Authentifikation für ein gereiftes Internet

Abschied vom Passwort

Die sichere und datenschutzkonforme Aufbewahrung und Nutzung der digitalen Identität hat zum heutigen Zeitpunkt einen höheren Stellenwert als jemals zuvor. Der Nutzung jeglicher Internetdienste liegen die Identifikation und die Authentifizierung des Dienstnutzers und des Dienstanbieters zugrunde. Die dafür erforderlichen Daten reichen von einem Pseudonym bis hin zu vollständigen Personendaten. In der Praxis ist nach wie vor die Kombination aus Nutzername und Passwort die häufigste Authentifizierungsmethode, ein erwiesenermaßen sehr anfälliges Verfahren, das dem modernen Internet längst nicht mehr angemessen ist. Das Institut für Internet-Sicherheit hat mit Xign eine passwortlose, einfach zu integrierende und leicht verwendbare Authentifizierungs-Technologie geschaffen.

Das Internet hat sich in den letzten 25 Jahren in seiner wirtschaftlichen Bedeutung rasant entwickelt. Aus einem losen Verbund an Informationen entstand ein weltumspannendes Netz mit zahlreichen wichtigen Kommunikations- und Handelskanälen. Heutige Kerngeschäfte im Internet sind zum Beispiel der Online-Handel (e-Commerce), das Nutzen von Online-Banking-Portalen und die zentrale Datenspeicherung in der Cloud. Im Business-Bereich steht der Zugriff auf Ressourcen durch autorisierte Personen aus allen Teilen der Welt im Vordergrund.

Während die IT-Infrastruktur zu Beginn des digitalen Zeitalters aus homogenen Komponenten bestand, liegt heutzutage ein in hohem Maße heterogenes Umfeld vor. Die größte Entwicklung macht sich im Bereich der Nutzerendgeräte bemerkbar. Erst waren es die PCs, dann die Notebooks, heute Smartphones/Tablets und morgen werden es zunehmend Wearables sein.

Authentifizierung im Unternehmen

Die Nutzung mobiler Endgeräte (Smartphones und Tablets) für den Internetzugang ist inzwischen fester Bestandteil unseres Alltags. Sie werden im privaten, aber auch im beruflichen Umfeld verwendet, so dass sich Unternehmen oft gezwungen sehen, eine Form von BYOD-Policy zu etablieren (BYOD = „Bring Your Own Device"). Aber: Kompromittierte Endgeräte gefährden jedes Netzwerk, das ihnen Zugang gewährt.

In diesem Kontext ist eine **moderne** und **sichere Authentifizierung** eines Nutzers enorm wichtig, um für einen zuverlässigen Schutz der persönlichen Daten zu sorgen. Aber auch, um für den Schutz der immer wichtiger werdenden IT-Infrastruktur zu sorgen.

Die primäre Form der Nutzerauthentifizierung ist heute immer noch die Kombination aus einem Nutzernamen und einem dazugehörigen Passwort. Die Authentifizierungsmethode Passwort war noch nie sicher und wird es auch in der Zukunft nie werden. Die Probleme und Angriffsmöglichkeiten sind sehr vielfältig, so sind zum Beispiel Brute-Force- oder auch Phishing Angriffe häufig sehr erfolgreich. Oft sind Passwörter aber auch einfach zu schwach gestaltet und können von Angreifern somit leicht erraten werden. Zudem werden Passwörter häufig über verschiedene Nutzerprofile hinweg benutzt, ein Umstand, der noch weiter zur Unsicherheit von Passwörtern beiträgt.

Dennoch wird das Passwort als Authentifizierungsmethode immer noch sehr breit genutzt, obwohl inzwischen viel sicherere Authentifizierungsmethoden zur Verfügung stehen. In diesem Zusammenhang steht besonders der Begriff **Multifaktor-Authentifizierung** im Vordergrund.

Viele Unternehmen setzen dabei auf Smartcards oder OTP-Tokens (One Time Password) als Basis für die Authentifizierungsmethode. Diese Ansätze eliminieren zwar die Abhän-

gigkeit von den klassischen Passwörtern, erfordern allerdings einen erhöhten Aufwand und eine Ausrichtung der IT-Infrastruktur des Unternehmens auf die Zieltechnologie. Des Weiteren sind die verschiedenen Lösungen nicht interoperabel und somit in ihrer Anwendung beschränkt.

