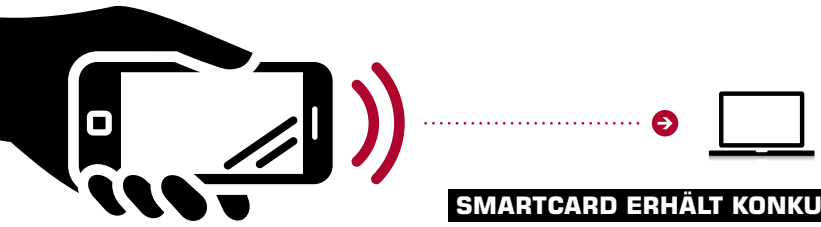

SMARTCARD ERHÄLT KONKURRENZ

Authentisierung via Smartphone

Nachdem die Sicherheitsindustrie bereits
DAS ENDE DES PASSWORTS
ausgerufen hat, leidet nun auch das Flaggschiff der starken Authentisierung, die Smartcard, unter dem immer größeren Anteil an Tablets, Smartphones und Ultrabooks.

Immer weniger Business-Modelle der PC-Hersteller besitzen fest verbaute Kartenleser und machen unbequeme, externe Lesegeräte notwendig. Bei anderen mobilen Endgeräten ist der Einsatz von Smartcards aufgrund der fehlenden USB-Ports gar nicht erst möglich. Gleichzeitig steigen jedoch die Anforderungen an die Sicherheit. Die Balance zwischen Benutzerfreundlichkeit, hohem Sicherheitsniveau und geringen Kosten zu finden, wird in diesem Kontext für viele Verantwortliche immer schwieriger. Eine Alternative könnte der Einsatz eines speziell ausgestatteten Smartphones bieten: In der Hardware von Android-Geräten wird das für die Zertifikate benötigte Schlüsselmaterial gesichert oder für iOS-Geräte mehrfach verschlüsselt in der App gespeichert.

Sicherheit ist ein hohes Gut. Erst recht, wenn es um die eigene Identität geht. Daher forschen Experten weltweit nach sicheren Authentisierungsverfahren, die fälschungsresistent und möglichst aufwandsarm Identitäten schützen helfen. Als Zwischenergebnis dieser Forschungen ist die Zwei-Faktor-Authentifizierung zu einem bewährten Mittel herangereift. Das Ziel jeder Art von Zwei-Faktor-Authentifizierung (2FA) ist es, das Vertrauen in die Identität eines Anwenders dadurch zu stärken, dass zwei unterschiedliche und unabhängige Faktoren zur Überprüfung der Identität herangezogen werden. Diese Faktoren resultieren in der Regel aus mehreren Komponenten: Aus etwas, was der Benutzer besitzt (Besitz) und etwas, was er kennt (Wissen) oder einer charakteristischen Eigenschaft (biometrische Merkmale).

Für Unternehmen sind Zwei-Faktor-Authentifizierungen ein wesentlicher Bestandteil der Sicherheitsstrategie, um hohen Zugriffsschutz auf die eigenen Systeme und Daten zu gewährleisten. Längst werden hierbei nicht mehr nur die eigenen Mitarbeiter betrachtet, sondern gleichermaßen externe Dienstleister und Zulieferer. Die immer enger verzahnten Wertschöpfungsketten erfordern eben auch ein durchgängiges Sicherheitsniveau in der Lieferkette. Um die erforderliche Sicherheit zu erreichen, setzen viele Unternehmen auf eine PKI-/zertifikat-basierte Authentifizierung und einer Smartcard als Träger der verwendeten Sicherheitsschlüssel.

Smartcards sind teuer

Smartcards gewährleisten bei kryptografischen Operationen eine hohe Sicherheit, da der private Schlüssel die Smartcard nie verlässt. Allerdings gehen mit dem physischen Medium „Smartcard" auch Nachteile einher. Die Kosten dafür sind recht hoch. Zudem schlagen die mit ihrem Handling verbundenen weiteren Kosten wie Hardware (z.B. Kartenlesegeräte) und vor allem der logistische Aufwand der Verteilung oder die komplexen Prozesse für einen Ersatz bei Verlust oder Beschädigung ebenfalls zu Buche. Folglich sind viele Verantwortliche auf der Suche nach preiswerteren Lösungen, die ihre Organisationen ohne großen Aufwand integrieren können.

