TCOS-SMARTCARD-TOKEN

High-End-Security für Ihre digitale Identität

T · · Systems ·

HINTERGRUND

Der Einsatz moderner Informations- und Kommunikationstechnologien ermöglicht eine Vielzahl von Prozessoptimierungen in weiten Teilen des gesellschaftlichen und geschäftlichen Zusammenlebens. Dies bietet heute nun die Möglichkeit der Fernabwicklung von Transaktionen, die bisherig ein Zusammentreffen der Geschäftspartner erforderten. Und zu der Notwendigkeit eines sicheren Vertrauensverhältnisses zwischen den Kommunikationspartnern, welches ohne den persönlichen Kontakt über eine eindeutige Identifizierung realisiert werden muss.

Vor dem Hintergrund der Datenmissbrauchsskandale der letzten Jahre und der Abhörpraxis diverser Geheimdienste nimmt der Wunsch nach mehr Datensicherheit und der Möglichkeit zur verlässlichen Identifizierung von Personen aber auch Institutionen und Servicedienstleistern immer weiter zu. Dabei ist eine Vor-Ort-Prüfung der Identität z. B. mittels Abgleich gegenüber einem Personalausweis aufgrund der räumlichen Trennung meist nicht möglich, so dass neue Lösungen zum Identitätsnachweis zu etablieren sind.

Laut einer Studie der Bitkom[1] legten bereits im Jahr 2012 rund 82 % der Internetnutzer Daten in Cloudspeichern und davon die Mehrzahl in sozialen Netzwerken ab. Gleichzeitig hatten jedoch auch 45 % der Internetnutzer Angst vor dem Ausspähen ihrer Daten, 75 % fühlten sich insgesamt bedroht, 62 % hatten Angst vor Infektion ihres Rechners mit Viren und Trojanern und 26 % der Personen, die Clouddienste nicht nutzen wollten, begründeten ihre ablehnende Haltung mit der Angst vor Datenmissbrauch. Neben den Privatanwendern sehen nach der gleichen Studie 57 % aller Unternehmen eine reale Gefahr in Angriffen auf ihre IT-Systeme. Aufgrund der immer professionalisierteren Technik von Betrügern zum Identitätsdiebstahl (Phishing, Pharming) und zum Ausspähen privater Daten besteht ein stetig größer werdender Bedarf an neuen Sicherheitslösungen, die den Identitätsdiebstahl verhindern und eine Möglichkeit schaffen, bisher unsichere und nur wenig vor Manipulation und Datendiebstahl geschützte Security-Credentials wie Schlüssel und Passwörter auf einem von Viren, Trojanern und weiteren Angriffen geschützten Speichermedium abzulegen.

In den folgenden Abschnitten werden Lösungen zur sicheren Identifizierung sowie zur gesicherten Übermittlung vertraulicher Daten vorgestellt.

ERSTELLUNG DIGITALER IDENTITÄTEN

In den letzten Jahren haben sich weltweit einheitliche Verfahren etabliert, um digitale Identitäten z. B. in Form von Zertifikaten zu erzeugen und zu verwalten. 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) – mittels elektronischer Signatur besiegelt wird.

International existieren verschiedene Zertifizierungsstellen, die die Glaubwürdigkeit solcher Zertifikate in einem sicheren, vor äußeren Einflüssen abgeschirmten Bereich, dem sogenannten Trust Center, sicherstellen. Um die Serviceleistung des Trust Centers nutzen zu können und ein Zertifikat zu erhalten, muss ein Teilnehmer einer solchen Public Key Infrastruktur (PKI) seine Identität einmalig entweder gegenüber dem Trust Center selbst oder gegenüber einer anerkannten Registrierungsstelle mittels eines physikalischen Ausweisdokuments persönlich nachweisen. Hierdurch wird sichergestellt, dass nur vertrauenswürdige und der Registrierungsstelle bekannte Personen am System teilnehmen. Der Nachweis einer Identität kann heutzutage auch mit Hilfe des neuen Personalausweises auf elektronische Art und Weise erbracht werden. So können beispielsweise abgeleitete Identitäten mit Hilfe des neuen Personalausweises erstellt werden, die dann für einen bestimmten Zeitraum gültig sind: eine sogenannte temporär abgeleitete digitale Identität.

