IT-Sicherheit als Wegbereiter für die Digitalisierung

Smartphone Bürger-ID

Um die Digitalisierung in Deutschland flächendeckend vorantreiben zu können, benötigt es mehr IT-Sicherheit und Vertrauenswürdigkeit in der digitalen Welt. Täglich finden immer mehr und neue Angriffe auf IT-Systeme statt. Eine starke Verbreitung von Ransomware oder der Datenklau von Milliarden von Passwörtern sind nur zwei Beispiele von sehr vielen. Die Studie „Cybersecurity as a Growth Advantage“[1] eines großen IT-Unternehmens findet 400 neue Anwendungsfälle, die nur dank adäquater IT-Sicherheit digitalisiert werden können. Damit zählen IT-Sicherheit und Vertrauenswürdigkeit als primärer Wachstumstreiber für Digitalisierung. Multifaktor-Authentifikation und digitale Signaturen sind hier gefragt, um Projekte, wie eine Art Bürger-Ausweis, auf Basis eines Smartphones realisieren zu können.

Digitalisierung bringt erstaunliche und großartige Szenarien. So hat Tesla zum Beispiel durch vernetzte smarte Autos die Möglichkeit eröffnet, binnen weniger Stunden Systemupdates auf die komplette Fahrzeugflotte auszurollen. Ohne entsprechende IT-Sicherheit wäre so etwas ein einfaches Einfallstor für Angreifer. Auch Cloud-Lösungen sind erst durch schützende IT-Sicherheit in der Masse möglich geworden. Heutzutage ist es fast undenkbar, Informationen nur auf einem Endgerät mitzuführen. Fotos, Dokumente und Notizen sind auf vielen unterschiedlichen IT-Systemen immer synchronisiert und können mit anderen schnell und sicher ausgetauscht werden.

Neue Ideen und Möglichkeiten durch Digitalisierung, etwa im Verwaltungsverwesen und in Smart-City-Anwendungen, bringen viele Vorteile für die Kommunen, Länder und Bürger. Mitarbeiter im Bürgercenter werden entlastet, und die Bürger genießen die vielen Vorteile, welche die Digitalisierung mit sich bringt.

Passwörter sind nicht die Zukunft, und das ist auch gut so!

Viele digitalisierte Prozesse stoßen früher oder später auf eine Herausforderung: Identifizierung und Authentifizierung von Nutzern. Die Kombination aus Nutzernamen und Passwort bietet zwar den Vorteil, dass jeder weiß wie es funktioniert, ist aber sehr unsicher! Einfach schnell den üblichen Nutzernamen verwendet und genauso einfach wieder das eine Passwort, das so gut im Kopf bleibt.

Doch dies birgt ein fatales Risiko: Gestohlene Passwörter gehören heutzutage zum Tagesgeschäft. Gerade das Passwort-Verfahren birgt neben dem hohen Sicherheitsrisiko zusätzlich noch ein hohes Kostenproblem. Die Verwaltungskosten für ein Passwort-Verfahren explodieren förmlich und summieren sich jährlich zu einem sehr relevanten Posten. Komplizierte Passwortregeln führen dazu, dass sich Nutzer aus Versehen aus dem IT-System aussperren, System-Admins verbringen viele Stunden pro Woche mit dem Zurücksetzen von Accounts. Identitätsdiebstahl durch schwache Passwörter, etwa für E-Mail-Konten, verursacht innerhalb von Unternehmen sehr

hohe Schäden. Sehr häufig werden so wichtige Dinge, wie Firmeninterna, Kundendaten, Protokolle und Betriebsgeheimnisse, auf einfache Weise gestohlen. Identitätsdiebstahl ist auch für Phishing-Angriffe, Malware, wie Keylogger (Ausspähen aller Eingaben über die Tastatur) und Social Engineering ein sehr beliebtes Einfallstor. Passwörter als Sicherheitsfaktor bieten hier inzwischen völlig unzureichenden Schutz.

Alternativen, wie Chipkarten oder Secure-Tokens zur Generierung von „time based onetime passwords", sind immer an zusätzliche Hardware und Mehrkosten gebunden. Entsprechende Systeme sind zudem nur selten interoperabel.

