WHITE PAPER
SICHERE IDENTITÄTEN IN DER DIGITALEN WELT

T · · Systems ·

INHALT

EINLEITUNG

Wir alle bewegen uns heute wie selbstverständlich in der virtuellen digitalen Welt des Internets. Dabei nehmen wir für verschiedene Zwecke unterschiedliche Identitäten an: In Chatrooms agieren wir anonym, beim Online-Shopping kaufen wir mit unserem Klarnamen ein, in einigen Social Media-Kanälen entscheiden wir uns für ein Pseudonym und im Büro weist uns der Arbeitgeber einen Nutzernamen zu.

Die Nutzer der digitalen Welt besitzen demnach viele Identitäten. Da man sich bei der Registrierung in einem Online-Shop oder in einem Chatroom i.d.R. nicht ausweisen muss, können die Chatpartner oder Shopbetreiber zumeist nicht wirklich wissen, wer sich tatsächlich hinter einer digitalen Identität verbirgt. Dies führt zu Missbrauch auf allen Seiten. Diebe kaufen unter falscher Identität Waren ein, plündern Online-Banking-Konten oder missbrauchen Chats für ihre persönlichen Zwecke.

Damit stellt sich die Kernfrage: Wer verbirgt sich tatsächlich hinter einer Identität?

In der realen Welt lässt sich diese Frage meist einfach beantworten: Die Identität einer Person lässt sich hier leicht mittels Ihres Ausweises nachweisen.

In der digitalen Welt ist der Nachweis der Identität um ein Vielfaches schwieriger, da sich Geschäfts- oder Kommunikationspartner oft nicht kennen und in der Regel auch nicht zusammentreffen können. Aus diesem Grund behelfen sich Online-Shops, Banken oder Social Media-Kanäle meist mit der Kombination aus einem Nutzernamen und einem Passwort, die bei der Registrierung des Nutzers durch diesen selbst zu vergeben sind. Dieses einfache Verfahren birgt jedoch zunehmend große Risiken, da Nutzername und Passwort in Datenbanken gespeichert sind oder über manipulierte Seiten ausgespäht werden können. Dies ermöglicht es Dieben, digitale Identitäten in großem Stile zu stehlen und zu verkaufen oder selbst für kriminelle Zwecke zu nutzen.

Obwohl inzwischen fast monatlich neue und immer verheerendere Fälle von Identitätsdiebstählen bekannt werden, scheinen sich viele Nutzer wenig Gedanken über die Risiken zu machen. Oder es bleibt ihnen keine andere Wahl, um am Leben in der digitalen Welt teilzunehmen. Es gibt kaum mehr einen Internetservice, für den sich die Nutzer nicht registrieren und dafür ihre persönlichen Zugangsdaten festlegen müssen.

Und da sich niemand für die Vielzahl der genutzten Internetzugänge unterschiedliche Passwörter merken kann, vergeben die Nutzer für diverse Online-Shops, E-Mail-Accounts oder den Facebook-Zugang immer wieder die gleichen, zu kurze oder triviale Passwörter, die durch Cyberkriminelle mit spezieller Software in wenigen Sekunden entziffert werden können.

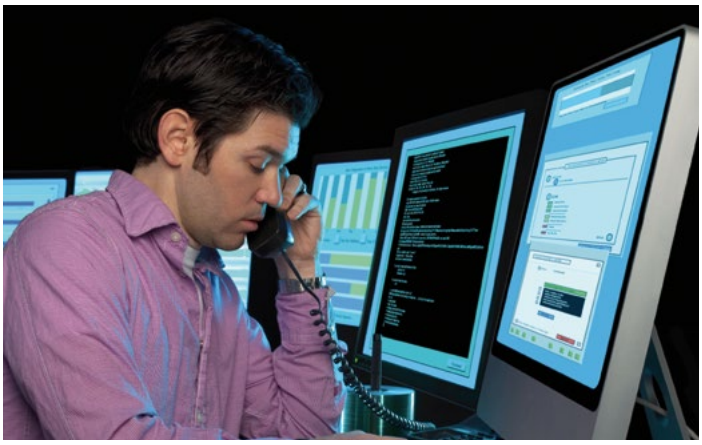
Zusätzlicher Druck droht Unternehmen und Betreibern von Infrastrukturen aus einer gänzlich anderen Ecke. Die Stichwörter heißen Internet der Dinge und Industrie 4.0. Bisher waren industrielle Steuerungssysteme (ICS – Industrial Control Systems) von anderen IT-Systemen und Netzen entkoppelt. Von außen gab es dabei z.B. keine Möglichkeit, auf die Steuerungssoftware einer Produktionsstraße zuzugreifen. Inzwischen werden Maschinen, Autos oder einzelne Geräte immer mehr mit dem Internet vernetzt. Sie bekommen wie Rechner, Drucker oder Smartphones eigene IP-Adressen, womit man sie über das Netz aus der Ferne ansteuern kann. Gartner sagt für 2020 bereits 25 Milliarden Geräte voraus, die mit dem Internet verbunden sein werden. Setzt man hier z.B. Nutzernamen und Passwort zur Identifizierung ein, so kann es Dieben ein Leichtes sein, nach einem Datendiebstahl auf die Geräte aus der Ferne zuzugreifen.

Das vorliegende Whitepaper soll zeigen, dass es Alternativen zur Abbildung digitaler Identitäten gibt, die fernab von der Verwendung der sogenannten Ein-Faktor-Authentifizierung mittels Nutzername und Passwort liegen. Die Stichworte heißen Zwei-Faktor-Authentifizierung und Erzeugung und Speicherung von Schlüsseln aus sicherer Quelle. Dabei ermöglicht die Zwei-Faktor-Authentifizierung eine sichere Zuordnung von Nutzern und Dingen durch eine Kombination aus dem Wissen eines Geheimnisses und dem Besitz eines Token zur Identifizierung.

RISIKEN IM INTERNET

Immer mehr Cyberkriminelle entdecken für sich ein neues Geschäftsfeld: Den Identitätsdiebstahl. Sie kapern Facebook-Accounts oder greifen Anmelde- und Bezahldaten von Online-Shops ab. Im Anschluss nutzen sie die Daten für eine Einkaufstour oder treten unter fremden Namen in Social-Media-Plattformen auf und beschimpfen und belästigen andere Mitglieder. Oder sie versenden massenhaft E-Mails, um weiteren Schaden auf fremden Rechnern anzurichten und noch mehr Daten abzuziehen. Oder sie bestellen Handy-Verträge, beantragen Kreditkarten mit der gestohlenen Identität oder eröffnen sogar Bankkonten.

