

Schutzschild für Smartphone-Daten

› Mit Hilfe des "Certgate Protector" können Firmen die Daten auf Windows-Mobile-Geräten schützen und Funktionen ab- oder zuschalten. Die COMPUTERWOCHE hat die Lösung auf Leib und Nieren getestet.

Von Manfred Bremmer (17.06.2009 05:07:00)

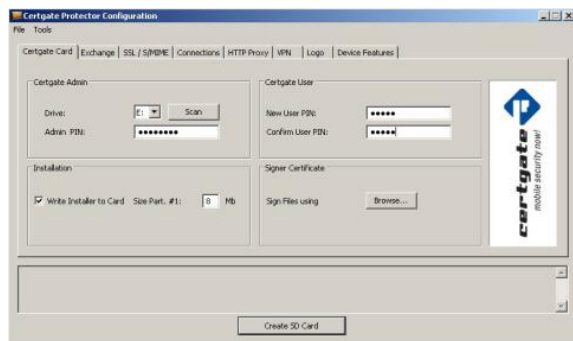
Die Ausstattung mobiler Mitarbeiter mit Smartphones ist für viele Unternehmen ein zweischneidiges Schwert. So wird zum einen zwar die Produktivität von Außendienstlern dadurch deutlich erhöht. Andererseits müssen die Firmen jedoch fürchten, dass die auf den Geräten gespeicherten Daten bei Verlust oder Diebstahl in falsche Hände gelangen. Nicht ohne Grund ist vor allem bei hochrangigen Mitarbeitern in Unternehmen oder Regierungen der Einsatz von Smartphones umstritten.

In Hinblick auf die mitunter hohen Sicherheitsanforderungen in Unternehmen hat das Nürnberger Startup [Certgate](#)¹ eine Lösung entwickelt, die unter anderem auch in dem von T-Systems entwickelten [SiMKo 2](#)² - besser bekannt als "Schäuble-Handheld" oder "Merkel-Phone" zum Einsatz kommt.

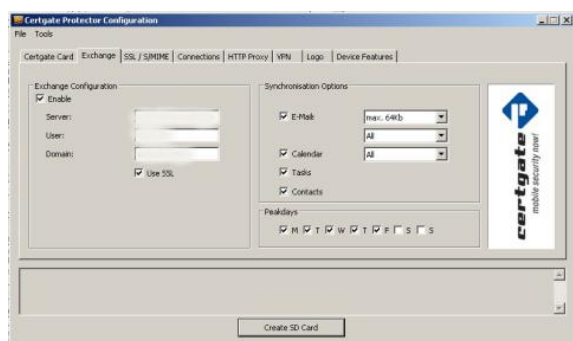
Während bei SiMKo 2 einzelne Sicherheitsfunktionen nicht separat an- beziehungsweise abschaltbar sind, hat Certgate mit dem Certgate Protector aber auch eine eigene, konfigurierbare Lösung im Programm. Die Funktionsweise ist schnell erklärt: Windows Mobile besteht aus dem Windows-CE-Kernel, um das herum das mobile Betriebssystem angelegt ist. Von diesem Gebilde wiederum gehen Programmierschnittstellen ab, etwa zu Bluetooth, zum User Interface oder zum GSM-Stack. Hier greift der von Certgate entwickelte und in der Lösung integrierte Kernel-Protector ein: Nach der sicheren Aktivierung durch den Nutzer legt er sich wie ein Schutzmantel um den Windows-CE-Kernel und verhindert Manipulationen in der Gerätekonfiguration. Das Sicherheitsniveau ist dabei beliebig festlegbar.



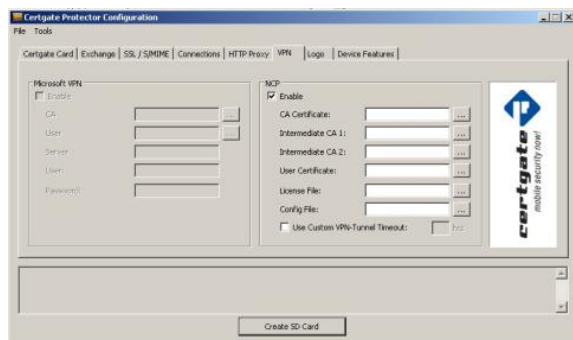
Certgate Protector Smartcard: Zentrales Element von Certgate Protector ist eine MicroSD-Card mit integriertem Kryptoprozessor, der digitale Schlüsselpaare generieren und speichern kann.