Passwörter werden bald keinen Platz mehr in der Industrie 4.0 finden. Smart-City-Anwendungsfälle, das „Internet of Things" und neue Mobilitätslösungen benötigen eine schnelle, einfache und sichere Authentifizierung, zum Beispiel mithilfe von Multifaktor-Authentifikationsverfahren. Eine Multifaktor-Authentifizierung dient der Verifizierung der Identität eines Nutzers mittels der Kombination verschiedener und insbesondere unabhängiger Klassen von Authentifizierungsverfahren. Eine häufige Variante ist die Zwei-Faktor-Authentifizierung (2FA) mit Besitz und Wissen, zum Beispiel Hardware-Sicherheitsmodul (Smartcard, USB-Token …) plus PIN zur Aktivierung des Hardware-Sicherheitsmoduls. Bei der Multifaktor-Authentifizierung (MFA) kommt mindestens noch ein weiterer Identitätsbeweis dazu, meist ein unverwechselbares körperliches Merkmal.

Die Klassen der Multifaktor-Authentifizierung sind also:

- etwas, das der Nutzer besitzt, wie zum Beispiel ein Hardware-Sicherheitsmodul;
- etwas, das der Nutzer weiß, wie zum Beispiel ein Passwort oder PIN;
- etwas, das als körperliches Charakteristikum untrennbar zum Nutzer gehört (das Sein), wie zum Beispiel ein Fingerabdruck, das Gesicht oder die Stimme.

Ein typisches Beispiel für eine MFA ist ein Hardware-Sicherheitsmodul, das mit einem Passwort oder einer PIN aktiviert werden muss. Um den Nutzerbezug zu verstärken, muss der Nutzer noch mithilfe eines Fingerabdrucks oder der Gesichtserkennung seine Identität zusätzlich verifizieren lassen.

Risikobasierte und adaptive Authentifizierung

Eine adaptive Authentifizierung entscheidet auf der Basis der Vertrauenswürdigkeit des zugreifenden Nutzers, der Kritikalität der konkreten Anwendung/Aktion und den Rahmenbedingungen des aktuellen Zugriffes darüber, welche Authentifikationsverfahren zum Einsatz kommen sollen. Dieser risikoorientierte Ansatz erhöht das allgemeine Sicherheitsniveau und vermindert die Anzahl nicht notwendiger starker Authentifizierungen. Es wird das Optimum zwischen Sicherheit und Komfort angestrebt. Umgesetzt werden Konzepte der adaptiven Authentifizierung mithilfe von MFA-Systemen, die flexibel in Abhängigkeit des gerade notwendigen Sicherheitsniveaus die passenden Authentifikationsverfahren auswählen.[2] Ein Beispiel: Überweisungen von bis zu 20 Euro können schnell mit dem Smartphone abgewickelt werden, wohingegen Transaktionen ins Ausland oder unübliche hohe Summen mehrere Faktoren, wie Biometrie und PIN, erfordern.

Smartphone Bürger-ID

Die Smartphone Bürger-ID ist ein Kooperationsprojekt zwischen dem Institut für Internet-Sicherheit der Westfälischen Hochschule, XignSys, der Stadt Gelsenkirchen und der Stadt Aachen. XignSys ist eine Ausgründung des Instituts für Internet-Sicherheit. Gegründet wurde sie 2016 und ist

maßgeblich für die Entwicklung der Technologie XignQR zuständig. XignQR ermöglicht eine sichere Multifaktor-Authentifizierung am Servicekonto. Für die Stadt Aachen ist der IT-Dienstleister „regio iT" Partner, der sowohl das Serviceportal „aachen.de" als auch die Implementierung der Smartphone Bürger-ID in das Portal begleitet. Gefördert wird es mit Mitteln der digitalen Modellregionen des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie des Landes NRW (MWIDE). Die Projektlaufzeit ist von Januar 2019 bis Ende 2021.

Zum aktuellen Zeitpunkt wird die digitale Identifizierung und Authentifizierung zum Beispiel am Servicekonto mit zwei verschiedenen Auswählmöglichkeiten angeboten: dem klassischen Nutzernamen und Passwort und mithilfe des neuen Personalausweises (nPA). Dabei weist nach eIDAS (electronic IDentification, Authentication and trust Services) nur der nPA das Vertrauensniveau „hoch" auf. Die klassische Registrierung per Nutzernamen und Passwort hingegen ist nur „niedrig" und kann damit aus Sicherheitsgründen nicht für die Nutzung kommunaler Dienste empfohlen werden. Es fehlt das nötige Vertrauensniveau, um sicherstellen zu können, dass die registrierte Person sicher identifiziert werden kann.

Der nPA leidet jedoch aufgrund mehrerer Probleme an Akzeptanz: Zusätzliche Hardware, etwa ein Kartenlesegerät, sind Kosten, die ungern in Kauf genommen werden. Zusätzlich ist die Online-Funktion noch nicht in jedem nPA aktiviert und selbst wenn, fehlt den meisten Bürgern die Freischaltung und die PIN, um die Dienste nutzen zu können.