Anfang 2014 haben Hacker zunächst 16 Millionen, kurze Zeit später 18 Millionen E-Mail-Adressen samt Zugangsdaten von fremden Rechnern gestohlen. Damit zählen die beiden Angriffe zu den größten, bisher bekannt gewordenen Diebstählen kompletter digitaler Identitäten in Deutschland. Für das Bundesamt für Sicherheit in der Informationstechnik (BSI) sind die beiden Fälle nur die Spitze des Eisbergs. Denn meist bleibt der Klau von E-Mail-Adressen, Passwörtern und PINs unerkannt. Das BSI zählt Identitätsdiebstahl daher zu einem der größten Risiken der Internetnutzung, da selbst der ständige Wechsel von Passwörtern oder ein Virenschutz samt Firewall kein wirkliches Hindernis für zunehmend professionellere Hacker darstellen. Eine repräsentative Online-Umfrage des Wirtschaftsauskunftsdienstes Schufa bestätigt das BSI: 15 Prozent aller deutschen Internet-Nutzer sind bereits Opfer von Identitätsdiebstahl geworden.



Für den Diebstahl von digitalen Identitäten setzen die Kriminellen auf ganz verschiedene Methoden. Der einfachste Weg ist ein nicht-digitaler Klassiker: Die Diebe stehlen Smartphones samt den gespeicherten Daten. Wer hier seine PINs und Passwörter unverschlüsselt abgelegt hat, wird dann schnell zum Opfer.

Die am weitesten verbreitete Methode ist der Einsatz von Schadsoftware, mit denen sich die Daten beliebiger Art von Computern abgreifen lassen. Um die Schadsoftware auf dem Fremdrechner zu platzieren, entwickeln die Hacker ihre Methoden ständig weiter. So fälschen sogenannte Phishing-Betrüger seriöse Internetseiten und verstecken dort z.B. Viren oder Verweise auf schadhafte Seiten in Werbebannern. Laut dem IT-Sicherheitsunternehmen Sophos werden auf diese Weise täglich rund 30.000 Webseiten infiziert. Ein weiterer Trick der Phishing-Betrüger besteht darin, E-Mails angeblich seriöser Banken, bekannter Firmen oder mit der E-Mail-Adresse eines Bekannten an ihre Opfer zu senden. Über einen verseuchten Link fordern sie die Empfänger auf, einen Anhang zu öffnen oder Daten auf einer Website zu aktualisieren. Tatsächlich führt der Link zu einer manipulierten Website, die die dort einzugebenden Daten – oft Kreditkartennummer oder Passwörter – nur abgreifen muss, um sich die Identität des Opfers anzueignen. Ein anderer Weg besteht darin, Mails mit Viren zu versenden, die sich unbemerkt im Rechner einnisten und im Hintergrund Daten protokollieren und an die Betrüger senden.

Aber was lässt sich gegen den Diebstahl der digitalen Identität tun? Wie kann ich mich schützen und verhindern, dass Betrüger meine Identität stehlen und für ihre Zwecke missbrauchen?

MEHR SICHERHEIT DURCH ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Wie in den vorangegangenen Abschnitten aufgezeigt besteht die digitale Identität eines Nutzers in der Regel aus einer Kombination von Benutzername und Passwort. Die geringe Sicherheit dieser sogenannten Ein-Faktor-Authentifizierung basiert auf dem Wissen des zu einem Benutzernamen gehörenden geheimen Passwortes.

Als sicherere Alternative zur Ein-Faktor-Authentifizierung bieten sich verschiedene Verfahren zur Zwei-Faktor-Authentifizierung an. Deren Sicherheit basiert nicht alleine auf dem Wissen eines Passwortes als „erstem Faktor" sondern zusätzlich auf einem zweiten Faktor, der z.B. im Besitz eines Hardwaremoduls bestehen kann.

Ein etabliertes Verfahren der Zwei-Faktor-Authentifizierung ist die Vergabe von Einmalpasswörtern mittels eines beim Nutzer vorliegenden One-Time-Pass-Token (OTP-Token), der als einzelnes Hardwaretoken oder auf einem Smartphone realisiert werden kann. Mit Hilfe des OTP-Token wird bei diesem Verfahren ein Einmalpasswort erzeugt, bei der Anmeldung am jeweiligen Service zusammen mit einem weiteren Passwort als Login-Information eingegeben und anschließend im Hintergrundsystem mit dem von einem Authentifizierungsserver generierten Einmalpasswort verglichen. Dabei arbeiten der Authentifizierungsserver und das Token mit den gleichen Schlüsseln und Algorithmen und können damit die gleichen Passwörter erzeugen. Der erste Faktor ist dabei das OTP-Token (Besitz) und der zweite Faktor das zusätzliche Passwort (Wissen). Dabei ist es von Vorteil, wenn die Server-Komponente der Zwei-Faktor-Authentifizierung in einer hochsicheren, zertifizierten Umgebung betrieben wird.

Neben OTP gibt es weitere hardwarebasierte Verfahren mit einer Zwei-Faktor-Authentifizierung, die die Sicherheit von digitalen Identitäten deutlich steigern können. Die Authentifizierung erfolgt hierbei zertifikatbasiert mittels einer Smartcard oder einem USB-Token. Ein Zertifikat ist dabei eine elektronische Sammlung von Identitätsmerkmalen des Inhabers wie z.B. Name, Anschrift oder Geburtsdatum, die durch eine allseits anerkannte Stelle – eine sogenannte Zertifizierungsstelle (CA) – in einem sogenannten Trust Center mittels elektronischer Signatur besiegelt wird.

DIE FUNKTION EINES TRUST CENTERS

Für die Ausstellung einer digitalen Identität mit einer Karte erzeugt in Deutschland ein vom BSI zertifiziertes Trust Center zunächst ein Zertifikat. Um ein Zertifikat zu erhalten, muss die Person ihre Identität einmalig gegenüber dem Trust Center selbst oder gegenüber einer anerkannten Registrierungsstelle mittels eines physikalischen Ausweisdokuments persönlich nachweisen. Der Nachweis einer Identität kann auch mit Hilfe des neuen Personalausweises elektronisch erfolgen.

