Pascal Manaras, Markus Hertlein, Norbert Pohlmann

Die Zeit nach dem Passwort

Handhabbare Multifaktor-Authentifizierung für ein gesundes Eco-System

In unserer heutigen vernetzten Welt sind persönliche Informationen das höchste Gut eines Nutzers. Jedoch werden diese immer noch mit der schwachen Authentifizierung, mittels Benutzername und Passwort, geschützt. Dies führt zu Problemen beim Nutzer und Unternehmen. XignQR wirkt mit starker und handhabbarer Multifaktor-Authentifizierung für alle Lebenslagen entgegen.

1 Einleitung

Noch vor 20 Jahren wäre niemand auf die Idee gekommen, dass das Internet einen derart großen Einfluss auf die heutige Lebensweise der Menschen haben wird. So hätte damals niemand gedacht, dass eines Tages Dienste angeboten werden, die es ermöglichen Überweisungen oder Einkäufe auf eine derart selbstverständliche Weise über das Internet abzuwickeln.

Insgesamt erlangen die digitalen Dienste immer größer werdende Sensibilität in Bezug auf die Daten ihrer Nutzer, sodass die sichere und datenschutzkonforme Aufbewahrung und die benutzerfreundliche Verwendung dieser Identitäten immer mehr an Bedeutung gewinnt. Jeder Nutzer besitzt mehrere digitalen Identitäten mit breitgefächerten Inhalten, beginnend beim Pseudonym bis hin zu umfangreichen persönlichen Daten. Geschützt wird der Zugriff auf die Identitäten durch diverse Verfahren, die in der Regel nicht interoperabel agieren. Diese Insellösungen werden den Anforderungen des heutigen komplexen IT-Eco-System nicht mehr gerecht und noch weniger den Herausforderungen, die mit dem fortschreitenden Wandel der personenorientierten vernetzten Welt hin zu einer geräteorientierten im „Internet of Things“ (IOT) auftreten.

Um den genannten Umständen Rechnung zu tragen, wurde XignQR geschaffen, eine interoperable Plattform für starke und benutzerfreundliche Authentifikation und Identifikation. Dabei reichen die Anwendungsfälle vom Ausführen von Bezahltransaktionen über das Leisten digitaler Unterschriften bis hin zur Verifikation digitaler Identitäten.

1.2 Die heutige Realität

Aktuell hat der jeder Dienstanbieter persönlich dafür Sorge zu tragen, auf welche Weise ein Nutzer identifiziert und authentifiziert wird. In diesem Zusammenhang stehen ihm verschiedene Formen und Mechanismen zur Verfügung, die von der Identifizierung per E-Mail bis hin zur Nutzung von Onlinefunktionalitäten bestimmter Ausweisdokumente, wie zum Beispiel dem neuen deutschen Personalausweis, reichen.

Die Art, auf die ein Nutzer authentifiziert wird, bestimmt zum einen wie hoch der Schutz der Nutzerdaten ist und damit auch über die Vertrauenswürdigkeit der digitalen Identität, zum anderen bestimmt sie aber auch den Grad der Benutzerfreundlichkeit, bei Verwendung des Dienstes (vgl. Abb. 1). Heutzutage ist schwache passwortbasierte 1-Faktor-Authentifizierung (Wissen),

Pascal Manaras

Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule sowie Co-Founder der in der Gründung befindlichen XignSYS

E-Mail: manaras@xignsys.com

Markus Hertlein

Wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule sowie Co-Founder der in der Gründung befindlichen XignSYS

E-Mail: hertlein@xignsys.com

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
E-Mail: pohlmann@internet-sicherheit.de

sowohl im Internet als auch in Unternehmen immer noch die am häufigsten verwendete Methode zur Authentifizierung.

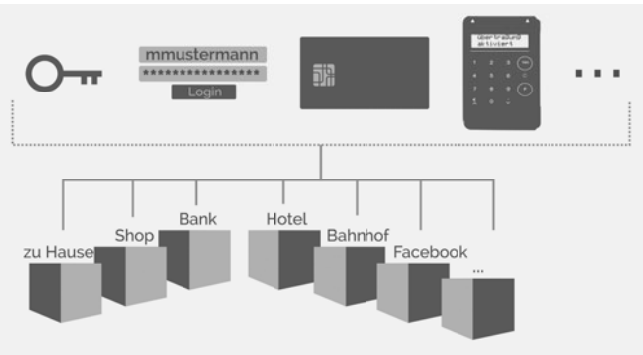
Bei der Verwendung von Passwörtern muss generell ein Spagat zwischen der Merkbarkeit und der Sicherheit des jeweiligen Passworts erfolgen. Ein Passwort, das ein Mindestmaß an Sicherheit gewährleistet, enthält Sonderzeichen, Zahlen und umfasst mindestens 12 Zeichen. Aus diesem Grund wählen Nutzer häufig leichte Passwörter und verwenden diese für mehrere Dienste, z.B. einen bestimmten Begriff, an den sie sich leicht erinnern können, und vergessen dabei aber, dass Angreifer solche Passwörter leicht erraten können (Brute-Force Angriffe).