Das Smartphone als Sicherheitsanker für die digitale Bürger-ID

Daher wird es als sehr gute Idee erachtet, wenn das Smartphone für die digitale Bürger-ID genutzt wird. Fast 90 Prozent aller Android Smartphones besitzen mittlerweile einen eingebauten Hardware Keystore[3] und bieten damit besseren Schutz als nur Passwörter. Ähnlich sieht es beim iPhone aus: Über 84 Prozent der Apple Smartphones laufen bereits mit der aktuellen iOS Version.[4] Dazu kommt viel weitere Technik, die das Smartphone anbietet: Biometrische Sensoren, zum Beispiel für Fingerabdrücke, Gesichtserkennung oder Iris-Scanner. Ebenso gehört dazu ein einfacher Multitouch-Bildschirm, mit dem vorher eingegebene Daten vom Server doppelt auf dem Smartphone überprüft werden können.

Mithilfe des Smartphones kann das passende Vertrauensniveau „substanziell" erzielt werden. Bestehende Basistechnologie erlaubt es Kommunen, Ländern und Unternehmen, neue E-Government- und Smart-City Anwendungen für den Bürger einfach und dennoch sicher zugänglich zu machen. Dies ist zwingend notwendig, um alle möglichen Dienste für das Onlinezugangsgesetz umsetzen zu können.[5] Deutschland befindet sich laut einer Studie des Fraunhofer-Instituts in einer schwierigen Situation. Nur neun Prozent aller Kommunen in Deutschland bieten mehr als 20 Online-Verfahren an. Das Fehlen von entsprechenden Angeboten führt dazu, dass diese kaum bekannt sind und selten genutzt werden. Dabei könnte über ein Drittel der Kosten für die Verwaltung in Deutschland eingespart werden. Diese Einsparungen könnten helfen, den Aufbau eines noch größeren Angebots herbeizuführen. Außerdem werden die notwendigen Behördengänge für die Bürger sehr viel einfacher, weil sie von zu Hause aus oder unterwegs einfach umgesetzt werden können.

Modernes Multifaktor-Authentifizierungssystem und Identifikationsverfahren

Ein modernes Multifaktor-Authentifizierungssystem muss das komplexe Umfeld von IT-Ökosystemen, einen flexiblen Schutz von Nutzerdaten und ein anwendungsspezifisches Vertrauensniveau bei der Authentifizierung des Nutzers berücksichtigen.[2] Daraus lassen sich die folgenden Anforderungen ableiten:

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

Im Folgenden wird eine Lösung einer handhabbaren und modernen Multifaktor-Authentifizierung vorgestellt.[6]

Für den Einsatz dieses modernen Multifaktor-Authentifizierungssystems sind grundsätzlich vier Akteure notwendig, die durch eine Public-Key-Infrastruktur (PKI) gestützt werden: die Smartphone App (APP), der Authentifizierungsmanager und die Einbindungskomponente beim Diensteanbieter.

