

Kartenmanagement

Das leichte Spiel mit den Karten...?

Einer der Hauptgründe für schwache IT-Security ist immer wieder in der altbekannten Passwort-Problematik zu finden. Selbst dann, wenn alle sonstigen Hausaufgaben zur Absicherung der Plattformen erledigt wurden, bleibt immer noch der Missbrauch von fremden Rollen durch ergaunerte oder erratene Passwörter, der dem Eindringling Tür und Tor öffnet.

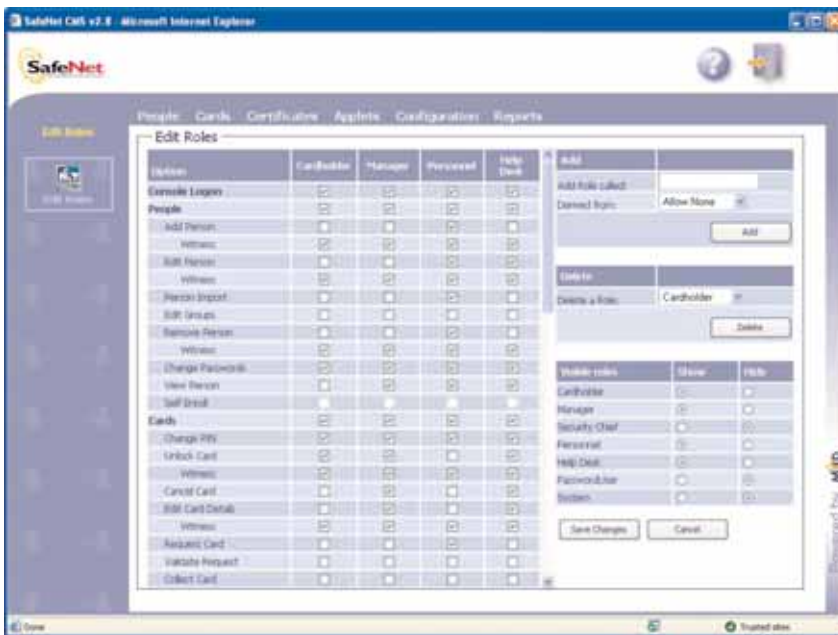


Bild 1: Rollen können beliebig definiert werden, um Genehmigungsprozesse einfach abbilden zu können.

Roll-Out: ist doch in der Plattform alles schon drinnen und ready-to-go! Man nehme einfach einen Windows Server (kann schon der SBS 2003 sein), konfiguriere das Active Directory, installiere IIS und die Certificate Authority und benutze ganz einfach das vorhandene Webinterface um Zertifikate auszustellen. So weit so gut. Man liest dort weiter, dass auch Microsoft selbst die dargebotenen Funktionen im großen Umfeld verwendet, also kann es doch gar nicht so schlecht sein und scheint wohl auch für die „Großen“ geeignet zu sein. Man beschaffe sich nur noch irgendwo ums Eck diese kleinen Plastikkarten mit Chip drauf plus die passenden Leser und schon verschlüsselt man E-Mails und meldet sich am System an – ganz ohne Passwort, sondern elegant mit Zertifikat.

Das klingt übertrieben? Ist es aber nicht, weil im Grunde genommen stimmt es ja und die Produkte sind tatsächlich so gut vorbereitet, dass man von Null auf Hundert in weniger als einer Stunde kommen kann.

Das ist nichts Neues und man kann das Thema ja auch schon gar nicht mehr hören, vor allem auch deshalb nicht, weil die Berichte über Phishing-Attacken ohnehin praktisch jede Woche in den Medien auftauchen. Die Lösung dazu wird ebenfalls wie Gulasch permanent aufgewärmt: Weg mit den Passwörtern – Her mit sicherer (2-faktor-)Authentifizierung. Das klingt alles recht fein und ist im kleinen Umfeld im Hand-

umdrehen umgesetzt – was aber wenn wir über einen Roll-Out von mehreren tausend Benutzern reden?