Ein eindrucksvolles negatives Beispiel im Umgang mit „sicheren" Passwörtern hat der Angriff auf den französischen TV-Sender, TV5 Monde, im April 2015 gezeigt. Die Passwörter waren auf Zetteln notiert und während einer Live-Ausstrahlung für das gesamte Publikum sichtbar.

Aber auch Nutzer, die sichere Passworte verwenden und geheim halten, sehen sich immer perfideren Angriffen, wie zum Beispiel Phishing gegenüber, sodass Passwörter schon längst der Vergangenheit angehören sollten.

Hiermit bilden Identifizierung und Authentifizierung des Nutzers die Grundlage für die Nutzung digitaler Dienste im Internet.

Abb. 1 | Übersicht über die heutige Authentifizierungs- und Identifizierungslandschaft



1.3 Starke Authentifizierung

Aus den genannten Gründen wird in Unternehmen häufig, ergänzend zum Passwort, auf One-Time-Passwörter (OTP), als zweiten Faktor, zurückgegriffen. Bei OTPs wird abhängig von der Zeit, einem geteilten Geheimnis und einem bestimmten Algorithmus ein Passwort mit kurzer Gültigkeitsdauer generiert.

Das OTP wird dazu in einem speziellen Hardware Token generiert, das als Besitzfaktor den zweiten Faktor bei der Authentifizierung bildet. Die Verwaltung kann aber, aufgrund des geteilten Geheimnisses, sehr komplex sein. Zudem bleiben viele Angriffe auf Passwörter bestehen, da dieses Verfahren, trotz der Zeitabhängigkeit, immer noch auf der Übertragung von Geheimnissen beruht.

Für sicherheitskritische Dienste und Zugänge wird daher auf starke protokollbasierte Multifaktor-Authentifizierung (MFA) gesetzt. Dieses Verfahren kommt ohne die Übertragung eines Geheimnisses aus und basiert auf einem Challenge-Response-Protokoll. Im Idealfall wird das Challenge-Response-Protokoll durch die Verwendung einer Public-Key-Infrastruktur (PKI) gestützt, wodurch ein effektives und schnelles Risikomanagement etabliert werden kann. Die PKI ermöglicht zu dem die organisationsübergreifende Verwendung des Authentifizierungsmediums.

Beim beschriebenen Ansatz der MFA besteht die Notwendigkeit einer Zusatzhardware, die in der Lage ist, das Challenge-Response-Protokoll zu sprechen. Dazu werden für gewöhnlich Smartcards verwendet, die den privaten Schlüssel des Nutzers sicher speichern und als Besitzfaktor gelten. Der Zugriff auf den Schlüssel ist durch eine PIN geschützt, die dem Nutzer bekannt sein muss und bei Verwendung eingegeben wird und somit als Wissensfaktor gilt. Problematisch ist die Nutzung in unterschiedlichen Szenarien vor allem aber in mobilen Bereichen, da als Bindeglied zwischen Smartcard und Authentifizierungssystem ein Lesegerät benötigt wird.

1.4 Anforderungen an ein modernes Authentifikationssystem

Zusammenfassend lässt sich festhalten, dass ein modernes Authentifizierungssystem, in dem komplexen Umfeld von IT-Eco-Systemen, flexiblen Schutz der Nutzerdaten und anwendungsspezifische Vertrauensniveaus bei der Authentifizierung des Nutzers bereitstellen muss. Gerade der Einsatz von passwortbasierten Systemen verliert daher immer weiter an Daseinsberechtigung. Aus der aktuellen Situation lassen sich daher folgende Anforderungen ableiten:

- Hohe Sicherheit bei geringer Komplexität
- Adaptive Balance zwischen Sicherheit und Benutzerfreundlichkeit
- Einfache Integration
- Interoperabilität und Flexibilität
- Datenschutz und -sparsamkeit
- Hohe Nutzerakzeptanz durch Verzicht auf Zusatzhardware, Transparenz, Informationelle Selbstbestimmung und einfache Verwaltung und Nutzung

Das XignQR-System adressiert die Herausforderung und macht sich bestehende Technologien und die extrem große Verbreitung von mobilen Endgeräten zu Nutze, indem es durch die Verwendung einer Smartphone App, eines QR Codes und eines optionalen Sicherheitstoken, die Nutzung starker passwortloser Multifaktor-Authentifizierung ermöglicht.

