

ALLES IN EINER, EINE FÜR ALLES

Die Entwicklung einer Public-Key-Infrastructure (PKI), die höchsten Sicherheitsanforderungen entspricht, erfordert die Nutzung bestmöglicher Technologien. Wenn die Umsetzung dieser Herausforderung auch noch den Alltag der Mitarbeitenden erleichtert, darf man von einer gelungenen Lösung sprechen. Die Multifunktionskarte der Schweizerischen Post vereint gleichzeitig Personalausweis, Zutrittsbadge für Türkontrolle, starke Authentisierung (Pin und physische Karte) für Windows-Login, Zeiterfassung und Bargeld für Kaffeeautomate, Personalrestaurant und Parking. Mehr noch: die auf die Post zugeschnittene Lösung mit internem Registrierungsmanagement ist ein Novum auf dem Markt. Die Multifunktionskarte der Post ist eine gemeinsame Entwicklung der Informationstechnologie Post, PostFinance, SwissSign und Trivadis.

HERAUS- FORDERUNG

Als Finanzdienstleister steht PostFinance in der Pflicht, höchste Sicherheitsanforderungen zu erfüllen. Dazu wird eine starke Authentisierung beim Zugriff auf Applikationen verlangt. Gleichzeitig bestehen auf Seite der Post Bestrebungen, den Mitarbeiter-Batch aktuellen Begebenheiten anzupassen. Zusätzlich sollten aus Sicherheitsgründen Maschinen-Zertifikate (Wireless Lan, Webserver, Domain Controller etc.) vergeben werden können.

DAS PROJEKTZIEL

Realisation einer Smartcard mit starker Authentisierung für PostFinance und einer internen Public-Key-Infrastructure

TECHNOLOGIEN & PRODUKTE

Microsoft .Net Framework 3.5, Spring Framework 1.1.0.2, BouncyCastle.Crypto 1.3.00, Novell.directory.Idap Version 2.1.10.0

KUNDE & BRANCHE

Die Schweizerische Post, Öffentlicher Sektor, Bankenbranche

Alle 29 Tage das persönliche Passwort wechseln, unterschiedliche Log-ins und Passwörter für verschiedenste Applikationen - wer kennt sie nicht die Tücken des heutigen Büroalltags. Darunter leidet nicht nur der Anwender, sondern auch die Sicherheit. Bei der Menge an unterschiedlichen Passwörtern verfällt der Mitarbeiter leicht in einfache Abwandlungen des Ausgangspasswortes oder vergisst selten gebrauchte Passwörter. Das zieht erhöhten Ressourcenaufwand mit sich und beschäftigt Systemtechniker und Administratoren. Mit dieser kombinierten Multifunktionskarte fallen viele dieser Probleme auf einen Schlag weg, denn der User muss sich nur einen Pin merken. Dieser erlaubt erst in Kombination mit der Karte selbst den Zugriff zum Windows-Desktop und den einzelnen Applikationen - sicherer und einfacher als mit jedem Passwort. Zusätzlich zu dieser starken Authentisierung vereint die Karte auch die Post-ID (Sichtausweis und Zutrittsberechtigung inklusive Zeiterfassung), bargeldloses Bezahlen an Verpflegungsautomaten, Personalrestaurant und im Parking. Die Karte kann auch biometrische Daten enthalten, die zur erweiterten Zutrittsberechtigung verwendet werden können. Ein nächster Schritt sieht die Nutzung der Karte für die Verschlüsselung von Harddisks und Emails sowie die Signatur von Dokumenten vor.

Starke
Authentisierung
(PostFinance)

Mitarbeiterausweis
(Post)

Zertifikate für Maschinen
(Informationstechnologie
Post)

Verschiedene Herausforderungen stellten sich dem wegweisenden Projekt auf der technischen, aber auch organisatorischen Ebene:

- Eine solche Kombination von starker Authentisierung (Zertifikat) mit Mitarbeiterausweis gibt es nicht „out of the box“ auf dem Markt.
- Die Multifunktionskarte muss nicht nur unterschiedliche Chips auf der gleichen Karte vereinen, sie muss auch alltagstauglich und robust sein (mechanische und thermische Festigkeit).
- Zertifikatsmanagement:
 - Die Überprüfung der Gültigkeit der Zertifikate muss auch bei einem Ausfall der Internetverbindung sichergestellt werden
 - Zertifikate sollten sowohl für Personen als auch Maschinen ausgestellt werden können.
 - Zertifikate müssen öffentlich anerkannt sein, damit auch mit externen Partnern sicher und vertrauenswürdig kommuniziert werden kann.
- Die Ausbaufähigkeit muss gewährleistet werden (Standards müssen eingehalten werden).
- Die technische (Betriebssicherheit) und organisatorische Sicherheit (Rollen, Verantwortung und Funktionen) muss sichergestellt werden. Für ein internes Registrierungsmanagement müssen die Ausstellungsprozesse hohen Anforderungen entsprechen.
- Projektkoordination von mehreren involvierten Abteilungen und Unternehmen
- Das Lifecycle Management muss bei vergessenen oder verlorenen Karten funktionieren, damit Mitarbeiter trotzdem arbeiten können.