„Die Hardware ist der Enabler – und zugleich oft auch der Stolperstein!“

Die braven Microsoft-Anwender unter uns finden in ihrem Wissensgrahl (Technet) haufenweise Informationen zum Thema PKI und Smart Card

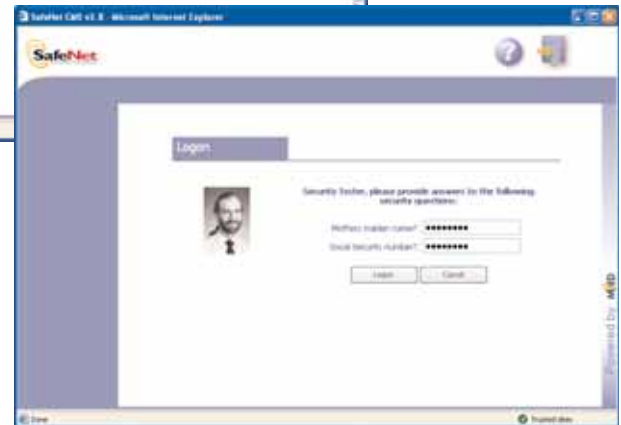
Mit der Windows 2003 CA kann man eigene Zertifikats-Templates definieren, Cross-Certification einrichten und Key Archival umsetzen. Auch das Handwerkszeug auch für „Große“ ist tatsächlich ohne Zusatzgebühren im Windows Server enthalten. Nur das Deployment ist nicht für „Große“. Genau betrachtet nicht einmal für „Mittlere“, sondern eher nur für die ganz kleinen. Das beginnt schon bei der Ausstellung der Karten, die nur manuell Stück für Stück erfolgen kann, zwar schon an zentraler Stelle durch einen so genannten Enrollment Agent, aber dennoch mit Boardwerkzeugen nicht automatisiert in einem Batch. Selbst bei mehreren Hundert zu personalisierenden Medien wird das bereits ein sehr aufwändiger und mühsamer Prozess. Ganz zu schweigen von den notwendigen Arbeitsschritten zum Beispiel bei Verlust der Karte oder was noch viel öfter vorkommt: die Vergesslichkeit der Benutzer, die dann ohne Karte zum Dienst erscheinen. Altes Zertifikat sperren, neue Karte initialisieren, Zertifikat beantragen, eventuell noch den Kartendruck anstoßen und dann das ganze auch noch einmal im Zutritts-/Zeiterfassungssystem. Dabei sind wir da noch nicht einmal auf das Thema der Verschlüsselung eingegangen, wo das sichere Archivieren der Schlüsselpaare essentiell ist und dadurch in der Regel auch mehrere Zertifikate pro Benutzer zur Anwendung kommen. Dazu aber später noch mehr.

Der eine oder andere wird angesichts des beschriebenen administrativen Aufwandes wohl schon an organisatorische Geißelungen denken, damit diese Fälle möglichst auf Null reduziert werden. Da bleiben aber trotzdem noch die Faktoren der Mitarbeiterfluktuation und der (empfohlenen) begrenzten Zertifikatsgültigkeit – so sollte man sich schon irgendwann mit dem Gedanken des Renewals beschäftigen. Außerdem müssen Sie auch damit rechnen, dass einige der lieben Anwender selbst den einen PIN noch vergessen und damit die Karte blockieren. Wie



Bild 2: Antrag auf eine Ersatzkarte durch den Benutzer.

Bild 3: Um den Verlust der Karte zu melden kann sich der Benutzer auch ohne Karte authentifizieren.



heißt es in der Werbung: „Es gibt immer was zu tun!“

Die Verlockungen rufen trotzdem...

Was sind jedoch all diese Schwierigkeiten auf der einen Seite gegen die vielen Anwendungsmöglichkeiten, die durch den Einsatz von digitalen Zertifikaten entstehen. Nicht nur der klassische Sicherheitsbereich mit Multi-Factor Authentifizierung mit der Bequemlichkeit eines Single-Sign-On Systems und die Verschlüsselung von Festplatten und E-Mails sei hier zu erwähnen, sondern auch das gesamte Gebiet der digitalen Signatur. Gerade dieser letztgenannte Bereich hält durch die damit erziel-

baren gewaltigen Effizienzsteigerungen beim Work-Flow-Management Einzug in viele Unternehmen.