Certgate Protector Start: Um ein Windows-Mobile-Gerät zu präparieren, benötigt man die MicroSD-Card und die Anwendung Certgate Protector Setup-Tool.



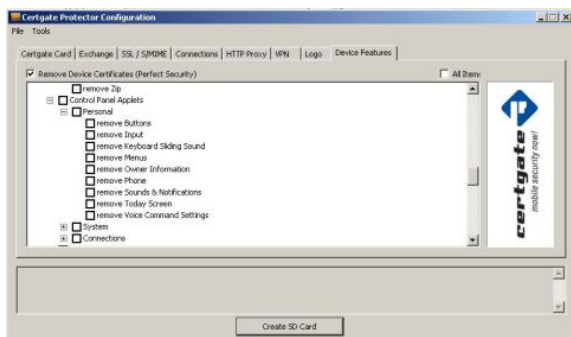
Certgate Protector Exchange: Erleichtert den Rollout: Im Folder Exchange kann der Administrator die Voreinstellungen des Mail-Accounts tätigen und verschiedene Optionen zur Synchronisierung festlegen.



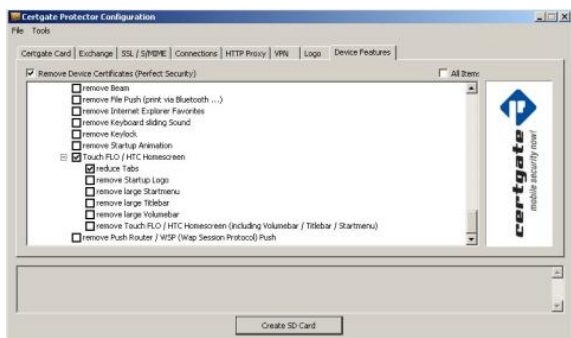
Certgate Protector VPN: Die Karteikarte "VPN" erlaubt die Konfiguration eines Virtual Private Network.



Certgate Protector Logo: Nettes Extra: Mit der Einbindung eines Firmenlogos in die Anmeldemaske kann man das Smartphone an die Corporate Identity anpassen.



Certgate Protector Personal: Wichtigster Punkt sind die Device Features: In dem Bereich lassen sich Funktionen ein- und (vor allem) ausschalten



Certgate Protector HTC: Auf Wunsch lässt sich auch die von HTC entwickelte Benutzeroberfläche Touchflo, beziehungsweise Teile davon deaktivieren.

Zentrales Element von Certgate Protector ist eine MicroSD-Card mit integriertem Kryptoprozessor mit der Zertifizierung EAL 4+ (Evaluation Assurance Level), der digitale Schlüsselpaare (RSA 2048 Bit) generieren und speichern kann. Die auf der Smartcard abgelegten Zertifikate und Schlüssel werden zur Verschlüsselung der gesamten Benutzerdaten genutzt, die damit selbst bei Verlust des Gerätes zuverlässig gegen unautorisiertes Auslesen geschützt sind. Darüber hinaus werden sie zur Verschlüsselung und Signatur von E-Mails und für den Zugriff auf ein gesichertes Netz (VPN) oder geschützte Internet-Seiten (SSL) eingesetzt. Aktuell unterstützt die Certgate-Lösung Geräte ab Windows Mobile 6.1, ein Update auf die geplante Version 6.5 ist für September vorgesehen.