Für die digitale Identität erzeugt das Trust Center ein Schlüsselpaar aus privatem und öffentlichem Schlüssel, hinterlegt den privaten Schlüssel sicher auf einem Token und erzeugt ein Zertifikat, das den öffentlichen Schlüssel zusammen mit den auf Echtheit geprüften Identifikationsmerkmalen des Teilnehmers sowie die Signatur des Trust Centers zur Zertifizierung der Echtheit des Zertifikats enthält. Das Zertifikat stellt sicher, dass der Schlüssel in einer vertrauenswürdigen Umgebung erzeugt wurde, der private Anteil sicher gespeichert ist und den Identitätsmerkmalen im Zertifikat vertraut werden kann. Damit ist die Basis für ein „elektronisches Vertrauensverhältnis" geschaffen. Diese Zertifikate können an alle Teilnehmer einer Public-Key-Infrastruktur (PKI) weitergegeben oder in Verzeichnissen veröffentlicht werden.

EXKURS: BESTANDTEILE EINER PUBLIC-KEY-INFRASTRUKTUR (PKI)

Digitale Zertifikate:	Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.
Trust Center:	Stellt das CA-Zertifikat bereit und übernimmt die Signatur von Zertifikatsanträgen.
Registrierungsstelle:	Hier können für Personen und Maschinen Zertifikate beantragt werden. Sie prüft die Richtigkeit der Daten und genehmigt den Zertifikatsantrag.
Zertifikatssperrliste:	Eine Liste mit zurückgezogenen Zertifikaten, bedingt durch Kompromittierung des Schlüsselmaterials oder Ungültigkeit der Zertifikatsdaten.
Verzeichnisdienst:	Ein durchsuchbares Verzeichnis, das ausgestellte Zertifikate enthält.
Validierungsdienst:	Ein Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht.

EXKURS: KRYPTOGRAPHIE

Kryptographie war ursprünglich ein Sammelbegriff für die Wissenschaft der Verschlüsselung von Informationen. Heute umfasst sie das weitreichende Thema der Informationssicherheit von der Konzeption über die Spezifikation bis zur Realisierung von Informationssystemen, die widerstandsfähig gegen unbefugtes Lesen und Verändern sind.

Die wichtigsten Säulen der Kryptographie sind Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit und Nichtabstreitbarkeit von Informationen. Zunächst wurde der Begriff Kryptographie nur für die Verschlüsselung und damit die Sicherung der Vertraulichkeit von Informationen verwendet. Dies bedeutete die Umwandlung der Informationen von einem Klartext in einen nicht verständlichen Geheimtext. Entschlüsselung bedeutet das Gegenteil, also das Umwandeln eines Geheimtextes in einen verständlichen Klartext. Später wurde der Begriff dann immer weiter gefasst und stellt nun einen Sammelbegriff für alle Funktionen dar, die zur Sicherung von Informationen nötig sind.

Bei Kryptographie wird zwischen symmetrischer und asymmetrischer Kryptographie unterschieden, hier erläutert am Beispiel der Verschlüsselung.

SYMMETRISCHE VERSCHLÜSSELUNG

Ausgangssituation:

- Der Sender Bob möchte der Empfängerin Alice eine verschlüsselte Nachricht senden.

Vorgehen:

- Zur sicheren Kommunikation erhalten Alice und Bob einen gemeinsamen, symmetrischen Schlüssel.
- Bob nutzt den symmetrischen Schlüssel, um die Nachricht für Alice zu verschlüsseln.
- Alice kann die Nachricht dann mittels des gleichen symmetrischen Schlüssels entschlüsseln.
- Das Modell lässt sich mittels eines Vorhängeschlosses darstellen, für den beide Parteien den gleichen Schlüssel besitzen.

ABB. 1. Symmetrische Verschlüsselung

ASYMMETRISCHE VERSCHLÜSSELUNG

Ausgangssituation:

- Der Sender Bob möchte der Empfängerin Alice eine verschlüsselte Nachricht senden, ohne mit ihr vorher einen gemeinsamen Schlüssel zur Verschlüsselung abgestimmt zu haben.

Vorgehen:

- Zur sicheren Kommunikation erhält Alice ein Schlüsselpaar bestehend aus öffentlichem und privatem Schlüssel, von dem sie Bob den öffentlichen Anteil übermitteln kann.
- Bob nutzt den öffentlichen Schlüssel, um die Nachricht für Alice zu verschlüsseln.
- Alice kann die Nachricht dann mittels ihrem privaten, nur ihr bekannten Schlüssel entschlüsseln.
- Das System lässt sich leicht mit einem Briefkastenmodell darstellen, in dem Bob den Einwurfschlitz kennt und nur Alice den Schlüssel des Briefkastens besitzt.

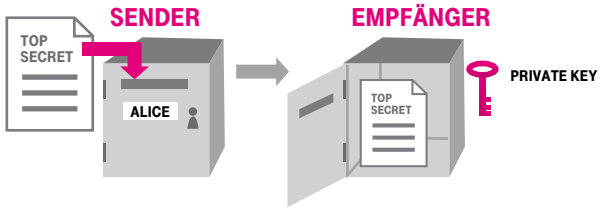


ABB. 2. Asymmetrische Verschlüsselung

Für die Zertifikate innerhalb einer PKI führt das Trust Center einen sogenannten Verzeichnisdienst. Dieser entspricht einer Art Telefonbuch, in dem Zertifikate anhand des Namens nachgeschlagen werden können. Ebenso wie beim Telefonbuch kann der Inhaber von Zertifikaten auch bestimmen, nicht in das Verzeichnis aufgenommen zu werden.

Über den Widerrufsdienst eines Trust Centers kann der Inhaber sein Zertifikat sperren. Dabei verliert das Zertifikat sofort seine Gültigkeit und kommt auf eine Sperrliste. Die Sperrliste kann von der Homepage des Trust Centers heruntergeladen werden.

Ohne es zu wissen nutzen Verbraucher längst Zwei-Faktor-Sicherheitslösungen, zum Beispiel mit ihrer chipbasierten EC-Karte. Hier authentifizieren sie sich gegenüber dem Geldautomaten mittels ihrer Karte und der nur ihnen bekannten PIN. Auch wenn bei diesem Verfahren Missbrauchsfälle nicht ausgeschlossen sind, ist es weitaus sicherer als nur der Einsatz von Benutzername und Passwort. Wer mit einer EC-Karte Geld abheben will, muss die Karte stehlen und die passende PIN kennen. Verliert jemand seine Karte oder wird sie gestohlen, lässt sie sich sofort sperren und wird damit unbrauchbar.

EXKURS: TRUST CENTER DER T-SYSTEMS

T-Systems betreibt ein akkreditiertes Trust Center in einem Hochsicherheitsrechenzentrum, das im Dezember 1998 als erstes Trust Center bundesweit die Genehmigung zum Betrieb einer Zertifizierungsstelle für die elektronische Signatur gemäß dem deutschen Signaturgesetz (SigG) durch die Regulierungsbehörde für Telekommunikation und Post (heute: Bundesnetzagentur) erhielt. Qualifizierte Zertifikate (TeleSec Public-Key-Service) sind seit 1999 Teil des Portfolios des Telekom Trust Centers. Dieses ist seit Oktober 2013 nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert.

