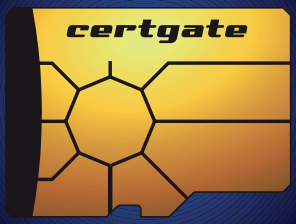
HIGH LEVEL SECURITY

FOR MOBILE & DESKTOP



certgate

MOBILE SECURITY SOLUTIONS

certgate

mobile security now!


certgate
mobile security now!
12:12
Smart Card Login
BlackBerry
Smartphone-Kennwort eingeben:
Smartcard-PIN eingeben:
certgate

Executive Summery

Die geschäftliche Nutzung von Smartphones und PDAs ist längst Alltag - besonders bei Führungskräften und im Außendienst sind die mobilen Mini-Computer für die Kommunikation unentbehrlich geworden. Notgedrungen werden Smartphones so zu „Geheimnisträgern“, auf denen unternehmenskritische Informationen empfangen, gespeichert, bearbeitet und gesendet werden. Das betrifft sowohl Kontaktdaten, E-Mails und Termine als auch Dokumente und Datenbanken der verschiedensten Art.

Somit ist es offensichtlich, dass Smartphones ebensolcher Sicherheitsmaßnahmen bedürfen, wie sie für Arbeitsplatzrechner seit langem selbstverständlich sind. Dass im Netzwerk erprobte Technologien sich nicht 1:1 auf mobile Geräte übertragen lassen, liegt in der Natur der Sache: Eine klassische Firewall um ein mobiles Kommunikationsgerät ziehen zu wollen ist ein absurdes Unterfangen. Andererseits erfordert die Einbindung von Smartphones in bestehende Sicherheits-Infrastrukturen den Rückgriff auf bewährte Sicherheitstechnologien und deren Anpassung auf die Erfordernisse des mobilen Arbeitens.

Das ist auch der Ansatzpunkt der certgate-Lösungen, die auf der Technologie der Smartcard aufbauen. Smartcards sind mit einem speziellen Chip in der Lage, eine Reihe kryptografischer Funktionen auszuführen, wie sie bei der Authentisierung eines Benutzers oder beim Verschlüsseln von Nachrichten und Dateien erforderlich sind.

Um diese Funktionalität auch auf handlichen mobilen Geräte nutzen zu können hat certgate eine Smartcard in Form einer microSD-Karte entwickelt und die erforderliche Software zur Einbindung der certgate SmartCard microSD in zahlreiche mobile Betriebssysteme geschaffen.

Als vom Gerät unabhängiger „sicherer Hardwarefaktor“ ist die certgate-Karte bereits unter Windows Mobile, BlackBerry, Android und Symbian einsetzbar. Darüber hinaus unterstützt sie auch PC-Betriebssysteme wie Windows oder Linux.

Die von certgate entwickelten Schnittstellen verbinden die certgate-Karte - immer abhängig von den Möglichkeiten des jeweiligen Betriebssystems - mit verschiedensten Sicherheits-Anwendungen. Die Spanne reicht dabei von einer sicheren 2-Faktor-Authentisierung am Gerät über die Verschlüsselung von Nachrichten und Daten bis zur kompletten Banking-Application. Diese Applicationen greifen auf die Fähigkeiten der certgate SmartCard microSD zum hochsicheren Speichern und Verwalten von Zertifikaten und Schlüsseln sowie zum Generieren von Zufallszahlen und digitalen Schlüsseln zurück.

Für das hohe Sicherheitsniveau der certgate-Technologie spricht ihr Einsatz im Projekt „SiMKo 2“ unseres Partners T-Systems. Bekannt unter dem Namen „Merkelphone“ stellt es hochsichere Kommunikation für Bundesministerien und Behörden bereit und verfügt als einziges derartiges System über eine Einsatzempfehlung des BSI für den Geheimhaltungsgrad „VS NfD“.

Die certgate-Technologie bietet Unternehmen und Organisationen die Möglichkeit, bestehende Sicherheitsrichtlinien auch auf Smartphones, PDA und andere mobile Geräte anzuwenden. Gemäß der Sicherheits-Anforderungen des Unternehmens können mobile Geräte und mobile Kommunikation gegen potentielle Bedrohungen abgesichert und Risiken vom Unternehmen abgewendet werden.