» Setup mit vielen Einstellungsmöglichkeiten

Um ein Windows-Mobile-Gerät entsprechend zu präparieren, benötigt man eine Certgate-MicroSD-Karte sowie die Anwendung Certgate Protector Setup-Tool - das Exe-File läuft auf Windows XP oder Vista. Die Applikation ist sehr übersichtlich in acht Folder unterteilt, in denen der Administrator verschiedene Einstellungen vornehmen kann. Nachdem die Karte in einem Lesegerät über mit dem PC verbunden wurde, empfiehlt es sich als ersten Schritt, im Folder SD Card den Speicher in einen Sektor für verschlüsselte Dateien sowie einen für unverschlüsselte Installationsdateien unterteilen - zum Schutz vor Manipulationen wird auch diese Partition mit Hilfe des CertProcessor und eines Zertifikats später verschlüsselt. Bereits bei diesem Prozess achtet Certgate auf den Schutz der gespeicherten Daten: Wird eine bereits genutzte Karte verwendet, kann der Administrator trotz PIN-Autorisierung nur die User-Daten löschen, nicht aber auf sie zugreifen. Der Zugriff ist nur mit der individuellen User-PIN möglich, die man an dieser Stelle auch gleich anlegt. Für die Erstinbetriebnahme ist ein Zertifikat erforderlich. Hat man keines parat, kann man unter dem Menüpunkt "Tools" auch ein selbstunterzeichnetes Zertifikat generieren, mit dem die zu installierenden Programme signiert werden müssen. Die Schlüssel, mit denen das Gerät und der Flashspeicher der SD-Card später verschlüsselt werden, erzeugt das System während der Erstinbetriebnahme direkt auf der Smartcard (Erstauthentifizierung).

Die übrigen Reiter bieten eine Reihe an Einstellungsmöglichkeiten und sind nahezu selbsterklärend: Im Folder "Exchange" kann der Administrator die Voreinstellungen des Mail-Account tätigen und verschiedene Optionen zur Synchronisierung festlegen. Dazu zählt etwa Größe und Alter der zu übertragenden Mitteilungen. Außerdem lässt sich einstellen, ob auch Kalender, Aufgaben und Kontakte aus Outlook synchronisiert werden sollen und an welchen Tagen das geschehen soll - nur werktags oder die ganze Woche über. Im Reiter "SSL /SMIME" lassen sich entsprechend Schlüssel für den Zugriff auf geschützte Web-Seiten (SSL mit zertifikatsbasierender Client-Authentisierung) generieren, während der Bereich "Connections" die Möglichkeit bietet, den Zugangspunkt (APN) zu konfigurieren. Dieser Schritt erleichtert nicht nur den Roll-out, er ist mitunter auch die einzige Option zur Eingabe der Daten, falls dieser Bereich in den Einstellungen auf dem Endgerät später gesperrt sein soll.

Unter "HTTP Proxy" können Einstellungen für einen entsprechenden Web-Filter vorgenommen werden, während "VPN" die Konfiguration eines Virtual Private Network erlaubt. Neben der Lösung von Microsoft kann auch ein VPN vom Certgate-Kooperationspartner NCP und anderen Anbietern genutzt werden - sofern der Lizenzschlüssel vorhanden ist. Mit der Funktion VPN Tunnel Timeout kann festgelegt werden, nach welcher Zeit eine VPN-Verbindung unterbrochen wird, um das generell mögliche - aber zeitaufwändige - Knacken der Verschlüsselung zu erschweren. Die Funktion "Logo" erlaubt es Firmen, die Certgate-Lösung durch die Einbindung eines Logos in die Anmeldemaske auf dem Smartphone an die Corporate-Identity anzupassen.

» Sperren von Funktionen

Wichtigster Punkt sind die Device-Features - hier geht es um das Ein- und Ausschalten von Funktionen. Um den Anwender (auch vor sich selbst) zu schützen, lassen sich unter anderem Bluetooth, WLAN oder ActiveSync abschalten, die Kamera oder bestimmte Anwendungen wie den Media-Player deaktivieren oder generell Ports blockieren. Außerdem besteht die Möglichkeit, Hersteller- oder Provider-Zertifikate abzuschalten - dies verhindert die Gefahr durch Trojaner, die sich solcher Hersteller-Zertifikate bedienen. In diesen Bereich hat Certgate einen großen Teil an eigenem Know-how eingebracht. So lassen sich nur mit tiefer Kenntnis über das Zusammenspiel einzelner Komponenten in den Windows-Mobile-Geräten Fehlermeldungen beim Deaktivieren von Funktionen wie der HTC-Touchflo-Oberfläche vermeiden.

Zur besseren Übersichtlichkeit hat Certgate die meisten Funktionen im Menüpunkt Advanced versteckt. Nach dessen Anklicken überfällt den Nutzer eine fast endlos - aber immerhin vollständig - scheinende Liste an Unterpunkten. Diese gilt es abzuarbeiten, wenn es erforderlich ist, eine Unternehmens-Policy abzubilden.