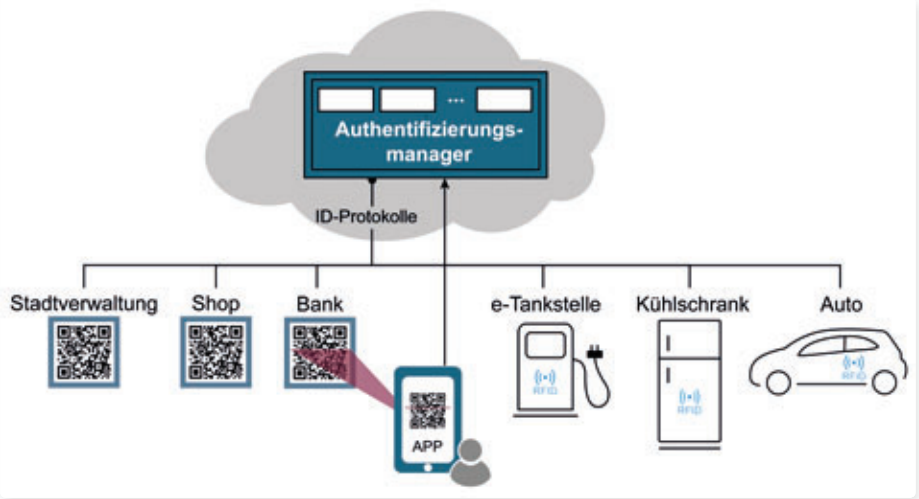

Bild 1: Funktionsweise des MFA-Systems

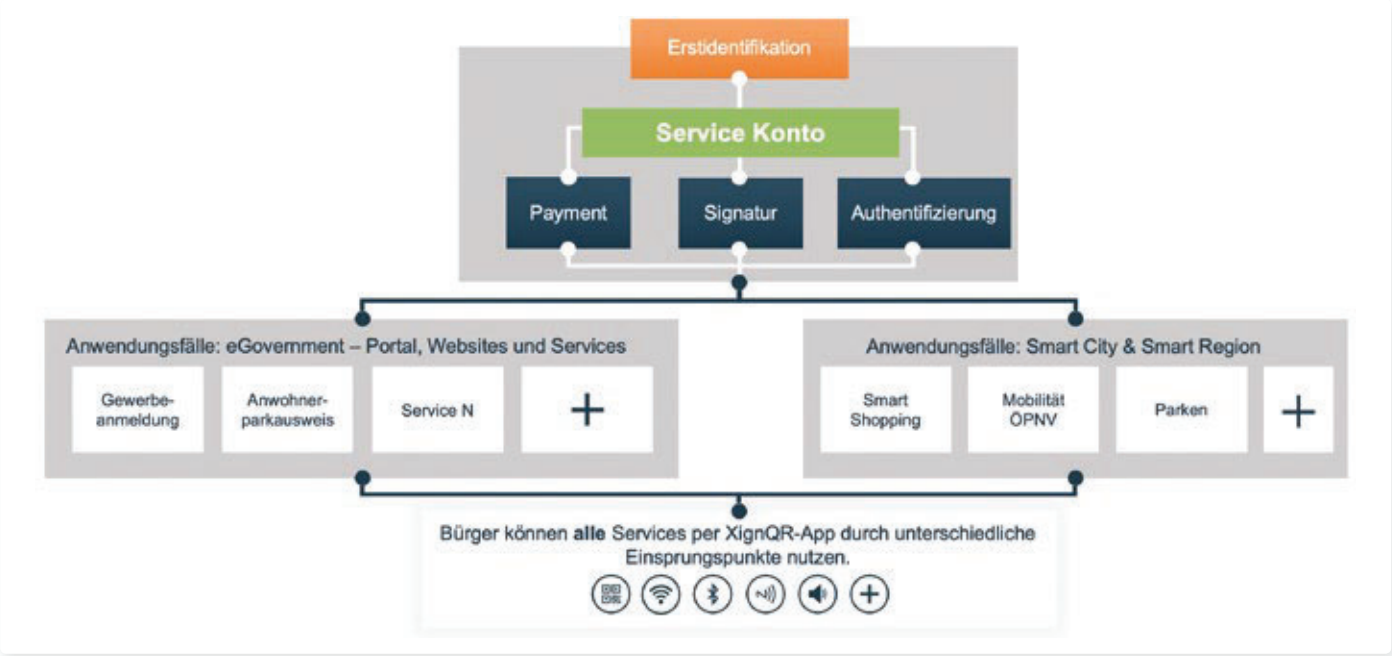

Bild 2: Konzept der Smartphone Bürger-ID App für NRW

Beim Diensteanbieter handelt es sich um ein IT-System, wie eine Webseite (Shop, Behörde, Bank, …), ein ERP-System oder einen lokaler Arbeitsrechner. Um dem Nutzer den Zugriff auf den Dienst zu ermöglichen, muss er zuvor vom Diensteanbieter authentifiziert werden. Zu diesem Zweck ruft der Diensteanbieter einen QR-Code vom Authentifizierungsmanager ab, der dem Nutzer zum Beispiel auf der Webseite präsentiert wird. Der Nutzer kann dann mithilfe der APP den QR-Code einlesen, um die Authentifizierung zu starten. Die APP verarbeitet die darin enthaltenen Informationen und kommuniziert mit dem Authentifizierungsmanager, um den Nutzer schließlich zu authentifizieren (Bild 1).

Das Authentifizierungsergebnis und die angefragten Nutzerdaten werden dann vom Authentifizierungsmanager an den Diensteanbieter übermittelt. Die Authentifizierung an sich wird über ein PKI-basiertes Challenge-Response-Verfahren unter Verwendung des persönlichen Schlüsselmaterials des Nutzers, umgesetzt.

Konzept der Smartphone Bürger-ID App für NRW

In Bild 2 ist das Konzept der Smartphone Bürger-ID App für NRW dargestellt. Die Anwendungsfelder im Bereich eGovernment und SmartCity sind dargestellt und die Sicherheitsfunktionen für die Authentifizierung, Signatur und Payment als wichtige IT-Sicherheits- und Vertrauensdienste sind als „enabler" positioniert.