Das der gegenseitigen Identifizierung zu Grunde liegende Prinzip basiert zumeist auf asymmetrischer Kryptographie. Hierbei werden für alle Beteiligte Schlüsselpaare aus privatem und öffentlichem Schlüssel erzeugt. Der öffentliche Schlüssel wird zusammen mit den auf Echtheit geprüften Identifikationsmerkmalen des Teilnehmers, in ein Zertifikat eingebunden. Dieses Zertifikat wird von der Zertifizierungsstelle signiert und kann als digitale Identität des Teilnehmers genutzt werden. Durch die Signatur der Zertifizierungsstelle kann sichergestellt werden, dass zum einen der Schlüssel in einer vertrauenswürdigen Umgebung erzeugt und sicher gespeichert ist und zum anderen den Identitätsmerkmalen im Zertifikat vertraut werden kann. Damit ist die Basis für ein „elektronisches Vertrauensverhältnis“ geschaffen. Diese Zertifikate können an alle Teilnehmer der PKI weiter gegeben oder in Verzeichnissen veröffentlicht werden.

1 Studie „Vertrauen und Sicherheit im Netz“, Bitkom 2012

NUTZUNG DIGITALER IDENTITÄTEN

Der Sender einer Nachricht nutzt beispielsweise seinen privaten Schlüssel, um eine Nachricht mit einer digitalen Signatur zu versehen. Der Empfänger kann anhand des Zertifikats des Senders die Gültigkeit der digitalen Signatur prüfen. Weiterhin ist es möglich, vertrauliche Nachrichten zu versenden. Der Sender sucht sich das Zertifikat des Empfängers aus einem Verzeichnis und verschlüsselt die Nachricht mit dem darin enthaltenen öffentlichen Schlüssel des Empfängers. Die Entschlüsselung der Nachricht kann nur der Empfänger vornehmen, da nur er den zugehörigen privaten Schlüssel besitzt und nutzen kann.

Auf diese Weise kann der Teilnehmer auch Dokumente für sich selbst verschlüsselt ablegen. Damit ist sichergestellt, dass nur der Teilnehmer selbst die Daten entschlüsseln und kein anderer die Daten einsehen kann. Dies könnte interessant sein, wenn beispielsweise Daten in der Cloud gespeichert werden. Auch bei der Anmeldung an Portalen könnte der Teilnehmer die digitale Identität zur Authentifizierung nutzen.

DIE SICHERHEIT EINER DIGITALEN IDENTITÄT

Die digitale Identität basiert auf einem Schlüsselpaar, das aus einem öffentlichen und privaten Schlüssel besteht. Wenn der private Schlüssel jedoch nicht geheim gehalten wird, dann ist ein Missbrauch der digitalen Identität nicht ausgeschlossen. Ein Angreifer könnte die Identität eines anderen Teilnehmers nutzen. Damit nur der rechtmäßige Teilnehmer seine Identität nutzen kann, muss ein besonderes Augenmerk darauf gelegt werden, wie der private Schlüssel aufbewahrt und vor Missbrauch geschützt wird. 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.

Zur sicheren Speicherung der privaten Schlüssel und zur gleichzeitigen Erreichung eines hinreichend hohen Sicherheitsniveaus haben sich Hardware-Sicherheitslösungen etabliert. Diese basieren auf hochsicheren Smartcard-Chips und werden als Hardware-Sicherheitsmodule, Security-Token oder Smartcard-Token bezeichnet. Es gibt sie in unterschiedlichen Formfaktoren und Ausprägungen, die einfach in bestehende Lösungen integriert werden können und einen hohen Schutz vor den im Netz lauernden Gefahren bieten. Solche Smartcard-Chips werden heute beispielsweise im elektronische Reisepass, dem neuen Personalausweis, der Gesundheits- oder der Geldkarte verwendet.

SMARTCARD-TOKEN: HARDWARE + SOFTWARE = SICHERHEIT

In komplexen IT-Systemen gibt es noch weitere Gründe für den Einsatz von Smartcard-Token. Smartcard-Token ermöglichen die gesicherte Ablage von Passwörtern und Schlüsselmaterial. Ohne ihren Einsatz kann die Geheimhaltung dieser Credentials und damit der Datenschutz sowie die Integrität und Authentizität von elektronisch ausgelesenen oder übermittelten Daten nicht gewährleistet werden. Softwarelösungen verfügen über keinen ausreichenden Schutz vor sogenannten Seitenkanalattacken, da Softwarelösungen über keine zur Smartcard Technologie vergleichbaren Mechanismen verfügen. Die Seitenkanalattacke[2] (englisch side channel attack) wurde 1996 durch den Kryptologen Paul C. Kocher bekannt gemacht und 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 kryptologischen Algorithmus zu provozieren. Geeignete Smartcards verfügen heutzutage zum einen über ein sicheres Smartcard Betriebssystem, das verschiedenste kryptographische Funktionen bereitstellt, die sichere Datenspeicherung und Datennutzung gewährleisten und meist eine entsprechende Sicherheitszertifizierung bietet und zum anderen mit unterschiedlichsten Sensoren und Hardwaremechanismen ausgestattet sind, die zusammen mit dem Smartcard Betriebssystem insbesondere Seitenkanalattacken effektiv abwehren.