Als Alternative bietet Certgate den Button "All items" an - hier werden alle relevanten Gerätefunktionen deaktiviert und der Administrator kann im Nachgang auf der Liste durch Entfernen von Häkchen benötigte Features wieder hinzuschalten. Etwas gnädiger mit dem Endanwender ist die Voreinstellung "Remove Device Certificates (Perfect Security)": Um potenzielle Sicherheitsrisiken zu stoppen, werden hier verdächtige Programme wie Adobe Reader, Opera-Browser und Google Maps deaktiviert. Spiele sind ebenso wenig zugelassen wie die Nutzung von integriertem Radio oder der Kamerafunktion. Außerdem setzt Perfect Security eine Reihe von Policies um. Unter anderem werden unsignierte .cab-Dateien, Anwendungen oder Themes nicht zugelassen.

Trotz der umfänglichen Auswahl dauert die gesamte Konfiguration in der Praxis keine fünf Minuten -

vorausgesetzt, man hat die benötigten Daten parat und eine klare Vorstellung über die Details der gewünschten User-Policy. Um die Einstellungen anschließend nicht bei jedem Gerät neu vornehmen zu müssen, kann man die Konfigurationsprofile - außer Exchange-Passwort und User-Pin - speichern. Dank offener Schnittstellen lassen sich außerdem für größere Roll-outs Libraries einbinden.

» Beschreiben der MicroSD-Card

Der Befehl "Create SD-Card" schließt den Prozess ab: Auf Knopfdruck formatiert das Programm die Certgate MicroSD-Karte, überschreibt - falls vorhanden - die vorherige PIN, erstellt eine Partition, schreibt Zertifikate in Filesystem der Smartcard und legt die Installationsdateien an. Im Programm wird der Ablauf dokumentiert, wurden Eingaben wie die User-PIN oder die Exchange-Einstellungen vergessen, tauchen Fehlermeldungen auf. Ein erfolgreicher Ablauf wird wie folgt protokolliert:

```
*** Creating card ***  
Formatting card (8Mb)... success  
Overwriting PIN... success  
Writing dummy certificate to slot 1... success  
Encrypting Exchange Config File using slot 1... success  
Writing installer and signing files... success  
Writing cgCustom... success  
Writing Bootstrap... success  
Generating Cleanup and Blacklist File... success  
*** Card successfully created ***
```

Nach diesem Prozess ist die Certgate-Karte einsatzbereit und wird dem Endanwender - möglichst getrennt von der User-PIN und dem Gerät - bereitgestellt. Steckt der Nutzer die MicroSD-card in den dafür vorgesehenen Slot des Smartphones, beginnt die automatische Installation. Nach einmaligem Neustart ist das Gerät einsatzbereit und die Anmeldemaske erscheint. Nach der anschließenden Eingabe des PIN kann das Smartphone verwendet werden. Allzu oft vertippen darf man sich dabei jedoch nicht: Nach drei Fehlversuchen wird die Karte deaktiviert, in diesem Fall ist nicht nur das Telefon gesperrt, sondern die Zertifikate auf der Smartcard sind unwiederbringlich verloren. Damit können die Daten auf dem Gerät ebenso wie auf der Karte nicht mehr ausgelesen werden. Wie Certgate erklärte, handelt es sich dabei um ein wichtiges Sicherheits-Feature. Einziger Weg, das Gerät wieder zu nutzen, ist, es durch einen Hard-Reset in seinen Ausgangszustand zurückzusetzen. Die Karte muss durch den Administrator neu konfiguriert werden. In beiden Fällen beginnt das mit einer Neuformatierung.

Wie ein Vergleich mit einem herkömmlichen Gerät zeigte - im Test handelte es sich um zwei HTC Touch Pro - , ist das Certgate-Device durch den Eingriff nicht langsamer geworden. Je nachdem, wie rechen- oder speicherintensiv die abgeschalteten Funktionen wären, reagiert es vielmehr schneller, auch die Batterielaufzeit nimmt zu.

¹ <http://www.certgate.de/>

² http://www.computerwoche.de/knowledge_center/mobile_wireless/1889331/

IDG Business Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Business Media GmbH. DPA-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass in Computerwoche unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von Computerwoche aus gelinkt wird, übernimmt die IDG Business Media GmbH keine Verantwortung.