Die Registrierung des Bürgers funktioniert über zwei einfache Schritte: Ein Bürger lädt sich die App auf sein Smartphone, etwa über den Play Store oder den App Store. Beim ersten Starten der App wird der Bürger nun aufgefordert, sein Smartphone zu personalisieren. Dafür kann er sich zum Beispiel an einem Self-Service-Terminal im Bürgerzentrum der Kommune registrieren. Dort wird einmalig der Personalausweis benutzt, um den Bürger sicher und einfach identifizieren zu können. Danach wird mit dem Smartphone ein QR-Code eingescannt, der dann die Smartphone-Bürger-ID-App koppelt. So kann innerhalb weniger Minuten die App lauffähig gemacht werden.

Um eine sichere Kommunikation zu ermöglichen, wird immer als erster Faktor für die Authentifikation ein Challenge-Response-Verfahren verwendet. Dafür werden während der Personalisierung mehrere Zertifikate zwischen dem Server und dem Smartphone ausgetauscht. So erhält jeder Faktor für die Authentifikation des Nutzers ein eigenes Schlüsselpaar, um später mehrere, unterschiedlich starke, Sicherheitslevel ermöglichen zu können. Das Smartphone, der biometrische Faktor, zum Beispiel ein Fingerabdruck oder eine Gesichtserkennung und eine PIN, bieten bis zu drei Faktoren: Besitz, Sein und Wissen.

Als Einsprungspunkt für die Authentifikation sind alle möglichen Auslöser denkbar, wie zum Beispiel QR-Codes, NFC (Near Field Communication), Bluetooth Beacons oder Sound. Bei jeder Authentifizierung oder Signierung von Daten, wird nun mithilfe der ausgerollten Zertifikate ein Schlüsselaustausch gestartet. Jede Session wird zusätzlich mit neuen Secrets (Geheimnissen) verschlüsselt, um dem Mitlesen von Informationen vorzubeugen. Die üblichen Angriffe, wie Man-in-the-middle-Attacken, werden zusätzlich durch das Signieren aller Daten verhindert. Passwörter werden komplett aus dem Authentifikationsprozess substituiert. Übliche Angriffsvektoren auf die Passwörter der Nutzer, etwa durch Keylogger, funktionieren somit nicht mehr.

Wird jetzt ein Dienst der Stadt genutzt, lassen sich mithilfe der Smartphone Bürger-ID unterschiedliche Sicherheitsniveaus realisieren. Handelt es sich um einen besonders schützenswerten Dienst, etwa das Beantragen eines polizeilichen Führungszeugnisses, können entsprechend viele Faktoren für die Authentifikation gefordert werden, wie eine Kombination aus Besitz des Smartphones, der dazugehörigen PIN und des registrierten Fingerabdrucks oder eine Gesichtserken-

nung. Somit ist auf modernen Smartphones eine Multifaktor-Authentifizierung von mindestens drei Faktoren möglich. Andere, weniger schützenswerte Dienste, etwa das Bezahlen der Hundesteuer, können schnell erledigt werden, nur mit dem Basis-Challenge-Response-Protokoll, ohne weitere Faktoren zu fordern.

Sicherheit der verwendeten Schlüssel und Zertifikate

Alle Zertifikate werden während der Personalisierung hart an ein Smartphone gebunden. Hierfür werden möglichst viele Informationen des Smartphones genutzt, um die Schlüsselpaare vor Diebstahl zu schützen. Zusätzlich wird bei Android-Geräten ein Hardware-backed Keystore verwendet, um die Zertifikate mithilfe von Hardware-Kryptografie zu schützen (Bild 3). Seit Android 5.0 (erschienen im November 2014) können kryptografische Funktionen mithilfe des Hardware Keystores durchgeführt werden, ohne dass die Schlüssel in den Speicher geladen werden müssen. Zusätzlich sind weitere Schutzmechanismen aktiviert. Schlüssel können nur genutzt werden, wenn sich der Besitzer des Smartphones authentifiziert hat, etwa durch Entsperren des Smartphones oder per Freigabe durch die Biometrie.[7]

Die API des Keystores wird mit jedem großem Android Update weiterentwickelt. So kamen zusätzliche Funktionen dazu, wie zuletzt die Verwendung der Gesichtserkennung.