Aus diesem Grund wurde im Rahmen von Forschungsaktivitäten im Institut für Internet-Sicherheit die **Xign-Technologie** geschaffen, um ein passwortloses, einfach zu integrierendes und leicht verwendbares Authentifizierungssystem in vielen alten und neuen Anwendungsfeldern nutzbar zu machen.

Die Basistechnologie

Die benötigten Technologien, um ein einfaches und modernes System zur Authentifizierung zu entwickeln, stehen uns schon seit längerem zur Verfügung. Die beiden Basistechnologien, auf denen das Xign-System beruht, sind der Quick Response Code (QR-Code) und eine Public-Key-Infrastruktur (PKI), mit allen notwendigen Verschlüsselungs- und Vertrauensdiensten.

Bei einem QR-Code handelt es sich um einen maschinenlesbaren 2D-Barcode, mit dem die benötigten Informationen zur Einleitung der Authentifizierung vom Server (XignManager) zur **XignApp** übertragen werden. Der QR-Code wird nachweislich vom **XignManager** ausgestellt und enthält keine sensiblen Daten.

Die PKI besteht aus einer Certification Authority (CA), die dazu dient, Nutzer- und Server-Zertifikate zu erstellen, sowie der Registration Authority (RA), die zur Nutzeridentifizierung, -registrierung und -verwaltung dient. Jede Komponente, die an dem Authentifizierungsprozess beteiligt ist, wird durch ein asymmetrisches Schlüsselpaar und das damit korrespondierende digitale Zertifikat repräsentiert. Neben der Verbindlichkeit und der Integrität wird durch die PKI auch ein einfaches, schnelles und kostengünstiges Risikomanagement ermöglicht.

Das Konzept

Das Xign-System besteht grundsätzlich aus vier Akteuren: der Smartphone-Applikation **(XignApp)**, optional erweiterbar durch einen Hardware-Token **(XignToken)**, dem Authentifizierungsmanager **(XignManager)** und der Einbindungskomponente **(XignIn)** beim Dienstanbieter. Ein Dienstanbieter kann zum Beispiel eine Website, ein ERP-System, ein lokaler Arbeitsrechner oder irgendein anderes IT-System (SmartHome, Elektrozapfsäule, Auto ...) sein, das Zugriff für seine Nutzer gewähren muss.

Der **Dienstanbieter** repräsentiert einen „Dienst", gegen den der Nutzer sich authentifizieren möchte. Um dem Nutzer die Authentifizierung zu ermöglichen, ruft der Dienstanbieter (XignIn) einen QR-Code vom **XignManager** ab und zeigt ihn dem Nutzer. Der Nutzer liest anschließend den QR-Code mit Hilfe seiner **XignApp** ein, um die Authentifizierung zu starten. Die Anwendung (XignApp) verarbeitet die darin enthaltenen Informationen und kommuniziert mit dem XignManager, um den Nutzer schließlich zu authentifizieren.

Der **XignManager** vermittelt zwischen der XignApp und dem Dienstanbieter. Er ist dafür zuständig, Authentifizierungsereignisse und QR-Codes an Dienstanbieter auszuliefern und kommuniziert mit den Smartphone-Clients, um die Nutzer zu authentifizieren. Die Authentifizierung wird mit Hilfe eines PKI-basierten Challenge-Response-Verfahrens realisiert.

Das Bild zeigt die Architektur des Xign-Systems und seine Integration. Es zeigt, auf welche Weise die verschiedenen Xign-Komponenten miteinander in Verbindung stehen.