Die certgate-Technologie ermöglicht Ihnen den risikolosen Einsatz handelsüblicher Smartphones auch in sensiblen Bereichen. Das erweitert Ihre geschäftlichen Möglichkeiten und steigert die Effizienz der mobil eingesetzten Mitarbeiter. Es stärkt gleichzeitig die Compliance sowie die Sicherheit des Unternehmens gegenüber Industriespionage und Datenverlusten.

Wer braucht die certgate-Technologie?

Sind Ihre mobilen Daten ausreichend sicher?

Wer im geschäftlichen Umfeld Smartphones einsetzt, wird in jedem Falle vertrauliche, oftmals geschäftskritische Informationen auf diesem Gerät nutzen. Seien es Kontaktdaten wichtiger Kunden, Partner oder Lieferanten, Vertragsunterlagen oder auch interne Dokumentationen zu den neuesten Produkten oder Projekten. Oft beruht der Geschäftserfolg Ihres Unternehmens gerade auf diesem Informationsvorsprung vor Ihren Mitbewerbern. Diese Informationen sind schützenswert und dürfen auf keinen Fall in falsche Hände geraten.

Schützen Sie Ihr Netzwerk!

Darüber hinaus ist oftmals eine Kommunikation mobiler Geräte mit dem Firmennetzwerk für eine effiziente Arbeit des Außendienstes oder anderer „mobiler" Mitarbeiter unerlässlich. Die dafür notwendigen sicheren Kommunikationskanäle (SSL/VPN) sind jedoch nur dann unbedenklich nutzbar, wenn sichergestellt ist, dass jeder Zugriff durch eine eindeutige Authentisierung des Gerätes und des Nutzers abgesichert ist. Wird dieser Anforderungen zu wenig Aufmeksamkeit geschenkt, ist Ihr gesamtes System der Gefahr von Spionage und Manipulation ausgesetzt.

Mobil sicher kommunizieren

Was bedeutet „sicher mobil kommunizieren"? Wir verstehen darunter, dass alle schützenswerten Inhalte, die sich auf Ihrem Mobilgerät befinden und die Sie mit seiner Hilfe empfangen, bearbeiten, speichern oder versenden, vor unbefugtem Zugriff gesichert sind. Das betrifft sowohl die „stationären" Daten auf Ihrem Smartphone als auch die Datenkommunikation Ihres Geräts. Unser Anspruch ist es, diese Sicherheit auf höchstem technologischen Niveau zu gewährleisten. Dazu verwenden wir erprobte Verfahren und Standards sowie sicherheitszertifizierte Hardwarekomponenten.

Begeben Sie sich auf die sichere Seite!

Die certgate-Technologie ist für die Anforderungen von Unternehmen, Behörden und Organisationen entwickelt worden, die einen hohen Wert auf die Vertraulichkeit ihrer Daten und Dokumente legen. Dabei ist es egal, von wem eine konkrete Bedrohung ausgeht: Hacker, Konkurrenten, investigative Journalisten, Industriespione oder fremde Geheimdienste - die certgate SmartCard microSD bietet Ihnen Schutz auf höchstem technologischen Niveau. certgate baut auf der bewährten Technologie der Smartcard auf und ermöglicht mit der certgate SmartCard microSD die Nutzung kryptografischer Funktionen auf mobilen Geräten. Erst der Einsatz der certgate SmartCard microSD als zusätzlicher Hardwarefaktor macht handelsübliche Smartphones zu sicheren Kommunikationsgeräten, mit denen Sie risikolos unternehmenskritische Informationen austauschen, sicher auf Ihr Unternehmensnetzwerk zugreifen und zertifikatbasierte Mobile-Banking-Operationen ausführen können.

Eine Karte für viele Anwendungen

Die certgate SmartCard microSD verfügt über 8 sichere Zertifikatspeicher. Dort können Sie digitale Zertifikate und Schlüssel für unterschiedliche Verwendungen Manipulations- und auslesesicher verwahren und für unterschiedliche Anwendungen einsetzen: zur Authentisierung am mobilen Gerät oder per USB auch an Ihrem Arbeitsplatz-PC, zur Ver- und Entschlüsselung von Daten, zum Signieren Ver- und Entschlüsseln von E-Mails, zum Authentisieren an Web-Anwendungen oder zur Anmeldung an einem Virtuellen Privaten Netzwerk (VPN). Dabei sind Ihre privaten Signaturen und Schlüssel auf der certgate SmartCard microSD so sicher als lägen Sie in Ihrem Firmen-Safe.