2 XignQR – Die 4. Generation der Datensicherheit

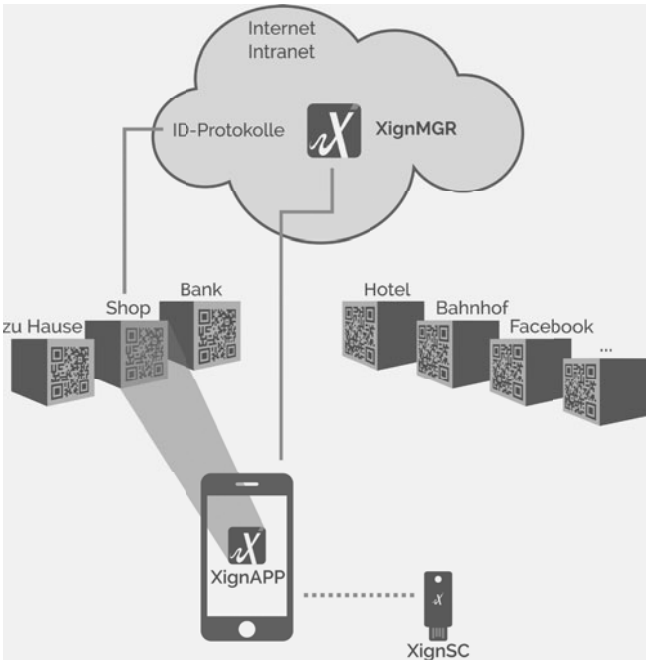
Für den Einsatz des XignQR-System sind grundsätzlich vier Akteure (vgl. Abb. 2) notwendig, die durch eine PKI gestützt werden: Die Smartphone App (XignAPP), optional erweiterbar durch einen Hardware-Security-Token (XignSC), der Authentifizierungsmanager (XignMGR) und die Einbindungskomponente (XignIN) beim Dienstanbieter.

Beim Dienstanbieter handelt es sich um ein IT-System, z. B. eine Webseite, ein ERP-System oder ein lokaler Arbeitsrechner.

Um dem Nutzer den Zugriff auf den Dienst zu ermöglichen, muss er zuvor vom Dienstanbieter authentifiziert werden. Zu diesem Zweck ruft der Dienstanbieter einen QR Code vom XignMGR ab, der dem Nutzer präsentiert wird und vom Nutzer mit Hilfe der XignAPP eingelesen wird, um die Authentifizierung zu starten. Die App (XignAPP) verarbeitet die darin enthaltenen

Informationen und kommuniziert mit dem XignMGR, um den Nutzer schließlich zu authentifizieren.

Abb. 2 | Der Einsatz von XignQR mit den beteiligten Akteuren in unterschiedlichen Szenarien



Das Authentifizierungsergebnis und die angefragten Nutzerdaten werden dann vom XignMGR an den Dienstanbieter übermittelt.

Die Authentifizierung an sich wird über ein PKI-basiertes Challenge-Response-Verfahren unter Verwendung des persönlichen Schlüsselmaterials des Nutzers realisiert.

2.1 XignMGR – Der Vertrauensanker

Als Trusted Third Party bildet der XignMGR die zentrale Komponente im XignQR System und somit den Vertrauensanker. Als Vermittler zwischen dem Nutzer mit der XignAPP und dem Dienstanbieter ist der XignMGR für die Verteilung der notwendigen Informationen und Ergebnisse während des Authentifizierungsprozesses zuständig.

Zum einen liefert er den QR Code an den Dienstanbieter aus, während er dem Nutzer über die XignAPP bescheinigt, um welchen Dienstanbieter es sich handelt und welche Informationen für die Erfüllung des Dienstes an den Dienstanbieter übermittelt werden müssen.

Zum anderen versichert der XignMGR dem Dienstanbieter, dass der Nutzer ordentlich und sicher authentifiziert wird.