Bei iOS-Geräten wird die Secure Enclave von Apple verwendet. Diese ermöglicht das Speichern von Passwörtern, Schlüsseln und Zertifikaten in einem geschützten, hardware-basierten Schlüsselmanager. Dieser ist isoliert vom Prozessor, auf dem die Software läuft (Bild 4). Bei Anfragen an die Secure Enclave, etwa zum Verschlüsseln oder Entschlüsseln von Daten, wird immer nur das Ergebnis der Operation übertragen. Die Schlüssel werden nie in den Arbeitsspeicher geladen und erschweren den Diebstahl damit deutlich für Angreifer. Dieser Schutz ist in allen iOS-Geräten möglich, die eine TouchID oder FaceID unterstützen.[8]

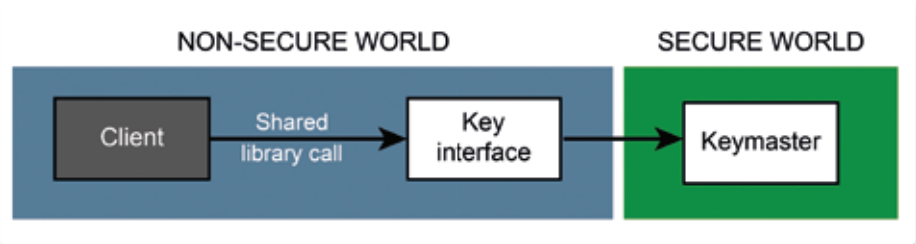

Bild 3: Aufruf des Keymasters durch die Smartphone App

Damit wird auf den beiden meistverwendeten Betriebssystemen für Smartphones sichergestellt, dass einem Angreifer der Datendiebstahl so schwierig wie möglich gemacht wird. Regelmäßige Überprüfungen, ob die Geräte nicht „gerooted" oder „gejailbreaked" wurden, vervollständigen das Sicherheitssystem.

Jede Session zwischen dem Server und dem Smartphone wird zusätzlich mit einem Session-Key und unter Verwendung der Perfect-