Die Komplexität im Karten- bzw. Zertifikatsmanagement hängt jedoch sehr stark von der umgesetzten Funktionalität ab. Generell lässt sich sagen, dass mit der Einbindung von Datenverschlüsselung die Anforderungen erheblich steigen, da für jede Entschlüsselung der private Teil des Schlüsselpaars benötigt wird, während die Signaturüberprüfung ausschließlich mit den öffentlichen Teil erfolgt. Wie schon die Bezeichnung nahe legt, ist der öffentliche Schlüssel für jeden zugänglich und daher bei Verlust der Karte immer noch verfügbar. So kann für die Authentifizierung und die Signaturfunktion auch recht

„Die Ausgabe von Kartenlösungen muss einfach und schnell erfolgen können.“

problemlos jederzeit ein neues Zertifikat mit neuem Schlüsselpaar ausgestellt werden. Anders bei der Verschlüsselung. Wenn hier Ihr Hund die Karte frisst und Sie kein Recovery-System einsetzen, sind von nun an Ihre geheimen Informationen auch vor Ihnen selbst geheim und das ist wohl nicht im Sinne des Erfinders.

Es bleibt daher nicht viel anderes übrig, als auch den privaten, geheimen Schlüssel an einer sicheren Stelle zu hinterlegen. Das nennt man Key-Archival. Nur ein oder mehrere vertrauenswürdige Dritte können bei abhanden kommen der Karte das Verschlüsselungszertifikat wiederherstellen. Angesichts des drohenden Verlusts aller wichtigen Informationen geht man diesen Kompromiss bei der Sicherheit wohl ein. Anders wenn es um Anwendungen der digitalen Sig-

num kommen, denn sonst verspielen Sie die erzielten Effizienzsteigerungen sofort wieder auf der Administrationsseite. Dabei bieten moderne CMS-Systeme neben der Kartenverwaltung noch einen weiteren Vorteil und erledigen durch einen Work Flow orientierten Ansatz auch gleich das Zertifikatsmanagement mit. In einigen Szenarien kann daraus sogar eine sehr praktikable Identity Management Lösung entstehen, daher sollte man das Kartenmanagement nicht nur als lästiges Übel das mit der Ausgabe von Smart Cards einher geht betrachten, sondern dessen volles Potential ausnutzen. Beispielsweise können dabei unterschiedliche Berechtigungen beliebig definierbaren Rollen zugeteilt werden (Bild 1), mit denen sich ein Ausstellungsprozess auch sehr einfach und

administrator, etc.). Wenn dies erfolgt ist, kann der Benutzer auch per E-Mail oder SMS zum Abholen seiner neuen Karte aufgefordert werden.

Der Einfachheit halber könnte die eigentliche Kartenproduktion von einem zentral liegenden Sekretariat erledigt werden, wo ein Kartendrucker mit eingebautem Kartenleser steht. In nur ganz wenigen Schritten wird eine neue Karte initialisiert, entsprechend der für den Benutzer geltenden Policy die neuen Zertifikate auf der neuen Karte aufgebracht (Bild 4) und gleich nach der definierten Vorlage bedruckt (Bild 5). Wenn Key Archival konfiguriert wurde muss eine bestimmte vertrauenswürdige Person diesen Recovery Vorgang bezeugen, um Missbrauch vorzubeugen.

Mit vergleichbaren Abläufen können auch temporäre Ersatzkarten ausgestellt werden, welche die ursprünglichen Zertifikate nicht gleich komplett widerrufen sondern nur aussetzen. Wenn die Karte wieder auftaucht, wird sie einfach wieder reaktiviert, was zu einer Wiederaufnahme der betroffenen Zertifikate führt.

„Datenverschlüsselung braucht ein Sicherheitsnetz, sonst sperrt man sich sehr schnell selbst aus!“

natur geht. Daher wird in der Regel auch mit mehreren Zertifikaten pro Benutzer gearbeitet. Sicherheitsfanatiker teilen die Anwendungen Authentifizieren, Signieren und Verschlüsseln auf drei unterschiedliche Zertifikate mit unterschiedlichen Policies auf, während für viele Anwendungen auch die Separierung auf zwei (Verschlüsselung und den Rest) ausreichen sollte. Dem Verschlüsselungszertifikat wird dabei das Key Archival erlaubt. Langer Rede kurzer Sinn: mit dem einen „Smart Card User“ Zertifikat werden Sie möglicherweise nicht das Auslangen finden, ergo steigt der Administrationsaufwand.

Zertifikats- oder Kartenmanagement?