Die Nutzerdaten werden bei der einmaligen Nutzerregistrierung erfasst und sicher im XignMGR gespeichert. Der Nutzer kann seine Daten jederzeit über den XignMGR verwalten.

Die Trennung von Authentifizierungsmedium, Smartphone inklusive personalisierter XignAPP und dem Authentifizierungsmanager XignMGR, führt zu einem weiteren Vorteil. Während bei den meisten Authentifizierungssystemen ein großer Eingriff in die bestehende IT-Infrastruktur stattfinden muss, kann XignQR, neben dem Betrieb in der eigenen Infrasturktur, auch komfortabel aus der Cloud genutzt werden. Für die einfache Integration unterstützt der XignMGR folgende Protokolle:

Das proprietäre XignQR-Protokoll, aufbauend auf das Websocket-Protokoll und JSON-Nachrichten, kann von Dienstanbietern dazu verwendet werden, XignQR direkt, mittels der Client-Library XignIN, in das System zu integrieren, auch dann wenn sie bisher keine ID-Protokolle unterstützen. Für öffentliche Systeme im Internet wird OpenIDConnect unterstützt.

Große Unternehmen verwalten die Nutzer von IT-Systemen typischerweise über LDAP, RADIUS oder ähnliche Protokolle. Auch diese Schnittstellen werden für die einfache Integration von XignQR in bestehende IT-Infrastrukturen unterstützt.

2.2 XignAPP – Das Smartphone als MFA fähiges persönliches Authentifizierungsdevice

Die XignAPP agiert als vertrauenswürdige Nutzerschnittstelle, Kontrollkanal, QR Code Scanner und Token-Lesegerät. Die XignAPP ist mit Schlüsselpaaren und den dazugehörigen Zertifikaten ausgestattet. Mit der Absicherung der App und dem Schlüsselmaterial, mit der Möglichkeit zur Verwendung einer PIN und der Fähigkeit das PKI-basierte Challenge-Response-Protokoll zu sprechen, bildet die XignAPP das Softtoken (Software-Token). Hiermit wird das Smartphone zum Personal Authentitication Device (PAD).

In Verbindung mit dem QR Code als Einsprungspunkt für die Authentifizierung kann auf zusätzliche Hardware, wie zum Beispiel Lesegeräte, verzichtet werden. Dadurch ist es möglich sichere benutzerfreundliche und adaptive Multifaktor-Authentifizierung, bestehend aus Besitz (Smartphone) und Wissen (PIN), oder Sein (Biometrie) oder allen Faktoren, optional auch mehrfach, zur Verfügung zu stellen.

So lassen sich unterschiedliche Vertrauens- und Sicherheitsniveaus realisieren und zudem eine ausgewogenen Balance, zwischen Benutzerfreundlichkeit und Sicherheit, erreichen.

Als Gegenstück zum XignMGR dient die Smartphone App zur Anzeige für den Nutzer. Hierüber erhält der Nutzer Transparenz und wird über alle Abläufe und Prozesse informiert. Nach dem Scannen des QR Codes werden die vom XignMGR übertragenen Daten dem Nutzer zur Gegenkontrolle in der XignAPP angezeigt. Der Nutzer hat nun die Möglichkeit, den Vorgang zu bestätigen oder zu beenden und kann dabei optional verlangte Nutzerdaten ablehnen.

2.3 XignSC – Optionale Hardware Sicherheit

XignQR unterstützt als Ergänzung zum Softtoken ein Hardware Security-Token (HW-Token), XignSC genannt. XignSC verhält sich ähnlich wie das Softoken in der XignAPP, dient aber als sicherer Schlüsselspeicher, vergleichbar mit einer EC-Karte oder dem neuen Personalausweis.