T-Systems bietet Trust Center Services für Großkunden, Mittelstand und Endkunden an. Das Portfolio umfasst qualifizierte Zertifikate und Zertifikate aus dem fortgeschrittenen Bereich. T-Systems plant, realisiert und betreibt eine Reihe von speziellen Public-Key-Infrastrukturen für Großkunden aus Industrie, Behörden, Ländern und Organisationen.

Das Trust Center bietet darüber hinaus verschiedene standardisierte Lösungen zur Authentifizierung, Verschlüsselung und elektronischen Signatur für den Mittelstand an. Ein wesentlicher Bestandteil der Trust Center Services sind Zertifikate für Webserver. Von großer Bedeutung ist die Bereitstellung standardisierter Schnittstellen und Protokolle, die eine kostengünstige Integration in die Anwendungen unserer Kunden ermöglicht.

EC- oder Kreditkarten sind die einzige Ausnahme, in der sich die Zwei-Faktor-Authentifizierung bisher flächendeckend durchgesetzt hat. Obwohl es seit vielen Jahren ausgereifte Lösungen dafür gibt, nimmt sie der Markt nicht an. Dies liegt an der oftmals unzureichenden Nutzerfreundlichkeit und dem komplexen Anmeldeverfahren für die bisherigen Zwei-Faktor-Sicherheitslösungen.

ABB. 3. Hochsicherheitsbereich – Security Made in Germany

Inzwischen bewegen sich auf Hardware basierende Authentifizierungslösungen aus einem Nischenmarkt heraus. Besonders größere Unternehmen erkennen, dass sie angesichts der zunehmenden Bedrohung aus dem Internet handeln müssen, denn ohne die Anbindung an das Internet läuft in den Unternehmen kaum mehr ein Geschäftsprozess ab. Dafür nutzen Mitarbeiter sensibelste Daten oder steuern geschäftskritische Abläufe. Stehlen Cyberkriminelle Zugangspasswörter, stehen ihnen Tür und Tor offen für Manipulation und Zerstörung. Im schlimmsten Fall muss eine Firma wegen eines Identitätsdiebstahls Software abschalten. Dann kann in nur wenigen Tagen das Aus drohen.

Ein zusätzlicher Anschub für die Zwei-Faktor-Authentifizierung könnte von Google ausgehen. Selbst Google hinterfragt den Username-Passwort-Ansatz und fordert digitale Identitäten, die über Hardware und Passwort doppelt gesichert sind. Jedenfalls will Google in die nächsten Versionen von Android und Chrome Schnittstellen für Authentifizierungslösungen auf Token-Basis einbauen. Einen weiteren Schub zur stärkeren Authentifizierung könnten hardwarebasierte Fast IDentity Online (FIDO)-Token bringen, die Verbraucher in jedem Elektronikmarkt kaufen können und die sich zur sicheren Anmeldung an verschiedenen Services nutzen lassen sollen.

HARDWARE-SICHERHEITS-TOKEN

Wird der private Schlüssel nicht geheim gehalten, so ist ein Missbrauch der digitalen Identität nicht ausgeschlossen. Ein Angreifer könnte die Identität eines anderen Teilnehmers nutzen. Die Sicherheit der digitalen Identität hängt daher maßgeblich von der Sicherheit des privaten Schlüssels ab. Dabei spielt nicht nur die sichere Speicherung des Schlüssels ein Rolle, sondern vielmehr der gesamte Lebenszyklus eines solchen privaten Schlüssels: von der sicheren Generierung über die Speicherung und Nutzung bis hin zur sicheren Vernichtung.

Wie zu Beginn erwähnt wird die Generierung von Schlüsseln in der sicheren Umgebung eines Trust Centers realisiert. Für die sichere Speicherung und Nutzung der Schlüssel haben sich Hardware-Sicherheitslösungen etabliert, sogenannte Hardware-Sicherheits-Token. Diese basieren in der Regel auf Smartcard-Technologie und ermöglichen es, den privaten Schlüssel vor Hackern geschützt sicher zusammen mit dem Zertifikat des zugehörigen öffentlichen Schlüssels abzulegen. Ferner unterstützen sie die Durchführung kryptographischer Operationen mit diesem Schlüssel. Dies bedeutet, dass der Schlüssel auch bei der Durchführung der Operationen im sicheren Speicher des Token bleibt und nicht ausgegeben werden muss.

Hardware-Sicherheits-Token gibt es inzwischen in verschiedenen Varianten, wie zum Beispiel als kleine Schlüsselanhänger, die der Nutzer immer bei sich tragen kann. Verliert der Nutzer den Token mit seinem Schlüssel, dann fällt das schnell auf und das Zertifikat lässt sich direkt sperren. Selbst wenn der Verlust erst spät bemerkt wird, ist der Token ohne das dazu passende Passwort unbrauchbar.

Interessant sind Hardware-Sicherheits-Token besonders für Unternehmen. Sie können jedem Mitarbeiter einen Schlüssel ausstellen, mit dem er sich dann je nach Aufgabengebiet gegenüber definierten Anwendungen identifizieren kann. So lassen sich Zugangsberechtigungen in einzelne Gebäudeteile festlegen, Mitarbeiter können sich mit dem Token am Rechner anmelden, Dokumente elektronisch signieren oder E-Mails verschlüsseln. Selbst die Bezahlung des Kantinenessens lässt sich bargeldlos mit dem Token abwickeln.

ABB. 4. Schlüsselgenerator der Telekom – deutsche Krypto-Codes sichern die Digitalisierung

EXKURS: DER AUTHENTIFIZIERUNGSPROZESS MITTELS HARDWARE- SICHERHEITS-TOKEN

Der Authentifizierungsprozess des Nutzers läuft in der Regel nach folgendem Schema ab:

- Der Nutzer leitet den Datenaustausch zwischen Token und Prüfsystem ein, indem er den Token zum Beispiel in ein Lesegerät steckt oder vor ein Lesegerät hält.
- Das Lesegerät identifiziert das Token über dessen eindeutige Identifikationsnummer.
- Der von dem Token gelesene Datensatz wird vom Prüfsystem nach einem definierten kryptographischen Prüfverfahren verglichen.
- Zur Sicherheit werden die lokalen Referenzdaten zusätzlich mit weiteren Referenzdaten aus einer Datenbank von einem entfernten Server verglichen.
- Bei ungültigem Token weist das Prüfsystem den Zugriff ab.
- Zur Rückverfolgung der Authentifizierung werden Ereignisdaten des Prüfvorgangs an den Server zurück übermittelt.
- Das Prüfsystem gibt die für den Träger des Token zulässige Benutzung wie Funktionen oder Daten frei.