Um einen Card Management Server (CMS) werden Sie somit kaum her-

unkompliziert auf mehrere Verantwortlichkeiten gemäß dem definierten Genehmigungsverfahren verteilen lässt.

Veranschaulichen lässt sich so ein Vorgang wieder am besten anhand eines Beispiels. Der Anwender mit dem Namen Tester kann sich auch ohne Karte am Portal anmelden (Bild 3) und stellt über ein in der Anwendung sehr einfach gehaltenes Web-Interface beispielsweise den Antrag auf Ausstellung einer Ersatzkarte, weil seine defekt geworden ist (Bild 2). Anhand der vergebenen Rechte werden auch nur die relevanten Optionen abgefragt, um den Prozess so einfach wie möglich zu halten. Daraufhin werden sofort alle auf der Karte befindlichen Zertifikate widerrufen und der Antrag durch den Genehmigungsprozess geleitet (Freigabe durch einen Manager, Ad-

Kartenausgabe als ernste Herausforderung

Die Kartenausgabe kann je nach Unternehmensgröße viele unterschiedliche Ausprägungen annehmen. Der vorhin beschriebene Einzelmodus ist im Normalfall nur für den operativen Betrieb und für kleine Installationen sinnvoll. Danach erweist sich ein Batch-Modus als adäquat, bei dem gleich ganze Benutzergruppen auf einmal beantragt, freigegeben und produziert werden. Rechnen Sie mit einem Zeitbedarf von mindestens zwei bis drei Minuten je Karte für die Produktion in einem handelsüblichen Drucker. Da dies auch ohne Benutzerinteraktion abläuft, kann die Herstellung auch über Nacht weiterlaufen. Wenn jedoch wirklich größere Mengen produziert werden sollen, wird man auf die Anlagen von professionellen Kartenherstellern zurückgreifen müssen.

Diese ausgelagerte Produktion sollte auch aus Kostengründen unterstützt werden, da so die Druckkosten geringer gehalten werden und die Produktionsdauer erheblich verkürzt wird. Wenn Sie zum Beispiel 30.000 Karten händisch anfertigen, benötigen Sie dafür in etwa ein halbes Mannjahr. Daher sind USB-Token in großen Anwendungen auch abgesehen vom Preis mit etwas Vorsicht zu genießen, weil eine Masseninitia-

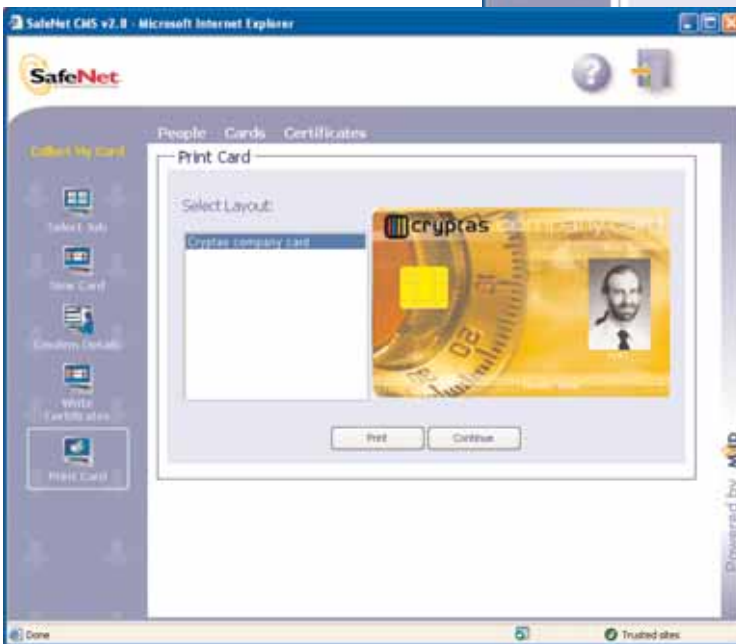
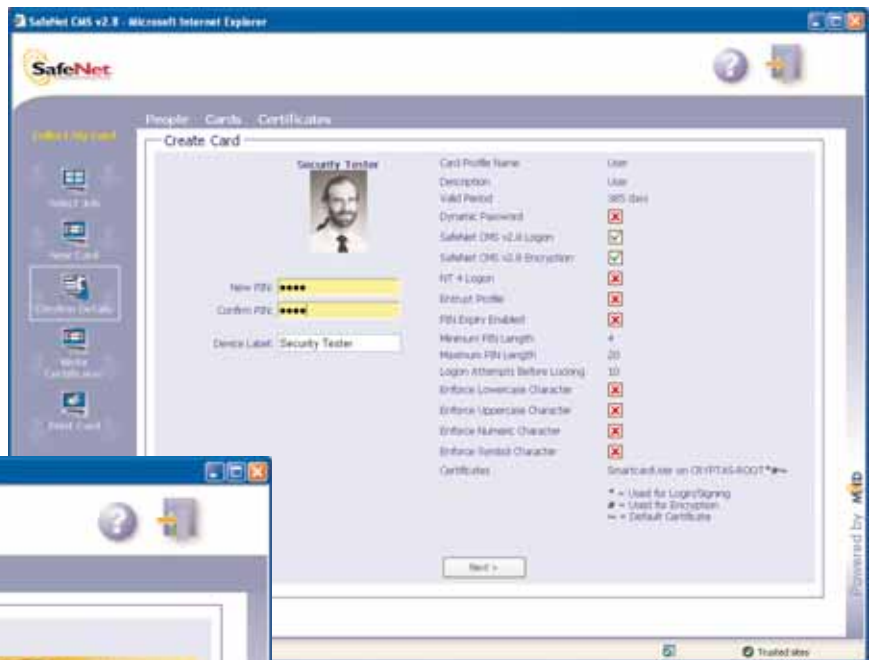