Die sich ändernden Anforderungen im Zusammenhang mit Cloud-Apps und dem Einsatz mobiler Geräte, kombiniert mit täglich zunehmenden Bedrohungen, erfordern neue Überlegungen zur sicheren Steuerung des Zugriffs auf IT-Ressourcen. Da neben einer technologischen Beherrschbarkeit und geringem Total Cost of Ownership auch eine einfache Handhabung für die Anwender Berücksichtigung finden sollte, wird die Nutzung von Smartphone-Apps für die Bereitstellung eines zweiten Faktors zunehmend interessanter.

Der Vorteil aus Sicht der User ist, dass die meisten ihr Smartphone ständig bei sich tragen. Der Google Authenticator und ähnliche Apps gewinnen bei den Privatnutzern mit mäßigen Sicherheitsanforderungen kontinuierlich an Bedeutung für die Anmeldung an lokalen Anwendungen oder Cloud-Diensten. Eine Anmeldung am Client ist mit diesen Systemen jedoch nicht abzusichern, da hier die Integration ins Betriebssystem fehlt. Bei einem im Geschäftsumfeld benötigten hohen Sicherheitsniveau einer Smartcard müssen die meisten app-basierten mobilen Authentisierungslösungen pas-

SO FUNKTIONIERT
DIE eSIM

Statt wie bisher für jedes Mobiltelefon eine SIM-Karte vom Provider zu erhalten und diese mühsam im richtigen Formfaktor in das Gerät zu setzen, können neuere Geräte einen speziell abgesicherten Speicherbereich – ähnlich eines Trusted-Platform-Modules (TPM) im PC – auf ihrer Platine nutzen, um Anwenderdaten und den Inhalt der aktuell zu verwendeten Provider-ID speichern. Hierfür werden standardisierte Verfahren und speziell abgesicherte Provisionierungs-Server eingesetzt, die über verschlüsselte Kanäle den entfernten Zugriff auf einzelne Segmente des sicheren Speichers ermöglichen. Diese Segmente können ähnlich wie Schließfächer exklusiv einem Anwendungsbereich zugeordnet werden, sodass sie potentiell zur sicheren Speicherung von Zertifikaten im geschützten Speicherbereich des Geräts nutzbar gemacht werden können.

Quelle: Apiida AG

sen. Die Schlüssel und Zertifikate werden hier meist im Speicher des Smartphones abgelegt und sind somit relativ einfach zu extrahieren, wie Berichte von Sicherheitsforschern zeigen.

Neue Horizonte eröffnen

Um kostengünstig ein hohes Sicherheitsniveau zu schaffen, wäre folglich die Speicherung des kryptographischen Schlüsselmaterials und der Zertifikate innerhalb einer separierten, sicheren Hardware erforderlich. Dies bieten aktuelle Lösungen für Smartphones bisher jedoch nicht. Hier bietet die Einführung der Embedded SIM (eSIM) neue Ansätze, welche – ähnlich einer Smartcard – einen abgesicherten Speicherchip auf der Platine des Smartphones nutzt. Damit scheint es möglich, künftig das Smartphone auch als äquivalent sicheren Ersatz für die Smartcard nutzen zu können. Es scheint nur eine Frage der Zeit zu sein, bis der Markt entsprechende Produkte bereithält. Ein deutsches Unternehmen, die Apiida AG, hat angekündigt, mit „Mobile Authentication“ noch 2017 eine entsprechende Lösung herauszubringen. Lösungen wie diese können eine Alternative zur Smartcard sein, indem sie auf der einen Seite, die spürbaren Nachteile (Hardware, Kosten) beheben und gleichzeitig deren Vorteile (hohes Sicherheitsniveau) beibehalten.

Durch die Nutzung vorhandener PKI-Infrastrukturen, können Firmen einen fließenden Umstieg oder eine hybride Nutzung von Smartphone und Smartcard realisieren. Damit sollen auch solche Unternehmen von den neuen Möglichkeiten profitieren, bei denen der Einsatz von Smartphones in bestimmten Umgebungen (z.B. in der Produktion) nicht möglich ist. Kurzum: Wo auch immer bereits Smartphones im Einsatz sind, können diese zur Authentifizierung im Firmennetzwerk genutzt werden.

SEBASTIAN ROHR