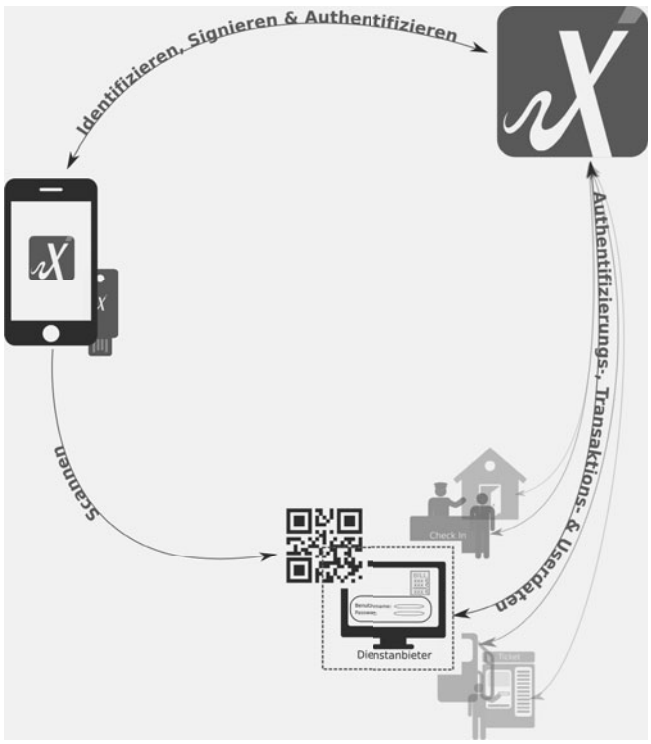
Als besonderes Merkmal lässt sich das XignSC mittels Pairing kryptografisch an die XignAPP binden. Das Pairing stellt sicher, dass der Nutzer im Besitz des Smartphones und des HW-Tokens ist. Damit lassen sich auch benutzerfreundliche Authentifizierungsfälle, die auf doppelten Besitz beruhen, realisieren und so ohne PIN-Eingabe auskommen. Die Kommunikation zwischen Smartphone und dem HW-Token findet gesichert über Near-Field-Communication (NFC) statt.

Vorgesehen ist die Unterstützung weiterer NFC-basierter Security-Token, wie z. B. dem neuen Personalausweis, aber auch der EC-Karte.

2.4 XignIN – Integration ohne Aufwand

Die Client-Library XignIN dient zur komfortablen Integration auf der Dienstanbieterseite und unterstützt den Anbieter bei nicht standardisierten Abläufen, wie z. B. dem Abrufen und Einbinden des QR Codes, und bei der Kryptografie. XignIN kann auch von Anbietern genutzt werden, die kein etabliertes ID-Protokoll, wie z. B. OpenIDConnect o. ä., unterstützten, um XignQR zu nutzen.

Abb. 3 | Die XignQR Architektur und das Zusammenspiel der Komponenten



3 Identifizierung, Registrierung, Personalisierung – Basis für vertrauenswürdigen Identitäten

In heutigen IT-Eco-Systemen ist die Vertrauenswürdigkeit einer digitalen Identität für die Nutzung eines Dienstes, besonders für sicherheitskritische und personenbezogene Dienste, entscheidend und muss neben starker Authentifizierung auch eine zuverlässige Identifizierung bei der Nutzerregistrierung aufweisen.

Dazu unterstützt XignQR vier grundsätzliche Vertrauensniveaus. Unterschieden werden dabei die aufgenommen persönlichen Daten des Nutzers und die Art der Verifizierung dieser Daten.

- **Vertrauensniveau 1: Nicht verifizierte Registrierung**

Der Nutzer gibt seine Daten persönlich ein. Die Daten werden nicht weiter mit einem Vertrauensanker verifiziert.

Aufgrund des einfachen Vertrauensniveaus werden hier nur wenige Nutzerdaten erfasst, im einfachsten Falle handelt es sich um den Benutzernamen oder ein generiertes Pseudonym.

- **Vertrauensniveau 2: E-Mail verifizierte Registrierung**

Der Nutzer beweist seine Identität, indem er zeigt im Besitz der angegebenen E-Mail Adresse zu sein. Damit wird nur die E-Mail Adresse verifiziert, was allerdings für viele Dienste, wie zum Beispiel soziale Netzwerke oder Blogs, ausreichend ist.

- **Vertrauensniveau 3: Registrierung per Videochat**

Der Nutzer beweist seine Identität mit dem, durch das Bundesfinanzministerium (BMF) beschriebene Verfahren, der Identitätsfeststellung per Videochat. Der Grund für diese Form der Registrierung ist die geringe Akzeptanz der Online-Funktion des neuen Personalausweises durch die Bürger, denn in 2015 haben insgesamt lediglich 400.000 Bürger diese Funktion aktiviert. Weiter bietet dieses Verfahren die Möglichkeit, jederzeit, ohne Zusatzhardware, eine starke Identifizierung durchzuführen.

Die Registrierung per Videochat ergibt eine Identität des Vertrauensniveaus 3, da die Erfassung auf zwischenmenschliche Kommunikation aufbaut, wodurch eine gewisse Fehlerquote entsteht.