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 zertifiziert werden.

Smartcard-Token unterstützen die gesicherte und performante Durchführung kryptographischer Operationen. Hierzu sind sie mit speziellen kryptographischen Coprozessoren ausgestattet. 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.

2 http://de.wikipedia.org/wiki/Seitenkanalattacke

HARDWARE-SICHERHEIT AUF BASIS VON TCOS

Wir tragen es meist in Portemonnaies und Jackentaschen mit uns, setzen es auf Reisen ein oder nutzen es für das Einchecken in den Büro-PC. Doch kaum jemand weiß, dass er dabei seine persönlichen Daten einem der sichersten Betriebssysteme auf dem IT-Markt anvertraut: TeleSec Chipcard Operating System – kurz TCOS.

Im analogen Leben überprüfen wir häufig, ob eine Person tatsächlich diejenige ist, die sie vorgibt zu sein. In der elektronischen Welt ist dies ungleich schwerer, da eine Person aus der Ferne oder mit einer Maschine agiert, zum Beispiel beim Online- Banking oder –Shopping. Um hier mehr Sicherheit zu erreichen, setzen Unternehmen zunehmend auf digitale Identitäten. Diese digitale Identität repräsentiert eine Person in elektronischen Systemen.

TCOS: EIN HOCHSICHERES SMARTCARDBETRIEBSSYSTEM

Solche digitalen Identitäten erstellt das vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Kartenbetriebssystem TCOS, das für Reisepässe oder Personalausweise nach dem international anerkannten Verfahren „Common Criteria“ geprüft wurde. Das Smartcard-Betriebssystem TCOS ist damit eines der sichersten Systeme für internationale Reisedokumente. Mehr als 100 Millionen Reisepässe, Personal- und Unternehmensausweise, digitale Tachografen oder elektronische Tickets sind inzwischen in Europa mit dem hochsicheren TCOS-Betriebssystem ausgestattet.

TCOS: VERSCHLÜSSELT PERSÖNLICHE DATEN

Die auf dem Telesec Chip gespeicherten digitalen Daten sind durch mehrere Sicherheitsmechanismen geschützt. Schutz vor dem unerlaubten Auslesen der Daten über eine kontaktlose Schnittstelle bietet ein spezieller Mechanismus, das sogenannte PACE-Protokoll. Auf dem Chip in Ausweisdokumenten sind unter anderem das Passfoto sowie Fingerabdrücke gespeichert. Die Telekom Software organisiert die Verschlüsselung, das sichere Auslesen der persönlichen Daten und schützt diese vor unerlaubtem Zugriff. TCOS ist also in der Lage, Schlüssel sicher zu verwahren und den kryptografischen Algorithmus innerhalb des Chips zu berechnen. Einmal sicher eingebrachte Schlüssel müssen die Chipkarte niemals mehr verlassen.

TCOS: ERFÜLLT HÄRTESTE ANFORDERUNGEN

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, ID-Karten in Unternehmen, elektronische Führerscheine (European Driver License), die Sicherheit für Cloud-Lösungen und die Sicherheit für intelligente Netzlösungen bei intelligenten Stromzählern (Smart Meter) sowie Sicherheitslösungen im Bereich Automotive, Gesundheitswesen oder Industrie 4.0.

Smartcard-Token auf Basis des von T-Systems in Deutschland entwickelten Smartcard Betriebssystems TCOS verfügen damit über ein großes Leistungsspektrum für verschiedenste Anwendungen.

TCOS-MYCARD: DER SCHLÜSSEL IM KONZERN DEUTSCHE TELEKOM AG

Im Konzern Deutsche Telekom AG wird die MyCard als digitale Identität des Mitarbeiters genutzt. Die MyCard wird für die Anmeldung am Arbeitsplatz, das Signieren und Verschlüsseln von E-Mails, das Signieren und Verschlüsseln von Dateien, das Drucken an Multifunktionsdruckern, das bargeldlose Bezahlen und zum Gebäudezugang genutzt.

