP or similar technologies, registration can be done automatically by using special adapters, effectively integrating the existing data sources.

New users are generally registered using the Registration Authority component of Xign. During registration the necessary user data is collected and stored. The stored information is then derived into a digital identity, a so called ***derived identity***, which is subsequently stored into a X.509 token and used for authentication later on. The process of storing the derived identity together with its corresponding key material is called personalization. Alternatively registration can be done using id cards, such as the new German identity card. These cards are suitable for the use in this context, as they contain sovereign information about a person, which is machine readable.

3.4.2 Authentication

The authentication process can be described as follows:

The user wants to authenticate with service provider in the realm of online services. To achieve this the service provider retrieves a QR code from the authentication server and presents it to the user. The user scans the QR code using his smartphone and the client smartphone application. The smartphone client communicates with the authentication server to authenticate the user and displays any information necessary to complete the procedure. Once the authentication process is finished an appropriate event is sent to the service provider, containing status information. Upon this information the service provider grants or denies the access to its system.

4 Threats

Phishing and similar attacks are not a threat, because there is no user interaction. Even a “stolen” QR-Code, that is placed at a different authentication point, will be detected by the system due the use of contextual information.

Using additional end-2-end encryption instead of only using plain TLS bears the advantage, that there are only the known threats, such as attacks on the PKI itself or on the infrastructure of the Xign-System (e.g. DDOS).

5 Outlook

The system can be extended in some different ways. First of all the system can be extended to support triggers different from QR codes, such as NFC tags or Bluetooth, to support devices lacking a suitable camera or to enable new use cases. NFC, for example, is commonly used for building and facility access and in automotive solutions.

As other smartphone applications may want to integrate smartphone-based two-factor-authentication, an API can be exposed to provide corresponding entry points to the calling application. Same goes for authentication in smartphone browsers.

The system also can be extended to support qualified signatures for different domains of application. In the domain of financial Services, e.g. Online Banking and Payment Services, the Xign-System can be used to accelerate and secure the execution of transactions. In a business environment Xign helps to securely digitalize the paper-based processes. Since the smartphone is used to sign data with the personal key of the user, it is particularly suitable for this use case, because any signature can be matched to a specific user and a corresponding authentication, thus providing non repudiation.

6 Conclusion

To enable the authentication of users by using their personal devices, the authentication system needs to be designed to be flexible. Since most enterprises use a well integrated infrastructure, the system needs to be easily integrated into the target system without the need to align the existing infrastructure.

Ideally the system does not depend on passwords, as the problems regarding that type of authentication are well-known. Most passwords are either easy to guess or, if password policies are in effect, not easy to remember. Systems that are not easy to use, typically won’t be used as frequent as their easier, maybe more unsafe counterparts.

A more suitable approach is the use of X.509 tokens for authentication as there is no symmetric secret that can be stolen. The whole system relies on two factor authentication.

Usability is achieved by the ease of use of the proposed system, as the user only needs to scan a QR code and remember a simple PIN, if any, instead of a complex password.

References

[DSBL10] Dodson, Ben, Sengupta, Debangsun, Boneh, Dan, Lam, Monica S.: Secure, Consumer-Friendly Web Authentication and Payments with a Phone. In: Processdings of MobiCASE 2010, the Second International Conference on Mobile Computing, Applications, and Services, p. 17-37.

[FePo08] Feld, Sebastian, Pohlmann, Norbert: Security analysis of OpenID, followed by a reference implementation of an nPA based OpenID provider. In: Information Security Solutions Europe (ISSE) conference, Madrid, Spain, 2008.

[Tech] Technology Nexus AB: Mobile PKI Security, Potential, Challenges and Prospects. In: https://www.nexusgroup.com/contentassets/0b5f8d23e4be466bb698b6f91769bb8f/nexus-white-paper-mobile-pki-en.pdf

[LiWe05] Liang, Wei, Wang, Wenye: On performance analysis of challenge/response based authentication in wireless networks. In: Computer Networks, Volume 48, Issue 2, 2005, p. 267–288.

[PhSS14] Philpott, Rob, Srinivas, Sampath, Kemp, John: UAF Architectural Overview. In: https://fidoalliance.org/specs/fido-uaf-overview-v1.0-rd-20140209.pdf, 2014.

[Pint12] Pintor Maestre, David: QRP: An improved secure authentication method using QR codes. In: https://www.grc.com/sqrl/files/QRP-secure-authentication.pdf, 2012.

[Bund13] Bundesamt für Sicherheit in der Informationstechnik, BSI: Überblickspapier Consumerisation und BYOD. In: https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile, 2013.

[Mtit] MTI Technology: Bring Your Own Device. In: https://mti.com/Portals/0/Documents/White%20Paper/MTI_BYOD_WP_UK.pdf.

[Open] OpenID Foundation: What is OpenID?. In: http://openid.net/connect/.

[Adva] Advancing open standards for the information society (OASIS): OASOS Security Services (SAML) TC - Overview. In: https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

Index

Authentication Across Organisations, Bridging, Bring Your Own Device, FIDO, Mobile Computing, Multi-factor Mutlirealm-Authentication, OpenIDConnect, Public-Key Infrastructure, QR Code, Token-Authentication, Usability