XignManager

ID-Protokolle für die Integration

Die existierenden Lösungen für die Nutzerauthentifizierung erfordern zwangsläufig eine entsprechende Ausrichtung der IT-Infrastruktur und sind deshalb nicht ohne großen Aufwand in bestehende Systeme integrierbar. Da Cloud Computing immer mehr an Relevanz gewinnt, wird auch Nutzerauthentifizierung in der Cloud immer wichtiger. Aus diesem Grund unterstützt das Xign-System die folgenden Protokolle, um Xign in bestehende Systeme zu integrieren:

- SAML
- OpenID Connect
- Xign-Protokoll
- FIDO UAF

Das Xign-Protokoll ist ein proprietäres Protokoll, das vom Xign-System verwendet wird. Es baut dabei vor allem auf dem Websocket-Protokoll und JSON-Nachrichten auf. Das Protokoll kann von Dienstanbietern dazu verwendet werden, Xign direkt in das System zu integrieren.

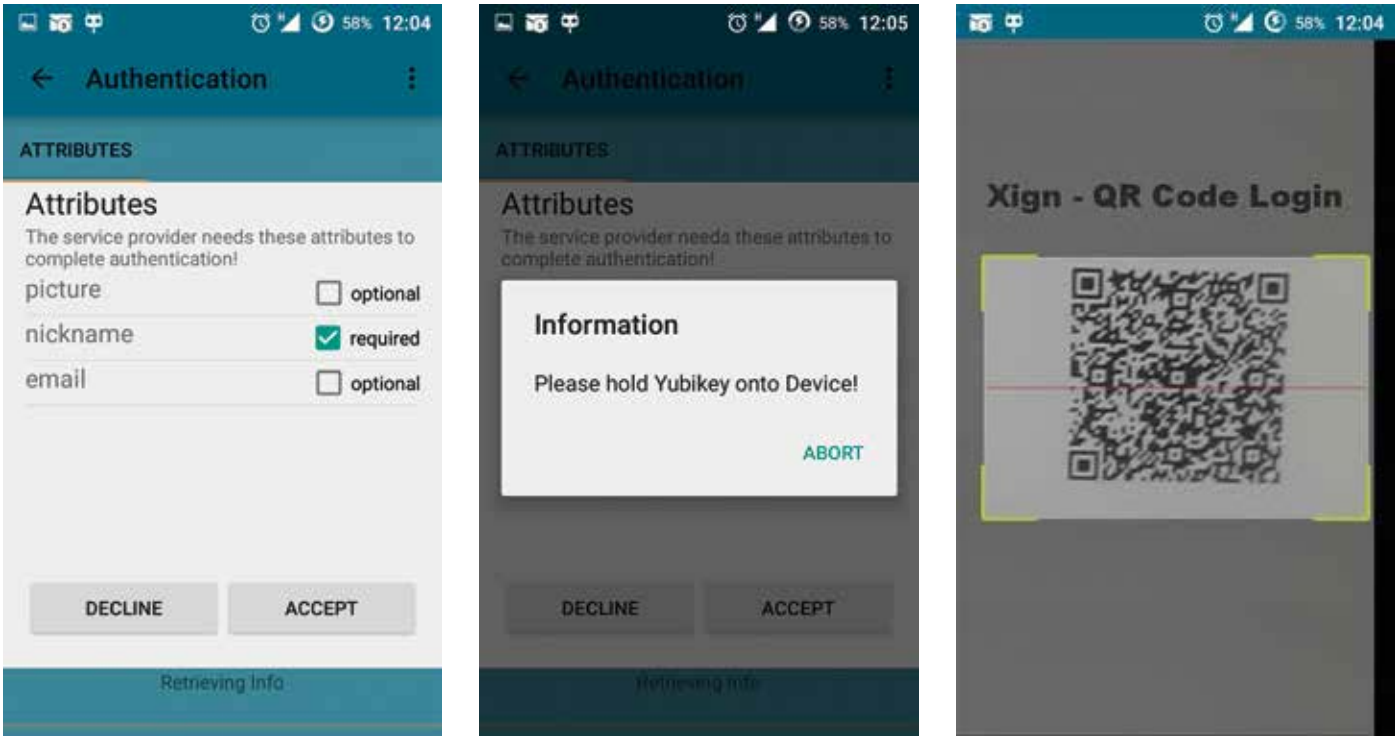
Große Unternehmen verwalten die Nutzer von IT-Systemen typischerweise über LDAP, RADIUS oder ähnliche Protokolle. Auch diese Schnittstellen werden vom Xign-System verwendet, damit vorhandene IT-Infrastrukturen eingebunden werden können.