Das kann die certgate SmartCard microSD

Smartphone liegengelassen?

Egal, ob Sie Ihr Smartphone bei einer Besprechung liegengelassen haben, ob Sie es verloren haben oder es gar gestohlen worden ist; die certgate SmartCard microSD verhindert in jedem Fall ein Auslesen vertraulicher Daten aus dem Gerät. Das Gerät wird im Ruhezustand durch einen sogenannten „Smartcard Logon" geschützt. Im Gegensatz zur „normalen" Geräte-PIN authentisiert sich der Nutzer dabei gegenüber der Smartcard. Erst nach erfolgter Authentisierung wird das Gerät entschlüsselt. Der Vorteil: Ein möglicher Angreifer hat tatsächlich nur 3 Versuche, den richtigen PIN einzugeben, danach schaltet sich die Karte unwiderruflich ab und das Gerät bleibt verschlüsselt. Damit wird das Klonen der verschlüsselten Inhalte und die Vervielfachung der Authentisierungsversuche ausgeschlossen. Ihre Daten bleiben unzugänglich, selbst wenn Ihr Smartphone in die Hände von Spezialisten fällt, die über hochentwickelte technische und kryptografische Möglichkeiten verfügen.

Wer hat den Schlüssel?

Entscheidend für jede Art von Verschlüsselung sind 2 Faktoren: zum einen die Stärke der Verschlüsselung und zum anderen die Sicherheit des Schlüssels, mit dem die Informationen in den Klartext zurückverwandelt werden können. Im Bezug auf die Verschlüsselungsstärke nutzt certgate zertifizierte Algorithmen, die - auch auf einen längeren Zeitraum bezogen - als sicher gelten. Die Sicherheit der Schlüssel gewährleistet certgate durch die certgate SmartCard microSD. Der auf der Karte befindliche Kryptochip generiert digitale Schlüsselpaare und speichert die zum Entschlüsseln nötigen „privaten Schlüssel" in einem speziellen Speicherbereich, der nicht auszulesen ist. So wird sichergestellt, dass dieser Schlüssel die Karte nie verlässt und somit auch nicht kompromittiert werden kann. Nur nach Freigabe der Karte mit Ihrer Smartcard-PIN können definierte Applicationen - wie beispielsweise Ihr E-Mail-Client - den Schlüssel nutzen, um Daten zu entschlüsseln oder E-Mails zu signieren.

Wozu Signaturen?

Wer Daten übertragen will, ohne dass diese in falsche Hände gelangen, sollte zunächst einmal sicherstellen, dass sein Kommunikationspartner auch der ist, für den er sich ausgibt. Die sicherste Methode, das zu gewährleisten, ist die Nutzung digitaler Zertifikate, die eindeutig einer Person zugeordnet sind. Die meisten E-Mail-Systeme unterstützen digitale Signaturen, die dem Empfänger die Sicherheit geben, dass der Absender authentisch ist und dass die Nachricht auf ihrem Weg durch die Netze nicht manipuliert wurde. certgate ermöglicht Ihnen den unbedenklichen Einsatz Ihrer „digitale Identität" auch auf Ihrem Smartphone, denn in der certgate SmartCard microSD ist sie ebenso sicher wie in einem Safe.