- **Vertrauensniveau 4: Registrierung mit dem neuen Personalausweis (nPA) per eID**

Der Nutzer registriert sich mit Hilfe der Online-Funktion (eID Schnittstelle) des neuen Personalausweises oder einer elektronischen Schnittstelle eines anderen hoheitlichen Dokuments. Die Registrierung per eID resultiert im höchsten Sicherheitslevel das von XignQR unterstützt wird. Diese Form des Identitätsnachweises ist besonders sicher, da es sich hier um einen rein elektronischen Nachweis mit einem sehr starken Vertrauensanker handelt.

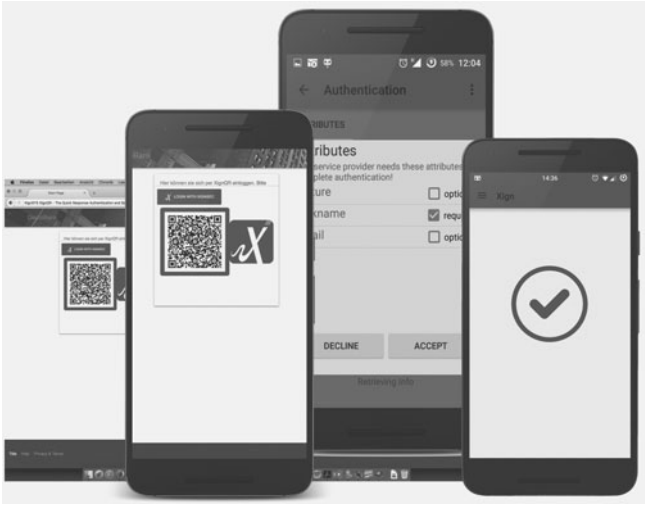
Der Nutzer benötigt für die Verwendung des nPA ein Lesegerät mit zusätzlich aktivierter Online-Funktion des Ausweises – ein Umstand, der nur bei den wenigsten Bürgern zutrifft – und eine spezielle Software auf seinem Computer, den sogenannten eID-Client (AusweisApp2 oder OpenECardApp).

Aus den erfassten Daten wird eine Kennung erzeugt, die zur Personalisierung der XignAPP (und XignSC) verwendet wird. Dazu wird dem Nutzer ein sehr kurzlebiger QR Code angezeigt. Nach dem Scannen des QR Codes mit der XignAPP, erhält der Nutzer über einen zweiten Kanal, in Abhängigkeit des Vertrauensniveaus, einen Verifizierungscode, der durch die XignAPP verarbeitet wird. Stimmen die Informationen aus dem QR Code mit den Informationen aus dem zweiten Kanal überein, wird die Registrierung mit dem Generieren der Schlüsselpaare, dem Erstellen und sicheren Speichern der Zertifikate und dem Festlegen der PIN abgeschlossen.

4 Adaptive Multifaktor-Authentifizierung – Starke benutzerfreundliche MFA für den Alltag

Die Authentifizierung ist ein Zusammenspiel aller Komponenten eines modernen Authentifizierungssystems. XignQR bietet auf diese Weise handhabbare starke Multifaktor-Authentifizierung, mit besonderen Features, wie z. B. der Nutzer-Anbieter-spezifischen Pseudonymfunktion, die das „Tracken“ eines Nutzers über mehrere Dienste verhindert. Den Ablauf aus Nutzersicht zeigt Abbildung 4.

Abb. 4 | Darstellung des Ablaufs zur Authentifizierung aus Nutzersicht



4.1 Neue Faktoren zur Multifaktor-Authentifizierung

Neben den klassischen Kombinationen der Faktoren Besitz, Wissen und Sein lassen sich auch andere Kombinationen im XignQR-System realisieren. Beispielsweise kann mit dem kryptografisch verbundenen HW-Token, XignSC, eine benutzerfreundliche Kombination aus doppelten Besitz, ohne die Notwendigkeit zur PIN-Eingabe, realisiert werden. Für kritische Zugänge, kann beispielsweise die Authentifizierung per PIN und Videochat gefordert werden. Dabei muss der Nutzer ein weiteres Mal seinen Ausweis per Smartphone Kamera vorzeigen.

4.2 Sicherheit im Zwiebelmodell

Das Smartphone bietet unzählige Sensoren die Informationen liefern, die in den Prozess der Authentifizierung einbezogen werden können. Im Allgemeinen bezeichnet man diese Informationen als kontextbasierte Informationen.