Service-Protokolle für die Authentifizierung

Die eigentliche Nutzerauthentifizierung wird über ein kryptographisches Challenge-Response-Protokoll durchgeführt. Das Protokoll wird zwischen XignApp/XignToken und dem XignManager umgesetzt. Da keine Passwörter zum Einsatz kommen, ist die Authentifizierung sicher vor Phishing-Angriffen. Die Unterstützung durch die Public-Key-Infrastruktur mit den Verschlüsselungs- und Vertrauensdiensten ermöglicht zusätzlich den Schutz vor Man-in-the-Middle-Angriffen.

XignApp

Die XignApp agiert als vertrauenswürdige Nutzerschnittstelle, QR-Code-Scanner und Token-Lesegerät für den XignToken. Die XignApp ist mit einem Schlüsselpaar und einem dazugehörigen Zertifikat ausgestattet. Durch das Schlüsselpaar und die mögliche Verwendung einer PIN kann das Smartphone als sogenannter Soft-Token (Software-Token) verwendet werden.



Die XignApp agiert als vertrauenswürdige Nutzerschnittstelle, QR-Code-Scanner und Token-Lesegerät für den XignToken. Die XignApp ist mit einem Schlüsselpaar und einem dazugehörigen Zertifikat ausgestattet.

Während der Authentifizierung stellt das Smartphone Kontextinformationen wie zum Beispiel den Standort bereit, die zusätzlich für die Authentifizierung ausgewertet werden. Über Kontextinformationen können Plausibilitätstests durch den XignManager vorgenommen werden.

Security-Token

Das Xign-System unterstützt Hardware-Token sowie Software-Token. Diese Token lassen sich in die Kategorie der sogenannten X.509 Token einordnen. Jeder Token enthält im Fall von Xign ein dediziertes Schlüsselpaar für jeden einzelnen Nutzer.

Um den Token verwenden zu können, muss dieser zunächst personalisiert werden. Während Hardware-Token von autorisiertem Personal über die Registration Authority personalisiert werden können, müssen Software-Token mit Hilfe des Smartphones personalisiert werden, da die verwendeten Schlüssel auf dem Smartphone gespeichert werden.

Darüber hinaus können Hardware-Token kryptographisch an das Smartphone gebunden werden, um die Sicherheit noch weiter zu erhöhen. Durch die kryptographische Verbindung stellt das Xign-System sicher, dass nur ein Nutzer, der im Besitz von Smartphone, PIN und Token ist, eine erfolgreiche Authentifizierung durchführen kann.

Die Schlüssel, die auf dem Token gespeichert sind, werden dafür verwendet, die vom Server übermittelte Challenge zu signieren. Die Hardware-Token werden über Near Field Communication (NFC) oder Bluetooth angesprochen.

Dienstanbieter

Ein Dienstanbieter kann Xign auf verschiedene Arten in sein IT-System integrieren. Eine Möglichkeit ist es, Xign direkt, mit Hilfe der Xign-Client-Bibliothek (XignIn), in das IT-System zu integrieren. Die Bibliothek stellt eine Reihe von Funktionen und Objekten bereit, die die Kommunikation mit dem XignManager realisieren.

