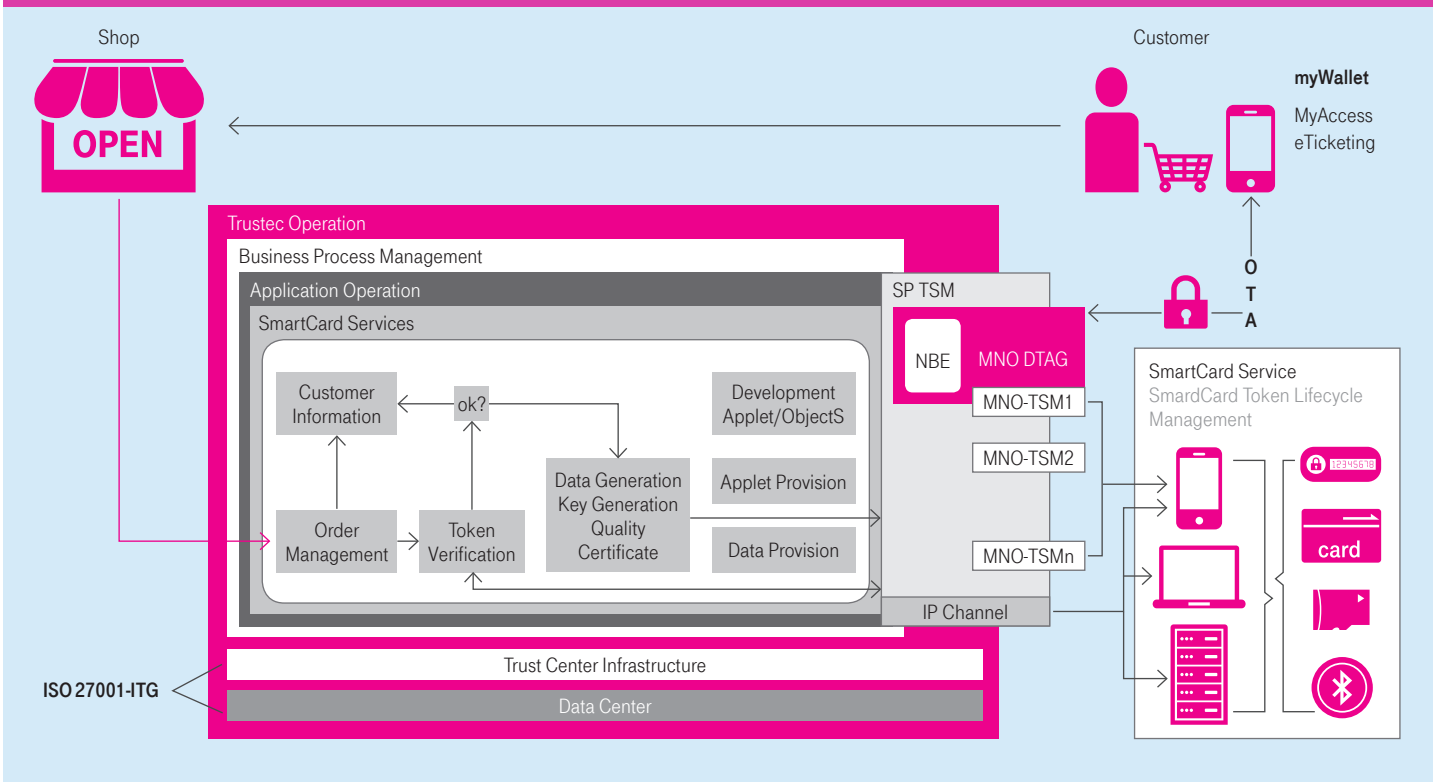
TCOS SMART CARD SERVICE
SICHERE ONLINE-PROVISIONIERUNG VON SMARTCARD-ANWENDUNGEN AM BEISPIEL MYACCESS

Flexible High-End Security – Made in Germany



Wir kennen es alle: Das Portemonnaie quillt über vor sicheren Kreditkarten, EC-Karten und Zutrittskontrollkarten und weniger sicheren Vanity-Karten zum vergünstigten Einkaufen, Mitgliedsausweisen und ähnlichen Plastikkarten im Checkkartenformat. Zudem ist genau die Karte, die wir gerade zu diesem Zeitpunkt nutzen wollen, nicht auffindbar oder zufälligerweise auf dem heimischen Schreibtisch liegen geblieben. Neben dem überfüllten Portemonnaie führen wir gleichzeitig ein kaum kleineres Smartphone mit uns herum, das wir in der Regel nicht vergessen, das wir nur zum Telefonieren, SMS-senden und Surfen im Internet nutzen und das im Normalfall immer betriebsbereit ist. Was spräche dagegen, dieses Smartphone auch für Smartcard-Anwendungen einzusetzen, um dem Dschungel an Karten zu begegnen und die jeweils nötige Applikation direkt verfügbar zu haben?