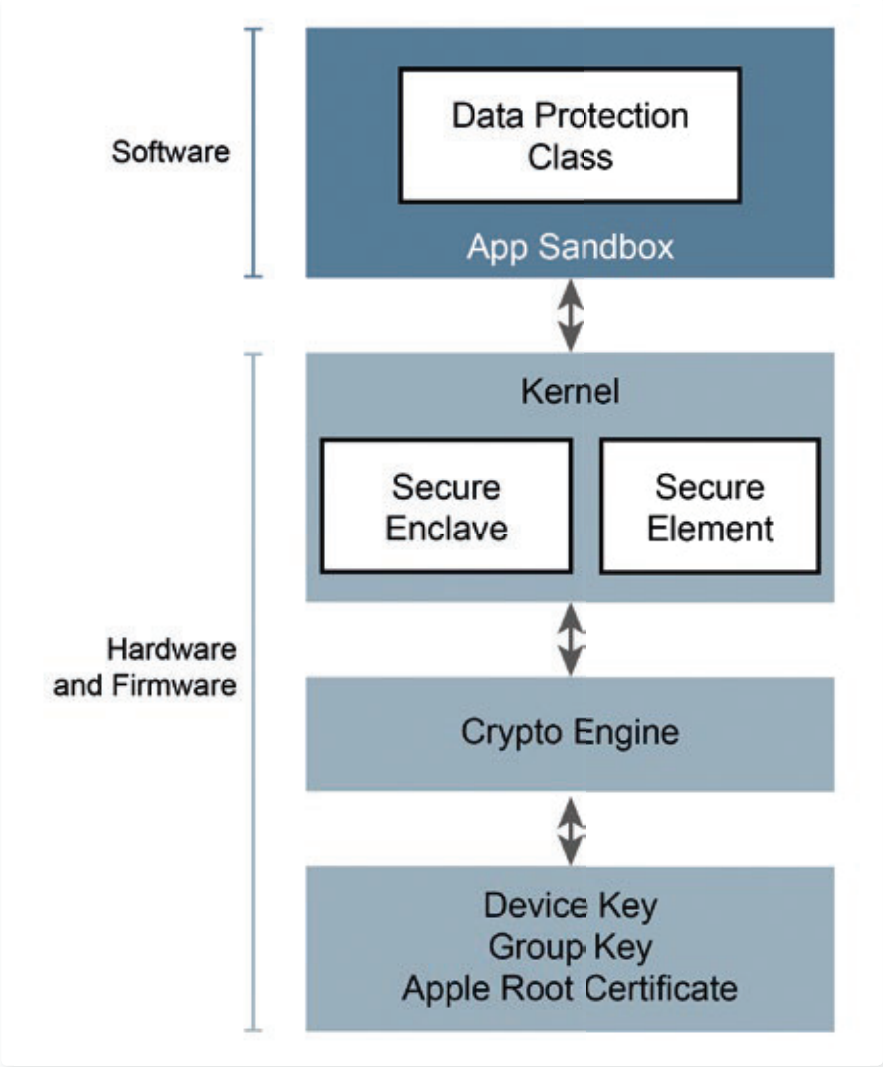

Bild 4: Aufruf einer kryptografischen Funktion in iOS

Forward-Secrecy-Methode verschlüsselt. Damit wird Replay-Attacken vorgebeugt und jeder Nachrichtenaustausch müsste explizit geknackt werden. Ein möglicher Angreifer im Netzwerk kann keine schützenswerten Daten mitlesen, da sie verschlüsselt sind.

Außerdem enthalten alle Einsprungspunkte einer Kommunikation, etwa die QR-Codes, nur das Minimum an Informationen, die benötigt werden, um eine Verbindung zum Server aufzubauen. Sollte dieser vom Angreifer gescannt werden, kann er keinen Schaden anrichten. Auch gefälschten QR-Codes wird vorgebeugt, da alle QR-Codes vom registrierten Identity-Manager signiert werden, dessen öffentlichen Schlüssel das Smartphone bei der Registrierung übertragen bekommt.

Um den Nutzer vor Schadsoftware zu schützen, die seinen Bildschirm aufnehmen oder sich als Keylogger ins System integriert haben, ist zusätzlich noch eine eigene Tastatur entwickelt worden. Diese ist immer zufällig angeordnet und liegt über der Softwaretastatur des Betriebssystems. Dadurch sind Eingaben des Nutzers, etwa die PIN, vor Angriffen geschützt.

Digitale Signatur

Mit der Smartphone Bürger-ID sind auch qualifizierte Signaturen nach eIDAS möglich. Mit dem substanziellen Sicherheitsniveau können elektronische Fernsignaturen realisiert werden, die eine physische Anwesenheit einer Person oder des bevollmächtigten Vertreters erübrigt. Die geforderte Zwei-Faktor-Authentifizierung ist ebenfalls sichergestellt. Die Anwendungsfälle sind breit gefächert: Anträge der Stadt lassen sich signieren, auch Geldüberweisungen können digital signiert werden, AGB und Verträge können bequem aus der Ferne mithilfe der Smartphone Bürger-ID unterzeichnet werden. Dies steigert nicht nur die Benutzerfreundlichkeit, sondern erhöht auch den Schutz, zum Beispiel gegen gefälschte Unterschriften oder bei gestohlenen Unterlagen. Damit können Bürger in Deutschland und in der ganzen EU Unterlagen rechtsgültig signieren.

Payment-Lösungen und weitere sicherheitsrelevante Dienste

Die entwickelte Technologie macht aber hier nicht Schluss: Um ein komplettes Ökosystem an digitalen Lösungen umsetzen zu können, ist auch die direkte Bezahlung von Warenkörben geplant. Statt den Nutzer zu zwingen, sich ständig neu registrieren und immer wieder die Rechnungsanschrift inklusive Überweisungsdaten einpflegen zu müssen, können Anbieter mit wenigen Schritten ihre Payment-Lösung ins System integrieren. Die verifizierten Nutzerdaten können über Föderationen mit Partnern erweitert werden, um den Bürger weiter zu schützen. Auch digitale Zahlungsmittel, wie Kryptowährungen (Bitcoin, Libra …) sind vorgesehen. Die Datenhoheit bleibt beim Nutzer.

Ausblick

Die Smartphone Bürger-ID ist ein Leuchtturmprojekt für die gesamte Bundesrepublik. Die Ideen für Anwendungsfälle sind fast grenzenlos. Aber auch die Interoperabilität der Lösung ist gegeben. Um in Zukunft möglichst keine Passwörter mehr benutzen zu müssen, gibt es die Möglichkeit, mehrere Identity Provider zu koppeln. So ist etwa denkbar, dass auch der Stromdienstleister der Stadt sein System anknüpft, um Auftragsbestätigungen digital ans Smartphone zu schicken und sich vom Bürger be-