Bild 5: Auf Knopfdruck fällt aus dem Drucker eine fertig bedruckte und mit Zertifikaten bespielte Karte.

Bild 4: Im Sekretariat ist der Job nach der Genehmigung eingegangen und eine neue Karte wird entsprechend der vordefinierten Policies ausgestellt.

lisierung sehr kompliziert wird. Abgesehen davon können bedruckte Karten in Form eines Mitarbeiterausweises sehr einfach einer Person zugeordnet werden, aber stellen Sie sich einmal eine Kiste mit 30.000 USB-Token vor, die alle gleich aussehen!

Worauf man bei der Auswahl achten sollte

In der Regel wird aus der Karte gleich ein Mitarbeiterausweis, welcher drei Funktionen erfüllen kann: Zutritt, Zeiterfassung und Kantinenabrechnung über ein kontaktloses Interface, IT-Sicherheit über die kontaktbehaftete Schnittstelle und natürlich Sichtausweis. Die Informationen

dafür kommen oft auch aus drei unterschiedlichen Quellen. Klassische Zutrittslösungen verwalten ihre Karten und Berechtigungen in einer eigenen Datenbank. Die Zusatzinformationen für die Funktion Sichtausweis können in einem Human Resource-System liegen und gehen wir mal beim IT-Part von einem X.500-Verzeichnis (wie dem Active Directory) aus. Für die zu wählende Lösung sollte es unbedingt möglich sein, alle diese Systeme zu integrieren, damit der Aufwand so gering wie möglich gehalten wird und eine Ausstellung auf Knopfdruck erfolgen kann. Die Verteilung der Karten und der Karten PINs sollte flexibel gestaltbar sein. Eine automatische Verständigung über die fertige Karte per E-Mail und die

Zusendung des PINs in einem eigenen Brief ist vielfach eine harte Anforderung. Auch die Flexibilität bei den Freigaben von Karten- oder Zertifikatsanträgen über spezielle Rollen oder einfach über Bezeugung anderer Benutzer (Mehraugenprinzip) kann viele organisatorische Hürden überwinden. Nicht zu vergessen die Möglichkeit der redundanten Ausführung mit Fail-over Fähigkeiten!

Microsoft hat bereits in Windows XP und Windows Server 2003 mit den vorhandenen Smart Card Unterstützungen einen wesentlichen Schritt zur sicheren Benutzerauthentifizierung in der breiten Masse gesetzt. Smart Cards sind nicht mehr nur für eine elitäre Gruppe von Großunternehmen, die sich eine enorme Anpassungsentwicklung leisten können, realisierbar. Mit Standardmitteln kommt man sehr weit. Einer der wichtigsten Teile fehlt jedoch noch und muss mit Produkten von Drittherstellern abgedeckt werden: das Management der Karten!

Stefan Bumerl
stefan.bumerl@cryptas.com