DIE VORTEILE VON HARDWARE-SICHERHEIT

Hardware-Sicherheits-Token basieren auf Smartcard-Technologie. Daraus ergeben sich eine Vielzahl von Vorteilen gegenüber Softwarelösungen.

Der Schlüssel liegt fest auf der Smartcard und kann nicht ausgelesen werden.

Der Nutzer kann den Besitz des privaten Schlüssels und damit seine Identität nur nachweisen, indem er die Smartcard verwendet. Nach Entfernung der Smartcard aus dem Lesegerät ist keine Authentifizierung mehr möglich. Darüber hinaus wird die Verwendung der Smartcard durch eine PIN geschützt. Der Besitz der Smartcard allein reicht also nicht aus, die PIN muss auch bekannt sein. Die Sicherheit der Authentifizierung beruht also auf zwei Dingen, dem Besitz der Smartcard und der PIN-Kenntnis.

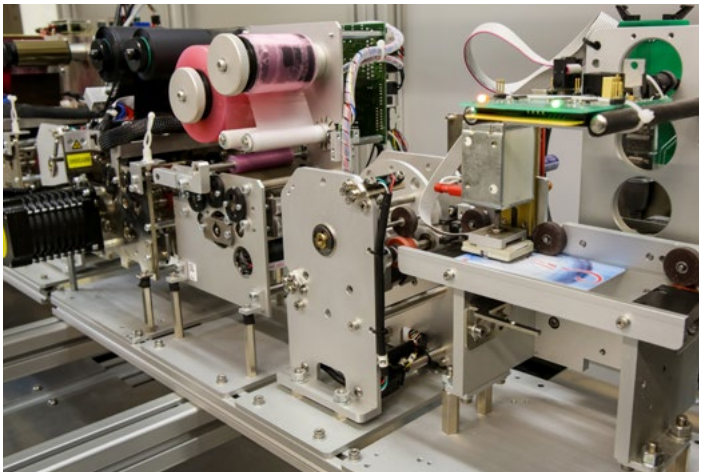


ABB. 5. TCOS Smartcard Personalisierung – Sichere Digitale Identitäten aus Deutschland

Smartcards besitzen einen Mikroprozessor, der den Zugriff auf die gespeicherten Daten ermöglicht.

Es ist nicht möglich den Datenspeicher direkt auszulesen, sondern nur über den I/O (Ein- und Ausgang) und über die CPU (Prozessor). Mit Hilfe des Prozessors lassen sich kryptographische Verfahren entwickeln, die die gespeicherten Daten vor fremdem Zugriff schützen. Ist der Chip einmal hergestellt, lassen sich die auf der Smartcard laufenden Programme nicht mehr ändern.

Smartcards ermöglichen die gesicherte Ablage von Passwörtern und Schlüsselmaterial.

Smartcards verfügen über ein sicheres Smartcard-Betriebssystem, das verschiedenste kryptographische Funktionen bereitstellt. Sie gewährleisten die sichere Datenspeicherung und Datennutzung und bieten meist eine entsprechende Sicherheitszertifizierung. Zudem sind Smartcards mit unterschiedlichsten Sensoren und Hardwaremechanismen ausgestattet, die zusammen mit dem Smartcard Betriebssystem insbesondere sogenannte Seitenkanalattacken effektiv abwehren. Softwarelösungen verfügen über keinen ausreichenden Schutz vor Seitenkanalattacken, da sie aus technischen Gründen keine zur Smartcard Technologie vergleichbaren Mechanismen bereitstellen können.

Smartcard-Token sind im Gegensatz zu reinen Softwarelösungen nicht kopierbar, können funktionstechnisch nicht manipuliert oder „reverse engineered“ werden und ermöglichen eine gesicherte, mehrstufige Identifikation durch Kombination von Wissen (z.B. Passwort) und Besitz des Token. Zudem kann die Sicherheit des Smartcard-Token durch eine anerkannte Prüfstelle nach Common Criteria evaluiert und anschließend zertifiziert werden.

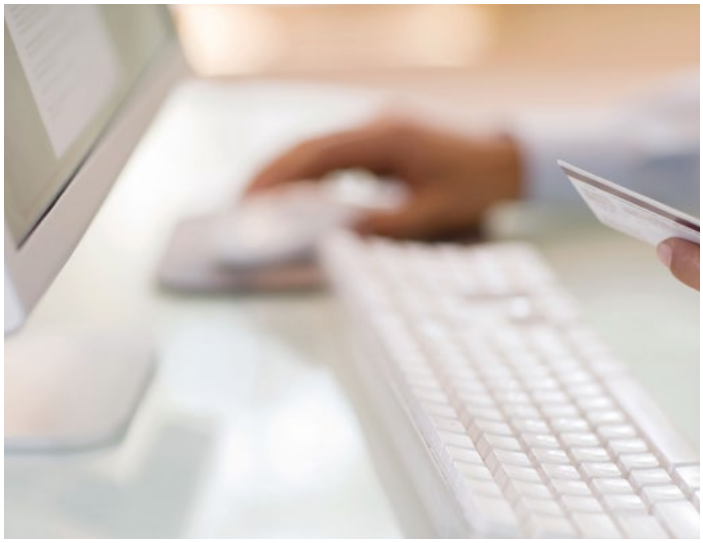
Smartcards unterstützen die gesicherte und performante Durchführung kryptographischer Operationen.

Für kryptographische Operationen verfügen Smartcards über spezielle kryptographische Coprozessoren.

Smartcards ermöglichen Prozessvereinfachungen.

Aufgrund der sicheren Speicherung von Schlüsselmaterial und z.B. patentierter Lösungen zum gesicherten Versand ermöglichen Smartcard-Token einen vereinfachten Roll-Out-Prozess. Darüber hinaus ist es möglich, die eindeutige Identifizierung von IT-Komponenten und deren Kopier- und Plagiatsschutz mittels Smartcard-Token zu realisieren. Da auch kleine Software- oder Datenmanipulationen, die keinen weitreichenden Schaden hervorrufen müssen, das Vertrauen in Komponenten oder eine IT-Gesamtlösung zerstören können, kann durch Smartcard-Token die Akzeptanz eines Produktes oder einer gesamten IT-Lösung deutlich erhöht werden.