Damit die Integration in verschiedenste Endgeräte ermöglicht wird, steht die MyCard in unterschiedlichen Formfaktoren zur Verfügung:

- Als Smartcard kontaktlos und kontaktbehaftet einsetzbar
- Als MikroSD-Smartcard für mobile Endgeräte geeignet
- Als Smartcard Token für Schlüsselanhänger kontaktlos oder über Bluetooth

TCOS-IDKEY:
DER SCHLÜSSEL ZUR GESICHERTEN IDENTITÄT

Mit dem TCOS-IDKey Token erhält der Anwender besonders hochwertige digitale Schlüssel auf einem Smartcard-Token. Durch diese wird es ihm ermöglicht, sich gegen viele Gefahren des Internets zu schützen und gleichzeitig durch eine eindeutige Identität seine Präsenz in der „virtuellen Welt“ aufzuwerten.

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

Zur Realisierung gesicherter Identitäten werden im Herstellungsprozess private Schlüssel aus dem Trust Center der Deutschen Telekom auf dem Token abgelegt. Diese wurden zuvor in einem hochsichern Schlüsselgenerator als Unikate erzeugt und nach dem gesicherten Aufbringen auf den Token nicht extern gespeichert, d. h. es existieren keine Kopien dieser Schlüssel. Zudem ist es nach dem Stand der Technik unmöglich, die Schlüssel aus dem Smartcard-Token auszulesen. 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.

Der TCOS-IDKey Token ermöglicht darüber hinaus einen vertraulichen Informationsaustausch sowie eine verschlüsselte Datenablage. Alle Daten, die unter Zuhilfenahme öffentlicher Schlüssel eines TCOS-IDKey Token verschlüsselt wurden, lassen sich nur mit den zugehörigen privaten Schlüsseln und damit nur mit passenden Token wieder entschlüsseln. Die Funktionen des TCOS-IDKey Token sind nicht an den Formfaktor des Token gebunden.

Damit die Integration in verschiedenste Endgeräte ermöglicht wird, steht der TCOS-IDKey Token in unterschiedlichen Formen zur Verfügung:

- Als Smartcard kontaktlos und kontaktbehaftet einsetzbar
- Als MikroSD-Smartcard für mobile Endgeräte geeignet
- Als Smartcard Token für Schlüsselanhänger kontaktlos oder über Bluetooth
- Als Embedded Sicherheitsmodul, für die Integration in Geräte, Maschinen, Fahrzeuge o. ä.

High-End-Security – Made in Germany

Sämtliche Smartcard Token der T-Systems basieren auf dem Telesec Chipcard Operating System (TCOS), welches seit vielen Jahren unter ständiger Begleitung durch neutrale Sicherheits-Evaluatoren entwickelt und gepflegt wird. So bildet TCOS unter Anderem die Basis für die qualifizierten Signaturkarten der Deutschen Telekom AG. Ferner wird das Betriebssystem auch im elektronischen Reisepass, dem neuen deutschen Personalausweis, in Sicherheitsmodulen für eTicketing-Terminals oder zur gesicherten Sprachkommunikation eingesetzt.

Seit Mitte der 1990er Jahre beliefert T-Systems Security Consulting & Engineering Kunden weltweit mit Smartcard Produkten und Smartcard Lösungen auf Basis des im eigenen Hause entwickelten Smartcard Betriebssystems TCOS, das in verschiedenen Produkten den hohen Evaluierungs- und Zertifizierungsanforderungen der Common Criteria genügt und auf zertifizierte Smartcard Chips aufsetzt. Zu den Produkten zählen dabei insbesondere der in vielen Ländern eingesetzte TCOS Passport, die TCOS Identity Card im neuen Personalausweis in Deutschland, die TCOS Signature Card, Sicherheitsmodule für die eTicketing-Terminals des Verbandes Deutscher Verkehrsunternehmen, TCOS Module zur gesicherten Sprachkommunikation, im Mautumfeld, im digitalen Fahrtenschreiber oder im Gesundheitswesen. Darüber hinaus werden Beratungsleistungen zu Security Produkten sowie PKI-Dienstleistungen des Trust Centers der Deutschen Telekom AG angeboten.

KONTAKT
T-Systems International GmbH
Security Engineering & Solutions
Dr. Friedrich Tönsing
Deutsche-Telekom-Allee 7
64295 Darmstadt
Tel.: +49 6151 58-37663
E-Mail: Friedrich.Toensing@t-systems.com
Internet: www.t-systems.com/security

HERAUSGEBER
T-Systems International GmbH
Hahnstraße 43 d
60528 Frankfurt
Deutschland