Kontextinformationen sind zum Beispiel der Standort oder das Netzwerk in dem sich das Smartphone befindet, aber auch die Informationen, die durch die Lagesensoren mitgeteilt werden. Über Kontextinformationen können nutzerspezifische Gebrauchsmuster analysiert werden und Prüfungen der Plausibilität vorgenommen werden.

4.3 Adaptive Wahl der Faktoren zur Authentifizierung

Der Nutzer kann in seiner XignAPP ein Mindestmaß an Faktoren festlegen, die zur Nutzung der XignAPP nötig sind. Für schnelle und nicht kritische Dienste kann der Nutzer auf eine PIN verzichten, sodass er die App ohne weitere Interaktion nutzen kann.

Jedoch ist die Wahl der Faktoren immer von den beiden Parteien Dienstanbieter und Nutzer abhängig.

Ist die Sicherheitseinstellung des Nutzers zu niedrig, für die des Dienstanbieters, kann der Dienstanbieter die Verwendung weiterer Faktoren erzwingen.

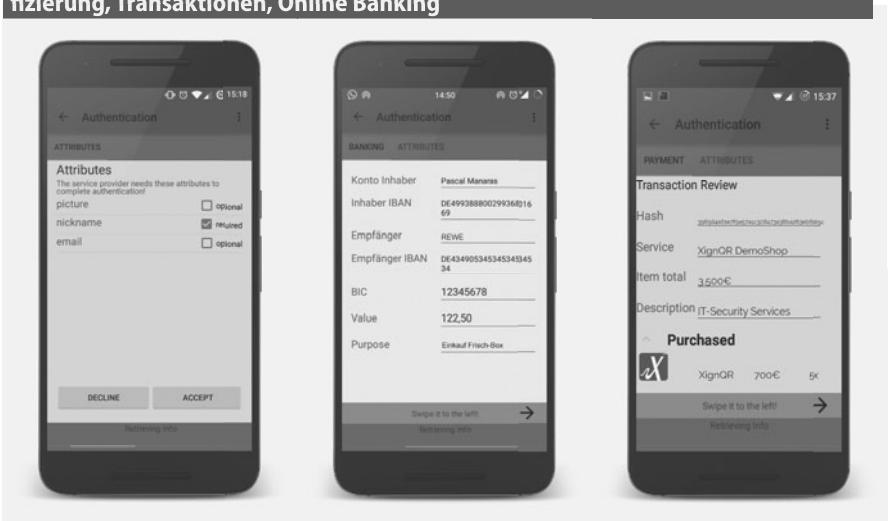
Durch die kontextbasierten Informationen kann auch das XignQR-System weitere Faktoren fordern. Dies kann der Fall sein, wenn die Plausibilitätsprüfung eine Warnung oder Alarm ausgibt. Als Resultat kann dann z. B. die Nutzung des HW-Tokens, wenn registriert, oder die nochmalige Identifizierung per Videochat eingeleitet werden.

4.4 Das Smartphone als Kontrollkanal

Während der Nutzer sich bei den übrigen Authentifizierungsmethoden, z. B. Passwort oder OTP, auf die Korrektheit der Anzeige verlassen muss, hat er mit der Authentifizierung mittels XignQR über die XignAPP einen weiteren Kanal zur Kontrolle. Nicht nur, dass der Nutzer selbst über seine übermittelten Daten zum Dienstanbieter bestimmt, er sieht in der XignAPP auch Informationen über den Dienstanbieter selbst.

Sind an die Authentifizierung weitere Daten geknüpft, die beispielsweise im Zuge einer Transaktion vorher in den Browser eingegeben wurden, werden diese dem Nutzer ebenfalls angezeigt. Ein Angreifer muss daher sowohl den Browser als auch das Smartphone unter seine Kontrolle bringen.

Abb. 5-7 | Anzeige der Kontrolldaten und benötigten Nutzerdaten bei Authentifizierung, Transaktionen, Online Banking



4.5 Remote Logout

Neben den zweiten Kanal zur Kontrolle der Daten bietet die Verwendung des Smartphones auch die Möglichkeit ausgeführte Prozesse wieder zu beenden. Bei einer sitzungsbezogenen Authentifizierung, z. B. auf Webseiten, lässt sich die Sitzung wieder beenden. Der Nutzer kann sich somit per XignAPP wieder abmelden.

5 Sicherheit und Vertrauenswürdigkeit

Da XignQR komplett auf das Übertragen von sicherheitskritischen Informationen verzichtet, ist XignQR nicht anfällig für Phishing- und Bruteforce-Angriffe.

