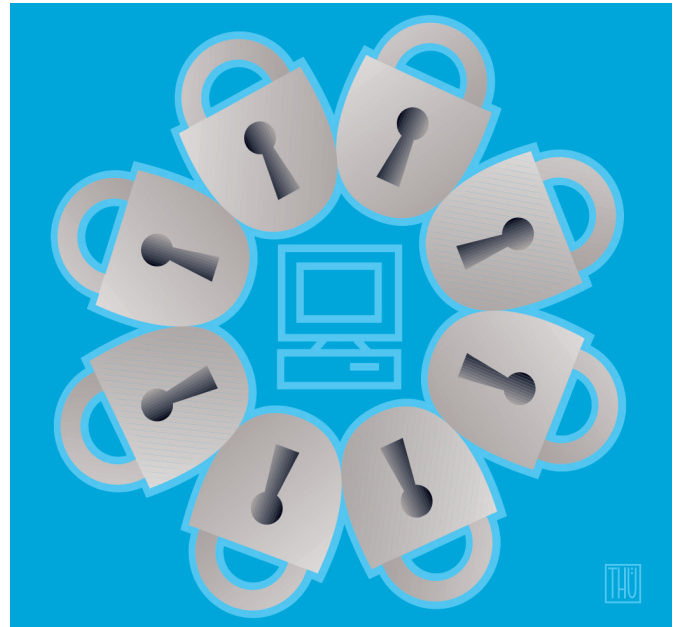


IT-SECURITY-HELPDESK

Komfort und Sicherheit mit Smartcards

Wir beabsichtigen, den physischen und logischen Zugang mit Smartcards abzusichern. Kann die Microsoft Certification Authority Smartcards personalisieren und verwalten?



Ab Windows 2000 unterstützt Microsoft starke Authentisierung mittels Smartcards beim Logon. Zusammen mit dem Active Directory bietet Microsoft eine umfassende Public Key Infrastruktur (PKI) an, die mit vernünftigem Aufwand aufgebaut und betrieben werden kann. Teil dieses Integrationspakets sind die verschiedenen, von Microsoft zur Verfügung gestellten Certificate Templates. Zur Ausstellung von Smartcards für das Windows-Logon steht Ihnen ein Smartcard Logon Template zur Verfügung. Dieses können Sie an Ihre spezifischen Bedürfnisse anpassen oder auch direkt übernehmen.

Die Personalisierung der Smartcard erfolgt durch eine vertrauenswürdige Stelle, welche oft auch als Registration Authority (RA) bezeichnet wird. Ihre Aufgabe ist, die Identität der Person vor der Ausstellung der Smartcard zu überprüfen.

Dieser relativ komplexe Prozess ist bei einer öffentlichen Certification Authority (CA) sinnvoll – in Ihrem Falle aber absolut nicht erforderlich.

Innerhalb eines Unternehmens können Smartcard und PIN (Personal Identification Number) auf separaten Wegen dem Benutzer, der ja schon bekannt ist und bei der Einstellung überprüft und identifiziert wurde, zugestellt werden. Um die Sicherheit zu gewährleisten, stellt Microsoft ein spezielles Certificate Enrollment Template zur Verfügung. Dieses Zertifikat wird nur für die Personen ausgestellt, die Smartcards personalisieren. Konzeption und Umsetzung dieser Lösung beanspruchen rund drei bis vier Wochen.

Nicht gelöst ist damit allerdings die Integration der physischen Zugangskontrolle und die Unterstützung der Mitarbeiter bei alltäglichen Problemen wie zum Beispiel dann, wenn eine

Karte vergessen wurde oder blockiert worden ist.

Wenn Sie Smartcards einsetzen, ist es daher ratsam, den Betrieb der PKI durch effizientes Smartcard Management zu ergänzen. Dabei übernimmt das Smartcard Management die Funktion der RA. Card-Management-Systeme, wie sie von Safenet, Thales und RSA angeboten werden, integrieren neben der PKI auch Lösungen für den physischen Zugang, die Zeiterfassung, das Zahlssystem und die Bildbearbeitung.

Smartcard Management hilft Ihnen, die Mitarbeiter über den gesamten Lebenszyklus der

Funktionalität mit eher eingeschränkter Kompatibilität.

Es ist deshalb wichtig, dass Sie sich vor dem Aufbau der Infrastruktur Gedanken über das genaue Einsatzszenario der Karte machen.

Innerhalb der Unternehmung können die Mitarbeiter über Self-Service-Kioske oder Supportstellen eine blockierte Karte entsperren oder eine vergessene Karte ersetzen. Ein mobiler Mitarbeiter kann hingegen mit einer blockierten Karte nicht einloggen.

Einige Kartenhersteller bieten auch für diese Fälle geeignete Lösungen an. So kann durch die Integration der Smartcard Middleware in die Microsoft GINA (Graphical Identification and

Authentication) über ein Challenge-Response-Verfahren die Karte des betroffenen Mitarbeiters via Telefon oder SMS wieder freigegeben werden.

Smartcard-Technologie richtig eingesetzt, verbessert die Sicherheit des Unternehmens und wird von den Mitarbeitern geschätzt und akzeptiert. ■

Personalausweise mit integrierten Sicherheitsfunktionen setzen neue Maßstäbe im Identity Management.

Smartcard effizient zu unterstützen und die kleinen Probleme im Betrieb zu lösen.

Auch wenn die Technologie vergleichbar ist, ist deren Implementation allerdings durchaus unterschiedlich. Einige Hersteller implementieren die minimalen Anforderungen der Smartcard-Standards wie PKCS#11 und PC/SC und erreichen so eine sehr hohe Kompatibilität. Wiederum andere Hersteller bieten eine sehr hohe



Der Autor
Antonio Retica ist Leiter IT-Security bei ITRIS Trading in Spreitenbach.
www.itris.ch

Jede Woche beantworten Sicherheitsexperten Ihre Leserfragen:

Haben Sie Fragen rund ums Thema IT-Sicherheit?

Schreiben Sie uns:
it-security@computerworld.ch

 **Archiv aller Helpdeskartikel:**
www.computerworld.ch