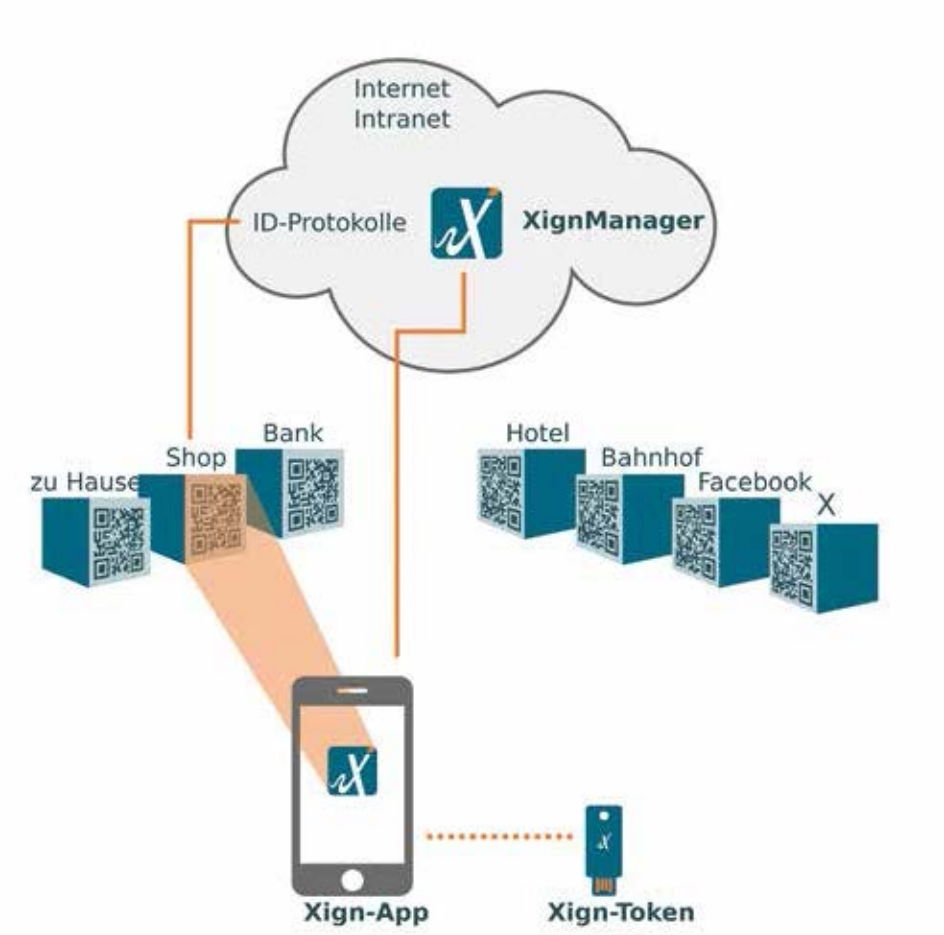
Um die Integration in verschiedenen Szenarios und in bestehende IT-Systeme zu vereinfachen, werden durch den XignManager zusätzliche Protokolle bereitgestellt. Bei diesen Protokollen handelt es sich (siehe Abschnitt zuvor) um beispielsweise OpenID Connect, SAML, FIDO UAF, RADIUS .... Wenn ein Service Provider bereits eine dieser Technologien verwendet, kann die Integration durch die Umleitung der Authentifizierungsanfragen an den XignManager durchgeführt werden.

Ist eine Schnittstelle bisher nicht vorhanden oder ein Dienstanbieter entscheidet sich zur Nutzung des XignPublicService, wird der Xign-Client (XignIn) verwendet. Dazu registriert der Dienstanbieter seinen Dienst bei der Registration Authority (RA) und erhält daraufhin den Client XignIn, das kryptographische Schlüsselmaterial und das passende digitale Zertifikat. Mit der Einbindung der erhaltenen Komponenten in seine Webseite oder in seine Anwendung ist Xign direkt nutzbar.

Wichtige Features

Multirealm

Das Xign-System baut unter anderem auf QR-Codes als Auslöser für den Authentifizierungsvorgang auf. Dieser Ansatz ermöglicht es, eine Authentifizierung durchzuführen, ohne dabei von Peripheriegeräten wie zum Beispiel Anzeige- oder Eingabegeräte abhängig zu sein. Aus diesem Umstand ergeben sich auch weitere neue Anwendungsfälle, da ein QR-Code dem Nutzer auf verschiedenste Weise dargestellt werden kann.



Das Xign-System baut unter anderem auf QR-Codes als Auslöser für den Authentifizierungsvorgang auf. Ein QR-Code kann überall angezeigt werden, sei es durch einen Aufkleber, einen Monitor oder sogar ein Blatt Papier.

Ein QR-Code kann überall angezeigt werden, sei es durch einen Aufkleber, einen Monitor oder sogar ein Blatt Papier.

In diesem Zusammenhang sind Anwendungsfälle im Bereich von physischem Zugriff bis hin zu Check-in-Systemen für Hotels, aber auch die Wahrnehmung von Reservierungen in Restaurants oder Ticket-Systemen denkbar.