Nach einer repräsentativen Studie der Bitkom aus dem Jahr 2011[1] besitzen rund 83 % der deutschen Bevölkerung ein Mobiltelefon, das regelmäßig mitgeführt wird. Dieses Mobiltelefon wird i.d.R. jedoch nur zum Telefonieren und SMS-senden und bei einem weitaus geringeren Teil der Bevölkerung (11 %) auch für Applikationen (Apps) genutzt.

Wenn es gelingt, die Welt der Chipkarten mit der Welt der Mobiltelefone ohne Abstriche an der Sicherheit zusammen zu führen oder Smartcards in anderen Formfaktoren zu liefern und die entsprechenden Kartenanwendungen von Ferne zu provisionieren, so öffnet dies ein neues Feld hochflexibler mobiler Anwendungen für Privatpersonen und Geschäftskunden.

1 Vgl. Studie „Netzgesellschaft“

T · · Systems ·

TCOS SMART CARD SERVICE FÜR ZUTRITTSMANAGEMENT

Mit dem TCOS Smartcard Service bietet T-Systems eine Lösung zum gesicherten Aufbringen von Smartcard-Anwendungen auf verschiedene Token sowie auf SIM-Karten NFC-fähiger Mobiltelefone. Im Folgenden soll eine solche Provisionierung anhand von MyAccess zum sicheren Gebäude-Zutritt dargestellt werden.

TCOS MYACCESS: FÜR MYCARD UND IDKEY-KARTE

Im Konzern Deutsche Telekom AG wird die so genannte MyCard als digitale Identität des Mitarbeiters genutzt. Diese Karte wird für die Anmeldung am Arbeitsplatz, für das Signieren und Verschlüsseln von Emails und Dateien, für das Drucken an Multifunktionsdruckern und für bargeldloses Bezahlen genutzt. Das Produkt MyAcess ist dabei eine Applikation der MyCard und wird zur Realisierung des Zugangs zu Gebäuden des Konzerns verwendet. Durch MyAccess ist es möglich, den Mitarbeitern des Konzerns befristeten Zugang zu bestimmten Gebäuden und Gebäudeteilen zu ermöglichen, ohne hierfür physikalisch neue Schlüssel oder Chipkarten verteilen und deren Ausgabe verwalten zu müssen. Die kartenindividuellen Schlüssel der MyCard werden für den Zweck der Zutrittsberechtigung im System hinterlegt und verwaltet. Die MyAccess-Applikation steht nicht nur Nutzern der MyCard zur Verfügung. Sie ist ebenso Bestandteil der IDKey-Karte, die sich bei zahlreichen Kunden der Deutschen Telekom AG im Einsatz befindet.

TCOS MYACCESS+: FÜR VERSCHIEDENE TOKEN

TCOS MyAccess+ ist eine Weiterentwicklung von TCOS-MyAccess auf der MyCard oder der IDKey-Karte. Es handelt sich hierbei um die MyAccess-Anwendung, die über eine Webanwendung auf verschiedene Token provisioniert werden kann. Zur Einrichtung der MyAccess-Lösung auf einem Smartphone oder einem anderen Token gibt es verschiedene Möglichkeiten.

PORTALBESTELLUNG

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

Nach der Bestellung werden die Daten im Auftragsmanagement der T-Systems einer Plausibilitätsprüfung sowie einer Formatprüfung unterzogen. Ferner prüft 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, ruft das erforderliche Schlüsselmaterial auf gesichertem und vor unberechtigten Zugriffen geschütztem Weg aus dem Trustcenter der DTAG ab und stellt daraus den individuell für den jeweiligen Token bzw. die SIM-Karte verschlüsselten Datensatz zur Provisionierung der MyAccess-Lösung zusammen.

APPLET-ÜBERTRAGUNG

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 Operator (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, oder eine IP-Adresse angeben, über die das jeweilige Token erreicht werden kann. Im Rahmen des Prozesses wird laufend über den jeweiligen Status der Beauftragung informiert.

FAZIT

Der gesamte Lebenszyklus der MyAccess-Anwendung wird vom Smart Card Service überwacht und koordiniert. Dies ermöglicht es nicht nur dauerhafte, sondern auch temporäre Identitäten zu vergeben, die z. B. für einen einmaligen Zugang eines Gastes oder eine bestimmte Nutzungsdauer geeignet sind.

NOCH FRAGEN?
www.t-systems.com/security oder
schreiben Sie einfach an
friedrich.toensing@t-systems.com

KONTAKT
T-Systems International GmbH
Security Engineering & Solutions
Dr. Friedrich Tönsing
Deutsche-Telekom-Allee 7
64295 Darmstadt
Tel.: +49 6151 58-37663

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