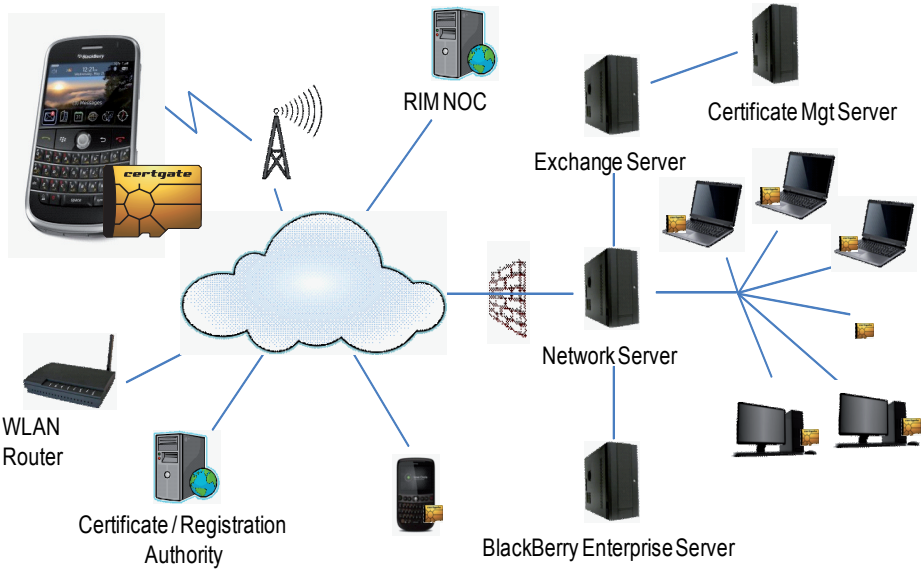
Der „Mann in der Mitte"

Bei einer signierten E-Mail können Sie sich auf die Authentizität und Integrität der Nachricht verlassen. Nicht jedoch auf die Exklusivität. E-Mails werden oft mit Postkarten verglichen: Unverschlüsselt gibt es auf Ihrem Weg eine Reihe von Stationen, wo sie mitgelesen werden können. Wie für die „Geschäftspost" ein Kouvert verwendet wird, sollten vertrauliche Mitteilungen in verschlüsselten E-Mails versandt werden. Auch dazu kommen digitale Schlüssel zum Einsatz. certgate unterstützt den S/MIME-Standard zur Verschlüsslung des E-Mail-Verkehrs und stellt den sicheren Zertifikatspeicher für Ihre Verschlüsselung auf

dem Smartphone zur Verfügung. Da es sich bei diesem System um eine starke „Ende-zu Ende"-Verschlüsselung handelt, hat der „Man-in-the-middle" keine Chance, Ihre Nachrichten mitzulesen.

Sicher ins Firmennetzwerk?

Schnell mal ins Unternehmensnetzwerk einklinken, um die neuesten Informationen abzurufen - über VPN (Virtual Privat Network) ist das sicher und komfortabel von unterwegs möglich. Der Datenaustausch über einen VPN-Tunnel erfolgt verschlüsselt. Voraussetzung für die Sicherheit dieser Verbindung und damit auch für Ihr Firmennetz ist natürlich Ihre sichere Authentisierung gegenüber Ihrem VPN-Client. Gerade bei der Sicherheit der Zugänge zu Ihrem Firmennetz steht sehr viel auf dem Spiel. Hier finden Hacker eine bevorzugte Hintertür für das Eindringen in Ihr System, für Spionageangriffe und Manipulationen an Ihren Daten. Deshalb sind hohe Sicherheitskriterien an diese Zugangsberechtigungen anzulegen. Username + Passwort reichen dafür in der Regel nicht aus. Eine zertifikatbasierte Authentisierung hingegen gilt als eine der sichersten Methoden. Auch in diesem Fall liefern die auf der certgate SmartCard microSD manipulationssicher verwahrten Zertifikate den Schlüssel zur Nutzung des sicheren Datenkanals.



Beispiel: E-Mail-Verschlüsselung

... und ins Intranet?

Das gleiche gilt, wenn Sie Daten in einem Intranet zur Verfügung stellen. Auch hier erreichen Sie mit zertifikatbasierten Zugängen zu https-Seiten ein höheres Sicherheitsniveau und können mittels sicherer, verschlüsselter SSL-Verbindungen auch von Ihrem Smartphone aus auf geschützte Informationen zugreifen. Die SSL-Zertifikate dafür liegen sicher verwahrt auf der certgate SmartCard microSD.