Auch das Entwenden eines QR Codes ist nur kurzzeitig möglich, da der QR Code eine begrenzte Gültigkeitsdauer hat. Sollte dies doch der Fall sein, helfen kontextbasierte Informationen dabei, den Betrugsversuch zu erkennen. Zusätzlich sieht der Nutzer in der App, gegen welchen Dienstanbieter er sich Authentifizieren möchte und kann den Prozess stoppen oder Rückgängig machen (Remote Logout).

Ein Abgreifen der Daten oder ein Man-In-The-Middle-Angriff wird durch die Verwendung der Zertifikate verhindert. Jegliche Kommunikation zwischen den beteiligten Parteien ist über TLS hinaus verschlüsselt und signiert. Somit ist Integrität, Authentizität und Vertraulichkeit der Daten zu jedem Zeitpunkt gewährleistet.

Bei Verlust oder Missbrauch des Smartphones, lassen sich die Zertifikate mittels der eingesetzten PKI mit „einem Klick" ungültig machen. Dies kann durch den Nutzer selbst geschehen, z. B. per Videochat oder mit dem nPA am XignMGR.

6 Ausblick und Fazit

Wie zu Beginn erwähnt sind die Anforderungen an ein modernes Authentifizierungssystem im Umfeld komplexer IT-Eco-System hoch. Neben der Sicherheit steht auch die Flexibilität, einfache Integration, Zusammenspiel mit anderen Applikationen und nicht zuletzt die Anwenderfreundlichkeit, mit allen Aspekten des Datenschutzes und der informationellen Selbstbestimmung im Fokus.

XignQR bietet mit der adaptiven und passwortlosen Multifaktor-Authentifizierung per Smartphone eine benutzerfreundliche und sichere Lösung, um Multifaktor-Authentifizierung, nicht nur in Unternehmen, sondern auch in einer Vielzahl von alltäglichen Szenarien, zu nutzen.

Aufgrund des modularen Aufbaus lässt sich XignQR auch für zukünftige Anforderungen nutzen. Die Anwendungen beginnen dabei mit der starken Authentifizierung über Wearables, bei der das Smartphone ersetzt wird. Auch die Wahl der Auslöser ist flexibel. Es kann z. B. der QR Code durch einen NFC Auslöser ersetzt werden, wodurch XignQR für den Einsatz innerhalb des Automotivumfelds geeignet ist. Maschinen-zu-Maschinen (M2M) Kommunikation kann mit der signaturbasierten Infrastruktur ebenfalls realisiert werden.

Der vorausschauende Einsatz von Signaturen bei der gesamten Kommunikation und der Trennung des Authentifizierungsdevice und PKI-gestützten Nutzerdatenverwaltung ermöglicht neben der Realisierung von Authentifizierungsdiensten auch weitere Vertrauensdienste, wie Signaturdienste. Signaturdienste können unter anderem beim Online-Banking und bei Bezahldiensten Transaktionen vereinfachen und beschleunigen und dabei gleichzeitig Kosten reduzieren und die Sicherheit erhöhen.

Auch im Businessumfeld, gerade unter der Berücksichtigung der europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS), ermöglicht XignQR die Verlagerung der papiergestützten Prozesse hin zu digitalen und unterstützt den rechtsgültigen internationalen Austausch von digitalen Dokumenten.

Literatur

[1] Hertlein, Markus / Manaras, Pascal / Pohlmann, Norbert: "Bring Your Own Device For Authentication (BYOD4A) – The Xign–System". In Proceedings of the ISSE 2015 – Securing Electronic Business Processes – Highlights of the Information Security Solutions Europe 2015 Conference

[2] de Borde, Duncan, „Two-factor authentication", http://web.archive.org/web/20120112172841/http://www.insight.co.uk/files/whitepapers/Twofactor%20authentication%20(White%20paper).pdf

[3] Adams, Carlisle & Lloyd, Steve (2003), „Understanding PKI: concepts, standards, and deployment considerations

[4] Vacca, Jhn R. (2004), „Public key infrastructure: building trusted applications and Web services"

[5] Schröder, Martin / Morgner, Martin (2013), „eID mit abgeleitetenIdentitäten", DuD Datenschutz und Datensicherheit 8-2013, https://www.bundesdruckerei.de/sites/default/files/documents/2013/08/fachartikel_dud_abgeleitete_identitaeten.pdf

[6] Okyle, Carly (2015), „Password Statistics: The Bad, the Worse and the Ugly (Infographic)" http://www.entrepreneur.com/article/246902