ABB. 6. Beispiel Smartcard von T-Systems



EXKURS: SEITENKANALATTACKE

Die Seitenkanalattacke bezeichnet eine kryptoanalytische Methode, die die physische Implementierung eines Kryptosystems in einem Gerät (z.B. einer Chipkarte, eines Security-Tokens oder eines Hardware-Sicherheitsmoduls) oder in einer Software ausnutzt. Dabei wird nicht das kryptographische Verfahren selbst, sondern nur eine bestimmte Implementierung angegriffen, d.h. andere Implementierungen können von dem Angriff unberührt bleiben.

Das Prinzip beruht darauf, ein kryptographisches Gerät bei der Ausführung der kryptologischen Algorithmen zu beobachten und Korrelationen zwischen den beobachteten Daten und dem verwendeten Schlüssel zu finden. Diese charakteristische Information kann durch die Analyse der Laufzeit des Algorithmus, des Energieverbrauchs des Prozessors während der Berechnungen oder der elektromagnetischen Ausstrahlung gewonnen werden. Aktive, invasive Angriffe bestehen darin, in das Gerät einzugreifen und Fehler bei der Ausführung des kryptographischen Algorithmus zu provozieren.

TCOS – HOCHSICHERES SMARTCARD-BETRIEBSSYSTEM – MADE IN GERMANY

Wie bereits dargestellt sind auf Smartcards basierende Hardware-Sicherheits-Token mit einem sicheren Betriebssystem, einer Art „Chipkartengehirn“ ausgestattet, das eine sichere Verwahrung der Schlüssel ermöglicht und die erforderlichen kryptographischen Algorithmen bereitstellt. Das „Chipkartengehirn“ TeleSec Chipcard Operating System – kurz TCOS ist eines davon.

Mehr als 100 Millionen Reisepässe, Personal- und Unternehmensausweise, digitale Tachografen oder elektronische Tickets sind inzwischen in Europa mit dem hochsicheren Betriebssystem der Telekom ausgestattet. Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dabei eine Vielzahl von Lösungen nach dem international anerkannten Verfahren „Common Criteria“ zertifiziert.

Beispiel Reisepass: Das Smartcard-Betriebssystem TCOS ist aufgrund der Zertifizierung eines der sichersten Systeme für internationale Reisedokumente. Die auf dem Chip des Passes gespeicherten digitalen Daten sind durch mehrere Sicherheitsmechanismen geschützt. Schutz vor dem unerlaubten Mitlesen der Daten über eine kontaktlose Schnittstelle bietet ein spezieller Mechanismus, das sogenannte PACE-Protokoll. Auf dem Chip des Reisepasses sind unter anderem das Passfoto sowie Fingerabdrücke gespeichert. Das Betriebssystem organisiert die Verschlüsselung, die Signaturberechnung, die Authentifikation gegenüber den Lesegeräten und das sichere Auslesen der persönlichen Daten für berechtigte Personen und schützt diese vor unerlaubtem Zugriff.

TCOS wird aber auch noch in einer Vielzahl weiterer Anwendungen eingesetzt. So unterstützt die TCOS Signature Card sowohl die fortgeschrittene als auch die qualifizierte elektronische Signatur gemäß Signaturgesetz. Die Sicherheitsmodule in den Terminals des deutschen ÖPV-Systems basieren genauso auf TCOS wie die Tachographenkarten in LKWs, die sichere TETRA-Kommunikation im Behördenfunk stützt sich auf die Sicherheitsmechanismen von TCOS, welches z.B. auch bei der neuen Gesundheitskarte zum Einsatz kommt. Ein weiteres großes Einsatzgebiet sind multifunktionale Unternehmensausweise, die Zutritt, Gleitzeiterfassung, das Bezahlen in Kantinen oder die Ansteuerung von Multifunktionsdruckern unterstützen.

Prinzipiell können Hardware-Sicherheits-Token mit TCOS-Betriebssystem in verschiedenen Bauformen bzw. Formfaktoren ausgeliefert werden. Der wohl bekannteste Formfaktor ist dabei die klassische Chipkarte mit TCOS-Chip, der je nach Anforderung kontaktlos oder kontaktbehaftet adressiert werden kann. Ferner werden Token mit TCOS-Betriebssystem als MicroSD-Smartcard z.B. für mobile Endgeräte, als Schlüsselanhänger mit Bluetooth-Unterstützung, als USB-Stick oder als Embedded Sicherheitsmodul geliefert, das in Geräte, Maschinen oder Fahrzeuge integriert werden kann.

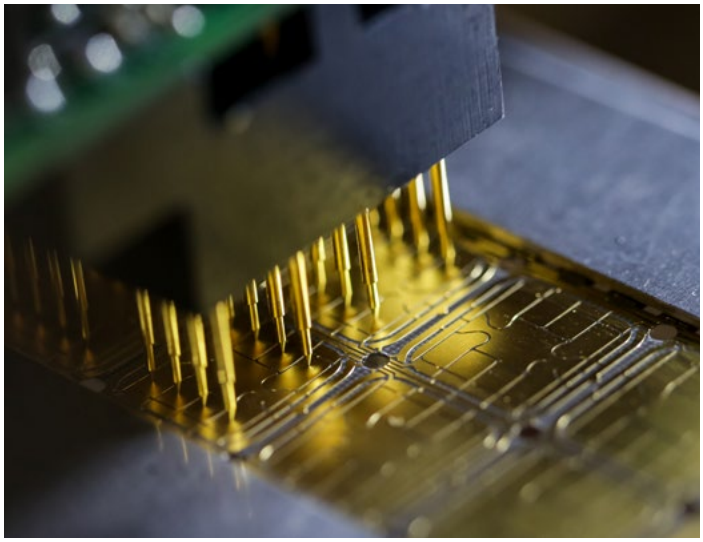


ABB. 7. Security Smartcard Chipmodule von der Rolle mit TCOS als Betriebssystem von T-Systems

T-Systems kooperiert seit Jahren mit Chipherstellern im Markt für sichere, elektronische Ausweise. Die Kombination aus TCOS und Sicherheitschip ist mit Blick auf deutsche und internationale Anforderungen für elektronische Dokumente zur Identifikation konzipiert. Mit verschiedenen Chipherstellern prüft T-Systems fortlaufend den Einsatz neuer Smartcard-Technologien sowie neue Anwendungsfelder. Neue Einsatzbereiche sind beispielsweise Mobile Security, die Weiterentwicklung der multifunktionalen ID-Karten in Unternehmen, elektronische Führerscheine (European Driver License), die Sicherheit für Daten aus intelligenten Stromzählern (Smart Meter) sowie Sicherheitslösungen im Bereich Automotive, Gesundheitswesen oder Industrie 4.0.