„Endpoint-Security“

Kriminelle nutzen vielfältige Methoden, um an Ihre sensiblen Daten zu gelangen. Auch für Smartphones wächst die Gefahr einer „Infektion“ durch Viren, Trojaner oder Spyware. Diese kleinen Programme sind deshalb so gefährlich, weil sie sich unbemerkt in Gerät einnisten und dort eingerichtete Sicherheitsvorkehrungen umgehen oder ausschalten können. So lassen sich beispielsweise über das direkte Mitprotokollieren von Tastatureingaben (Keylogging) PIN oder Passworte abfangen. Spezielle Spyware-Tools können verschlüsselte Dokumente in dem Moment kopieren, wenn sie zum Anzeigen oder zur Bearbeitung unverschlüsselt in den Arbeitsspeicher geladen werden. Um solchen Angriffen wirkungsvoll begegnen zu können, muss auch das Betriebssystem des Smartphones gegen Manipulationen geschützt und das Eindringen von Maleware unterbunden werden. Dabei ist die Anfälligkeit der einzelnen Betriebssysteme für Maleware-Attacken und die standardmäßigen Sicherheitsvorkehrungen sehr unterschiedlich.

Kernel Protection

Die certgate SmartCard microSD ist in der Lage, das Eindringen von Malware zu unterbinden. Speziell unter dem Betriebssystem Windows Mobile kann Ihr Administrator sämtliche Schnittstellen, Anwendungen und Funktionen Ihres Smartphones entsprechend den Sicherheitsanforderungen Ihrer Organisation einstellen. So können beispielsweise Schnittstellen wie WLAN oder BlueTooth, die häufig zum Einschleusen von Trojanern missbraucht werden, abgeschaltet oder Funktionalitäten wie GPS und Kamera wahlweise aktiviert oder deaktiviert werden. Diese Geräte-Konfiguration lässt sich weder durch den Anwender am Gerät noch durch einen Administrator aus der Ferne verändern. Sie wird durch ein Zertifikat auf der certgate SmartCard microSD vor jeglicher Manipulation geschützt.

Code Signing

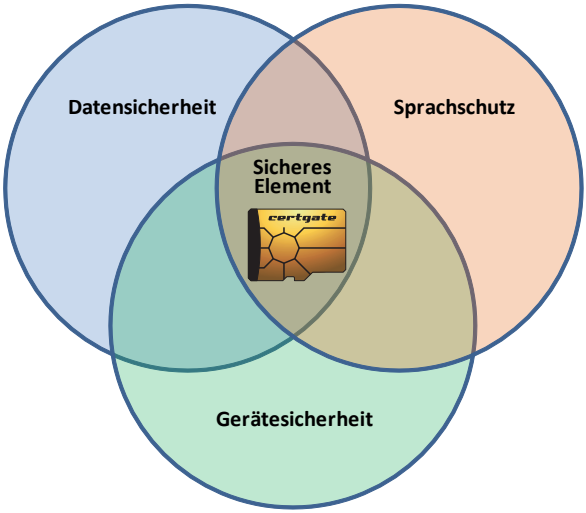
Sollte es einem Angreifer trotzdem gelingen, schädliche Software auf irgendeinem Weg auf das Smartphone zu schleusen - sei es als Anhang an eine unverdächtig wirkende E-Mail oder als Software-Update getarnt - verhindert eine digitale Signatur die Installation im System. Die dazu genutzte Technologie wird als „Code Signing“ bezeichnet. Sie verhindert jegliche Installation von Software, soweit diese keine speziellen Signatur trägt, die auf der certgate SmartCard microSD manipulationssicher hinterlegt ist. Damit stellt certgate sicher, dass keine infizierten Programme auf Ihr Smartphone gelangen können. Eine ähnliche Lösung ist auch für das Android-Betriebssystem in Vorbereitung.

Zertifizierte Sicherheit

All diese Maßnahmen erreichen ein sehr hohes Maß an Sicherheit für Ihre mobile Kommunikation. Deshalb verfügt die beschriebene Technologie im Rahmen des Projekts SimKo 2 über die Einsatzempfehlung des BSI (Bundesamt für Sicherheit in der Informationstechnik) für den Geheimhaltungsgrad VS NfD und wird vom Bundeskanzleramt, vom Bundesinnenministerium und vielen weiteren Bundesbehörden zur sicheren Datenkommunikation eingesetzt.