Organisationsübergreifende Authentifizierung

Die Tatsache, dass das Xign-System durch eine PKI gestützt wird, liefert sowohl aus Sicht des Nutzers als auch aus Sicht des Unternehmens mehrere Vorteile. Eine PKI bietet neben effizientem Risikomanagement auch die Möglichkeit, einen Nutzer über mehrere Organisationen hinweg zu authentifizieren. Mit Hilfe von sogenannten Bridge-CAs können auf der Basis von gemeinsamen Policies Föderationskonzepte einfach umgesetzt werden, die eine Authentifikation mit der XignApp und den entsprechenden Token organisationsübergreifend ermöglichen.

Der Ablauf

Registrierung

Während der einmaligen Registrierung werden die benötigten Nutzerdaten mit der Registration Authority (RA) erfasst und in die XignID für den Nutzer überführt. Im Unternehmensumfeld wird dazu auf die bestehenden Nutzerdaten zurückgegriffen. Im öffentlichen Umfeld, bei der Nutzung des XignPublicService, bietet die RA dem Nutzer die Möglichkeit, sich mit dem neuen Personalausweis (nPA) zu registrieren. Damit ist durchgängig ein sehr hohes Sicherheitsniveau eingehalten.

Im Anschluss personalisiert der Nutzer seine(n) XignApp/XignToken mit dem erstellten Profil. Hierzu scannt er den von der RA bereitgestellten QR-Code und legt die PIN für die XignApp fest. Während dieser Prozedur wird das kryptographische Schlüsselmaterial berechnet, ebenso das dazugehörige digitale Zertifikat von der Certification Authority (CA) ausgestellt und zusammen sicher gespeichert.

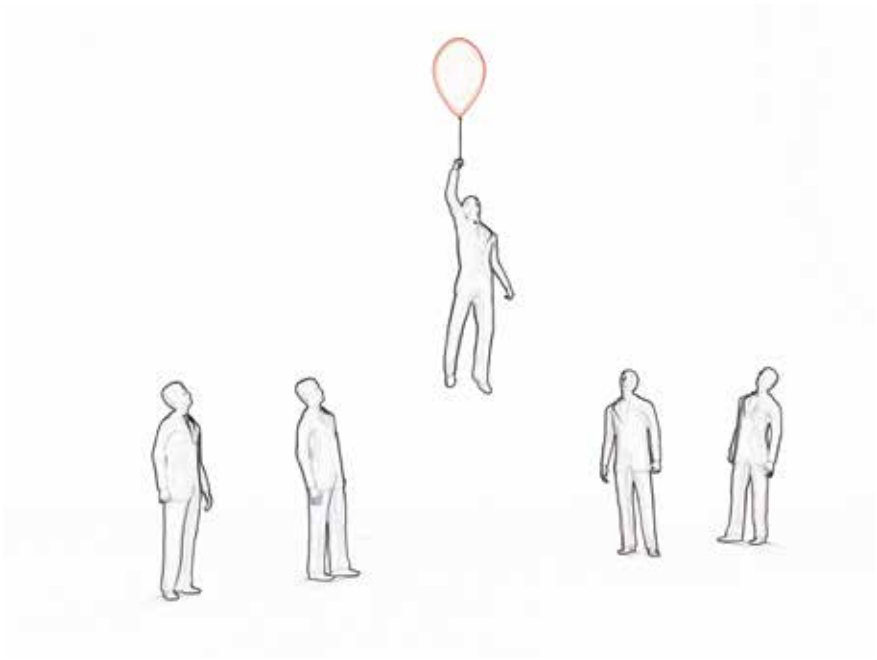
Das Bedrohungspotenzial

Das Xign-System ist im Vergleich zu den herkömmlichen Authentifizierungsverfahren wie zum Beispiel Passwort- und TAN-basierte Verfahren gegen eine Vielzahl von Bedrohungen und Angriffen resistent. Der Hauptgrund für die Robustheit ist neben der PKI-gestützten Kommunikation die einfache Nutzung einer 2-Faktor-Authentifizierung, ohne die Notwendigkeit der Eingabe von sensiblen Nutzerdaten.