TCOS-IDKEY-TOKEN – SECURE IDENTIFICATION – MADE IN GERMANY

Der TCOS-IDKey-Token wurde speziell für Anwendungen zur Identifizierung mit Hilfe verschiedener Identifizierungsmerkmale und zur Authentifizierung mittels symmetrischer und asymmetrischer Schlüssel oder Einmalpasswörtern entwickelt.

Er ist als klassische Chipkarte, MicroSD-Smartcard oder Embedded Modul lieferbar und kann kontaktlos, kontaktbehaftet oder über I²C genutzt werden.

Der TCOS-IDKey-Token wird als nicht personifizierter Kryptochip mit dem T-Systems-eigenen Betriebssystem TCOS 3.0 (TeleSec Chipcard Operating System) ausgeliefert. Seine Anwendungen sind dabei speziell auf die Verwendung im Windows-Umfeld optimiert.

Zur Realisierung gesicherter Identitäten werden im Herstellungsprozess private Schlüssel aus dem Trust Center der Deutschen Telekom AG auf dem Token abgelegt. Diese wurden zuvor in einem hochsicheren Schlüsselgenerator als Unikate erzeugt und gesichert und nach aktuellem Stand der Technik nicht auslesbar auf dem Token gespeichert. Die Qualität der asymmetrischen Schlüssel wird durch ein Gütesiegel des Trust Centers nachgewiesen.

Die kryptographischen Schlüssel, von denen keine Kopien existieren, sind in Verbindung mit den jeweiligen physikalischen Kartennummern eindeutig und können als Basis für verschiedene digitale Identitäten genutzt werden.

Die Schlüssel innerhalb des Chips des TCOS-IDKey-Token können nur dann verwendet werden, wenn dem Token gegenüber das gültige Passwort – im üblichen Sprachgebrauch die PIN – präsentiert wurde. In Kombination mit den zugehörigen Zertifikaten über die öffentlichen Schlüssel ermöglicht die kryptografische Anwendung der privaten Schlüssel die eindeutige Zuordnung von Aktionen zu einer Person oder einem System.

IDKey enthält bei Auslieferung verschiedene asymmetrische Schlüsselpaare mit zugehörigem Herkunftsnachweis aus der Trust Center-Produktion der T-Systems.

IDKey unterstützt das Windows Life Cycle Management (ILM) und kann unter Windows für folgende Anwendungsfelder genutzt werden:

- Zugangsberechtigungen zu Personal Computern
- Authentifizierung gegenüber Servern, Netzen oder Cloud Diensten
- Integritätssicherung
- Sichere E-Mail Kommunikation (Ver- und Entschlüsselung/Signatur)
- Ver- und Entschlüsselung beliebiger Dateien

Zudem verfügt der IDKey-Token über weitere Anwendungen wie eine Zutrittsapplikation (TCOS myAccess), eine OTP-Anwendung oder eine Anwendung zur Realisierung von Gleitzeitkonten.

IDKey wird im sogenannten Null-PIN-Status ausgeliefert. Die Null-PIN sichert die Unversehrtheit des Produkts und erspart den Versand von PIN-Briefen. Vor einer Nutzung von IDKey muss die Null-PIN durch eine persönliche PIN ersetzt werden. Eine Zuordnung zu bestimmten Personen oder Systemen (Personalisierung) wird nach Auslieferung im Kundenumfeld vorgenommen.

TCOS MYACCESS+ – SECURE IDENTITY PROVISIONING „OVER THE AIR“

TCOS MyAccess+ ist eine Weiterentwicklung der auf dem IDKey-Token vorhandenen MyAccess-Applikation. TCOS myAccess+ kann über eine Webanwendung auf verschiedene JAVA-basierte Token provisioniert werden.

Zur Einrichtung der MyAccess-Lösung auf einem Smartphone oder einem anderen Token gibt es verschiedene Möglichkeiten.

Der Nutzer kann die MyAccess-Lösung direkt in einem Portal oder in einem Onlineshop bestellen. Hierbei muss er die Telefonnummer sowie die SIM-Karten-ID bzw. die Token-ID hinterlegen. Ferner ist es möglich, dass Unternehmen Sammelbestellungen für verschiedene Endnutzer in die Wege leiten. Die Angabe der SIM-Karten- bzw. der Token-IDs dient dazu, Daten individuell für das jeweilige Token bereitstellen zu können. Dies gewährleistet die Eindeutigkeit jedes Token und verhindert ein Klonen von Daten und damit von Identitäten.

Nach der Bestellung werden die Daten einer Plausibilitätsprüfung sowie einer Formatprüfung unterzogen. Ferner überprüft T-Systems die Rechtmäßigkeit der Bestellung sowie der geforderten Accessrechte. Sind alle Daten korrekt, so generiert der Smartcard Service die entsprechenden Daten für den Access und ruft das erforderliche Schlüsselmaterial auf gesichertem und vor unberechtigten Zugriffen geschütztem Weg aus dem Trust Center der DTAG ab. Anschließend stellt er daraus den individuell für den jeweiligen Token bzw. die SIM-Karte verschlüsselten Datensatz zur Provisionierung der MyAccess-Lösung zusammen.

Im Fall der SIM-Karten-Provisionierung wird der fertige Datensatz sowie das jeweils aktuelle Applet über den Service Provider Trusted Service Manager (SP-TSM) „Over-the-Air“ an die SIM-Karte des jeweiligen Mobile Network Operators (MNO) bzw. dessen Endnutzer übertragen. Das Applet kann dann über die Mobile-Wallet des Smartphones administriert werden. Bei der Übermittlung des Applets kommen ein IPSEC-Tunnel sowie Verfahren nach dem Global Platform Standard zum Einsatz.

Im Fall der Provisionierung auf andere Token kann der Nutzer die individuell für seinen Token konfektionierten Daten an einer Webschnittstelle abrufen und selbst in sein zugehöriges Token einbringen. Alternativ ist es möglich, eine IP-Adresse anzugeben, über die das jeweilige Token erreicht werden kann.