Ihre Vorteile von der certgate-Technologie

- Schnelle und kostengünstige Einbindung mobiler Endgeräte in die existierende Sicherheits-Infrastruktur Ihres Unternehmens
- Erhöhung des Sicherheits-Levels beim Einsatz mobiler Anwendungen und bei mobilen Netzwerkzugriffen
- Sicherheitsniveau individuell skalierbar – bis hin zu Hochsicherheitsbereichen
- Nutzung aller Sicherheitsanwendungen, die über herkömmliche Smartcards abbildbar sind, auch für mobile Endgeräte
- Unterstützung zahlreicher mobiler Betriebssysteme
- Einsatz im normalen Kartenslot (SD, miniSD, microSD) der Mobilgeräte
- Kein Austausch der eingesetzten Endgeräte (Smartphones, PDA, Laptops etc.) notwendig
- Keine zusätzlichen Kosten für Karten-Lesegeräte oder spezielle mobile Geräte
- Auf der certgate Karte gespeicherte Zertifikate sind auch am Desktop-PC direkt oder per Adapter nutzbar
- Geringer Administrationsaufwand durch einmalige Konfiguration der certgate Anwendung gemäß den internen Sicherheitsrichtlinien
- Höchstmögliche Sicherheit für Benutzer-, Anwendungs- und Unternehmensdaten
- Sichere Erstauthentisierung des Benutzers
- Einmalige Prüfung der Berechtigungen (Single Sign On)



Technische Highlights

Eigenschaften

- SmartCard-Einsatz mit Windows Mobile™, BlackBerry™, Symbian und Android via SD™ Card Slot
- SmartCard-Einsatz mit Windows™ oder Linux Desktop oder Notebook Anwendungen über SD™ Card Slot, USB-Card Reader oder ActiveSync, drahtlos über Bluetooth oder WLAN mit der ***certgate*** **SmartCard microSD** im Card Slot des mobilen Gerätes
- Laden von Zertifikaten und Schlüsseln auf die ***certgate*** **SmartCard microSD** (RSA 2048 Bit, 8 Keystores verfügbar)
- On-card Generierung von RSA Schlüsselpaaren (RSA 2048 Bit)
- On-card Signatur Generierung mit privatem Schlüssel (RSA, PKCS#1.5 padding)
- On-card asymmetrische Verschlüsselung (RSA, no padding)
- On-card Generierung und Export echter Zufallszahlen
- Verschlüsselungszeit: RSA 2048 Bit Signatur: ca. 0,5 s; RSA 2048 Bit Schlüsselgenerierung: ab 3 s

Hardware-Standards

- SD Spezifikation: 1.10 und microSD™ Addendum 1.10
- Smartcard-Chip: NXP P5CC072 Smartcard-Controller; Common Criteria EAL5+ zertifiziert
- On-card sicherer Zufallszahlengenerator; FIPS PUB 140-2 und BSI AIS 31 konform
- Erweiterter 80C51 Microcontroller (Secure_MX51/NXP)
- ISO7816 Schnittstelle für APDU-Transfer zwischen Smartcard und SD-Controller
- Smartcard Betriebssystem: JCOP™ 2.3.1 (Common Criteria EAL4+ zertifiziert), JavaCard™ 2.2.1
  und GlobalPlatform™ 2.1.1 konform
- Hoch resistent gegen SPA/DPA Counter Measure Attacks; BSI DSZ CC 0227 konform

	Windows XP/Vista/7	Windows Mobile	Linux*	BlackBerry	Symbian	Android
certgate SmartCard microSD	✓	✓	✓	✓	✓	✓
Smartcard Logon	✓	✓	✓	✓	✓	✓
Geräte-Verschlüsselung**	✓	✓	✓			✓
Email-Verschlüsselung**	✓	✓	✓	✓		
VPN**	✓	✓	✓			
SSL**	✓	✓		✓	✓	
Kernel-Protection		✓				
Code-Signing		✓				
Bankiing Solution**	✓	✓		✓		

* Kompilierung für einzelne Linux-Derivate auf Anfrage
** unter Nutzung von Zertifikaten/Schlüsseln auf der ***certgate*** SmartCard microSD


certgate
mobile security now!
Smart Card Login
1
2
3
4
5
6
7
8
9
0
C
OK
certgate
icc

certgate **GmbH**

Merianstrasse 26
90409 Nürnberg
Deutschland

Tel + 49 (911) 9 35 23 - 0
Fax + 49 (911) 9 35 23 - 52
Email info@certgate.com
www.certgate.com