Auf Grund von kontextbasierten Informationen, beispielsweise über den Standort eines Nutzers, werden auch gestohlene QR-Codes und nicht sinnhafte Authentifizierungsvorgänge erkannt. Auch der direkte Angriff auf die Nutzerdaten, die bei der Kommunikation zwischen Dienstanbieter und XignManager übertragen werden, ist nicht möglich, weil sie zum einen auf die nötigste Anzahl zur Erfüllung des Dienstes reduziert und zum anderen Ende-zu-Ende verschlüsselt sind. Die Verschlüsselung erfolgt neben der Transportabsicherung durch TLS zusätzlich durch einen ausgehandelten Sitzungsschlüssel.

Ausblick

Neben dem QR-Code als Auslöser für den Authentifizierungsvorgang ist es auch denkbar, weitere Auslöser zu verwenden, um Endgeräte, die nicht im Besitz einer Kamera sind, in das Xign-System zu integrieren. Die Bandbreite der Auslöser beginnt bei Near-Field-Communication (NFC)-Tags und reicht bis hin zu GPS-, Bluetooth- und WLAN-Daten.



Neben dem Einbinden anderer Auslöser und Endgeräte kann das Xign-System auch in neuen Szenarien, die starke und sichere Authentifizierung benötigen, eingesetzt werden. Als klassische Anwendungsbeispiele sind hier der physische Gebäudezugang und das Automotivumfeld zu nennen. Im Zusammenspiel mit Wearables adressiert das Xign-System Problemstellungen im Bereich von Industrie-4.0-Anlagen.

Neben der signaturbasierten Authentifizierung können auch reine Signaturdienste (Vertrauensdienste) abgedeckt werden. Die Signaturdienste können im Finanzwesen, unter anderem bei Online-Banking und Bezahldiensten, Transaktionen vereinfachen und beschleunigen, bei gleichzeitiger Kostenreduktion und Erhöhung der Sicherheit. Auch im Businessumfeld, gerade unter der Berücksichtigung der Europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS), ermöglicht das Xign-System die Verlagerung der papiergestützten Prozesse hin zu digitalen und unterstützt den rechtsgültigen internationalen Austausch von digitalen Dokumenten.

Fazit

Um Nutzern die Authentifizierung mit ihrem eigenen mobilen Endgerät zu ermöglichen, müssen neben den üblichen und strikten Policies für „Bring Your Own Device" (BYOD), spezielle Anforderungen an das Authentifizierungssystem gestellt werden.

Das Authentifizierungssystem muss flexibel, einfach zu bedienen und zu managen sowie sicher und vertrauenswürdig sein. Die Flexibilität ist aufgrund der heterogenen Endgeräte und Authentifizierungspunkte zur einfachen Integration unabdingbar. Gerade im Unternehmensumfeld muss das Authentifizierungssystem nahtlos in die bestehende IT-Infrastruktur integriert werden können. Der Faktor Sicherheit bedeutet zum einen, dass das Authentifizierungssystem die bestehende IT-Infrastruktur nicht gefährdet, zum anderen aber auch die Pflicht zur Einhaltung von Verbindlichkeit und der Zusicherung der Integrität der verwendeten Daten.

Ein modernes Authentifizierungssystem muss möglichst vielen Angriffsvektoren entgegenwirken. Auf die Verwendung von Nutzername und Passwort sollte es gänzlich verzichten und stattdessen auf PKI-gestützter Multifaktor-Authentifizierung beruhen. Das Xign-System wurde unter genau diesen Prämissen entwickelt. Das Institut für Internet-Sicherheit bietet Interessenten die Möglichkeit, Xign für einen vorgegebenen Zeitrahmen kostenfrei zu testen. ■

Norbert Pohlmann,
Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Außerdem ist er Studienbeauftragter für den Master Internet-Sicherheit.

Markus Hertlein,
Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen

Pascal Manaras,
Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen

Quellen:
SAML: https://www.oasis-open.org/committees/security/
OpenID Connect: http://openid.net/connect/
FIDO UAF: https://fidoalliance.org/specifications/overview/