ABB. 8. Einsatz von TCOS-Chips

AKTUELLE ANWENDUNGEN MIT ZWEI-FAKTOR-AUTHENTIFIZIERUNG

E-PASS
Der elektronische Reisepass ist mit einem Radio-Frequency (RF)-Chip ausgestattet. Bei diesem RF-Chip handelt es sich um einen zertifizierten Sicherheitschip mit kryptographischem Coprozessor, auf dem neben den bisher üblichen Passdaten auch biometrische Merkmale gespeichert werden. Der Chip mit TCOS Betriebssystem ist eine Hürde für Fälscher. Die biometrischen Merkmale im Chip können maschinell geprüft werden. Damit ist eindeutig feststellbar, ob Pass und Person wirklich zusammengehören. Die Mechanismen des Zugriffschutzes stellen sicher, dass ein unautorisiertes Auslesen der Daten aus dem RF-Chip sowie ein Belauschen der Kommunikation unterbunden werden.

NEUER PERSONALAUSWEIS NPA
Klassische Sicherheits-Token tragen schon heute viele Nutzer in Form von mehr als 100 Millionen Reisepässen (e-Pass) sowie Personal- und Unternehmensausweisen mit sich. Sie vertrauen dabei ihre persönlichen Daten einem der laut Bundesamt für Sicherheit in der Informationstechnik (BSI) sichersten Betriebssysteme an, TCOS.

Auch der neue Personalausweis kann für ein Zwei-Wege-Verfahren verwendet werden. Anbieter können sich beim Bundesverwaltungsamt anmelden und werden gegebenenfalls berechtigt, den Ausweis als „zweiten Faktor“ nutzen zu dürfen. Er kann dann mit einem Kartenlesegerät und passender Software verwendet werden.

E-TICKET / VERBAND DEUTSCHER VERKEHRSUNTERNEHMEN E.V.
Zu den wichtigsten Projekten des VDV gehört die bundesweite Einführung der elektronischen Fahrkarte (eTicket) für den ÖPV. Hierfür entwickelte die VDV eTicket Service GmbH & Co. KG (VDV eTS) zusammen mit Industriepartnern die „VDV-Kernapplikation“, die Fahrgästen einen bequemen, bargeldlosen Kartenkauf und den Verkehrsverbünden eine vereinfachte Abrechnung ermöglicht. Unverzichtbar für den Erfolg eines solchen Systems war ein umfassendes Sicherheitsmanagement, für das T-Systems verantwortlich ist. Dazu gehörte auch die Ausstellung von Zertifikaten für die Tickets im sicheren Trust Center sowie die Entwicklung und Lieferung von auf TCOS basierenden Sicherheitsmodulen (sogenannten Secure Application Modules oder auch SAMs) für die Kundenterminals, die T-Systems seit 2006 stetig weiterentwickelt und zur Verfügung stellt.

Mithilfe der SAMs lässt sich die VDV-Kernapplikation kryptographisch sicher betreiben und eine Kundenabrechnung fälschungssicher erstellen. Durch Nutzung von Zertifikaten lassen sich die Tickets fälschungssicher ausstellen und kontrollieren. Einheitliche Schnittstellenspezifikationen sorgen dafür, dass alle Systemkomponenten interoperabel sind. So realisierte T-Systems für die VDV eTS ein sicheres und performantes Sicherheitsmanagement, bestehend aus der Public-Key-Infrastruktur (PKI), dem Keymanagement (KM) und den Secure Application Modules (SAM).

DE-MAIL
Im Gegensatz zur E-Mail können bei De-Mail sowohl die Identität der Kommunikationspartner als auch der Versand und der Eingang von De-Mails jederzeit zweifelsfrei nachgewiesen werden. Die Inhalte einer De-Mail können auf ihrem Weg durch das Internet nicht mitgelesen oder gar verändert werden. Denn abgesicherte Anmeldeverfahren und Verbindungen zu den De-Mail-Anbietern sorgen ebenso wie verschlüsselte Transportwege zwischen den De-Mail-Anbietern für einen vertraulichen Versand und Empfang von De-Mails. De-Mail erhöht so die Sicherheit der elektronischen Kommunikation im Vergleich zur herkömmlichen E-Mail.

Für die Nutzung von De-Mail benötigen Personen ein De-Mail-Konto und die dazu gehörende De-Mail-Adresse. Für die De-Mail-Adresse registriert sich ein Nutzer bei einem De-Mail-Anbieter. Nach der Registrierung erfolgt eine Überprüfung der Identität anhand eines Personalausweises oder Reisepasses. Darüber hinaus kann der De-Mail-Anbieter auch eine Identifizierung anhand der Online-Ausweisfunktion (eID-Funktion) im neuen Personalausweis (nPA) anbieten.

Um eine De-Mail zu versenden oder eine empfangene De-Mail zu lesen, meldet sich der Nutzer am De-Mail-Konto an. Soll das Sicherheitsniveau „hoch" sein, kommt ein Token zum Einsatz. Diese Zwei-Faktor-Authentifizierung erfolgt je nach Anbieter mit verschiedenen Mitteln:

- Chipkarte mit eID-Funktion, z.B. der neue Personalausweis oder eine Signaturkarte
- USB-Gerät in der Größe eines Speicher-Sticks, das eine mit PIN oder Passwort geschützte Authentifizierungsfunktion enthält
- One-Time-Password-Generator (OTP, Einmalpasswortverfahren), mit dem der Nutzer bei Bedarf ein Passwort anfordert, das er nur für eine Anmeldung nutzen kann

Die Deutsche Telekom ist De-Mail-Anbieter und hat mit T-Systems das Sicherheitsmanagement für verschiedene De-Mail-Anbieter konzipiert und aufgebaut.

DEUTSCHE TELEKOM: MYCARD

Die Deutsche Telekom setzt einen TCOS-Token als Digitale Identität für alle Mitarbeiter ein. Sie nutzen die MyCard für die Anmeldung am Arbeitsplatz, das Signieren und Verschlüsseln von E-Mails und Dateien, das Drucken an Multifunktionsdruckern, das bargeldlose Bezahlen – z.B. in der Kantine sowie für den Gebäudezugang. Die MyCard wird dabei als klassische Chipkarte kontaktlos oder kontaktbehaftet, als MicroSD-Smartcard und als Schlüsselanhänger eingesetzt, der über Bluetooth kontaktiert werden kann.

ABBILDUNGSVERZEICHNIS

KONTAKT

Marketing
T-Systems International GmbH
Uli Kunesch
Market Intelligence
Fasanenweg 5
70771 Leinfelden-Echterdingen
Uli.Kunesch@t-systems.com

Fachbereich
T-Systems International GmbH
Dr. Friedrich Tönsing
Security Engineering & Solutions
Deutsche-Telekom-Allee 7
64295 Darmstadt
Friedrich.Toensing@t-systems.com

HERAUSGEBER

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main

http://www.t-systems.de

Stand: Februar 2015

T · · Systems ·