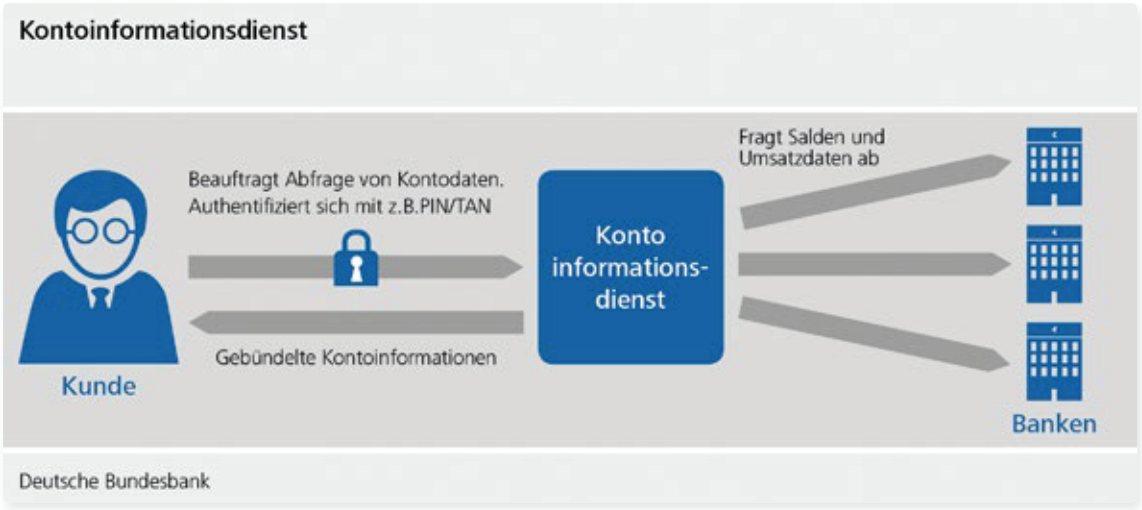

Bild 5: Übersicht aller Kundenkonten durch eine Kontoinformations-dienstleister

stätigen zu lassen. So können ganz neue Prozesse medienbruchfrei digitalisiert werden, ohne Briefe oder E-Mails verschicken zu müssen.

Mit den neuen Möglichkeiten der Authentifizierung gibt es auch neue Ideen und Richtlinien, die damit umsetzbar sind. Am 14. September 2019 trat die neue Zahlungsdienstrichtlinie in Kraft, besser bekannt als PSD2 (Payment Services Directive 2). Diese soll die Sicherheit im Zahlungsverkehr erhöhen und den Verbraucherschutz stärken, etwa durch Entfernen veralteter TAN-Verfahren. Ebenso bietet sie Dienstleistern die Möglichkeit, von Banken Salden und Umsatzdaten abzufragen.

Zusätzlich verpflichtet die PSD2 zur „starken Kundenauthentifizierung". Diese fordert mindestens zwei unabhängige Merkmale aus den Authentifikationskategorien Wissen, Besitz und Sein.[9]

Die Smartphone Bürger-ID ist ein wichtiger Baustein für eine sichere und vertrauenswürdige Digitalisierung und wird sicherlich noch in vielen weiteren Anwendungsfeldern helfen, die Risiken zu minimieren. ■

Literatur

[1] *Barbier, J. u.a.: „Cybersecurity as a growth advantage", abgerufen am 09.08.2019 von: https://www.cisco.com/c/dam/assets/offers/pdfs/cybersecurity-growth-advantage.pdf*

[2] *N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Springer Vieweg Verlag, Wiesbaden 2019*

[3] *Statista: Anteile der verschiedenen Android-Versionen an allen Geräten mit Android OS weltweit im Zeitraum 01. bis 07. Mai 2019, abgerufen am 09.08.2019 von: https://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os/*

[4] *David Smith: iOS Version Stats, abgerufen am 09.08.2019 von: https://david-smith.org/iosversionstats/*

[5] *BSI / juris: Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG), abgerufen am 09.08.2019 von: https://www.gesetze-im-internet.de/ozg/BJNR313800017.html*

[6] *M. Hertlein, P. Manaras, N. Pohlmann: „Die Zeit nach dem Passwort – Handhabbare Multifaktor-Authentifizierung für ein gesundes Eco-System", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 4/2016*

[7] *Google: Hardware-backed Keystore, abgerufen am 09.08.2019 von: https://source.android.com/security/keystore*

[8] *Apple: Storing Keys in the Secure Enclave, abgerufen am 09.08.2019 von: https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/storing_keys_in_the_secure_enclave*

[9] *Deutsche Bundesbank: PSD2, abgerufen am 09.08.2019 von: https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/psd2/psd2-775434*

NORBERT POHLMANN,
Informatikprofessor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

ALEXANDER STÖHR,
technischer Projektleiter für Smartphone Bürger-ID im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Er beschäftigt sich mit Multifaktor-Authentifikation sowie mit digitalen Signaturen für mehr Sicherheit und Vertrauenswürdigkeit in der Digitalisierung.