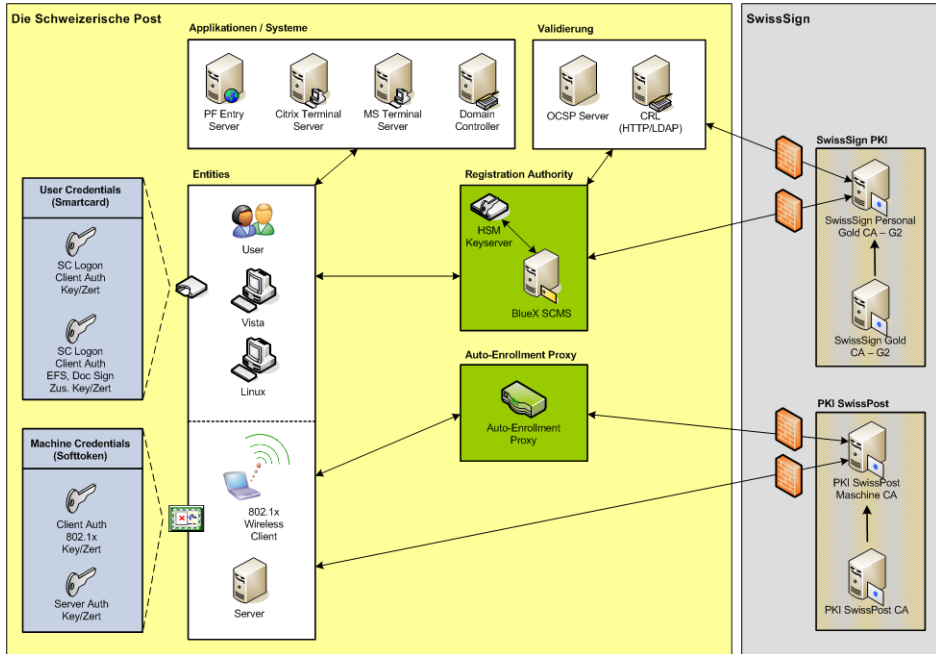
**DIE LÖSUNG:
MEISTERN DER
HERAUSFORDERUNG**

Eine ausführliche Analyse der Informationstechnologie Post ergab, dass zu vergleichbaren Kosten keine selbstentwickelte Public-Key-Infrastructure Lösung auf gewünschtem Niveau erstellt werden könnte. SwissSign, eine Tochterfirma der Post, erfüllte alle Voraussetzungen für die Bereitstellung dieser Infrastruktur als Managed PKI-Lösung. SwissSign besitzt zudem eine eigene Zertifizierungssoftware (CA-Software), die schnell flexible Anpassungen und Erweiterungen erlaubt. Zusätzlich wurde mit Trivadis AG ein erfahrener Anbieter von IT-Lösungen und -Dienstleistungen für die Gesamtprojektleitung hinzugezogen. Gemeinsam wurde eine Lösung entwickelt, welche die unterschiedlichen Anforderungen optimal erfüllt. Die Schnittstelle zwischen SwissSign als CA-Lieferant und der Post spielt dabei eine zentrale Rolle.

Drei Neuentwicklungen tragen dabei zum Erfolg bei:

- **Schnittstelle BlueX-SCMS / SwissSign-CA:**
 - Schnittstellenerweiterung am Smartcard Management System (BlueX SCMS)
 - BlueX übernimmt RA-Funktion (Personen-Zertifikate)
- **CRL-Publisher:** Die Eigenentwicklung von Trivadis ermöglicht es, die Zertifikatssperreliste (CRL) Post intern zu publizieren und periodisch zu aktualisieren. Somit kann die Überprüfung der Gültigkeit von Zertifikaten unabhängig von einer Verbindung zum Internet sichergestellt werden und garantiert so höchste Verfügbarkeit.
- **Rollout von Client-Zertifikaten:** In einer ersten Phase werden Maschinen-Zertifikate für Windows-Clients manuell mittels einer eingerichteten Webapplikation ausgestellt. Dies ist bei der noch relativ kleinen Anzahl von Clients sinnvoll. Zu einem späteren Zeitpunkt, wenn auch die Anzahl der einzurichtenden Maschinen um ein Vielfaches höher sein wird, werden diese Zertifikate automatisch generiert werden: mit einer selbst entwickelten Applikation, dem „Auto Enrollment Proxy“.

Die ausgestellten Personen-Zertifikate entsprechen dem SwissSign Gold CA Standard. Für die Erfüllung dieser qualitativ hochwertigen Standards werden hohe Anforderungen an die Registrierung der Personen und interne Prozesse gestellt. Für die Maschinenzertifikate wurde eine eigene CA Infrastruktur (PKI Swiss Post) aufgebaut.



DER NUTZEN

Dank einer sauberen Projektorganisation und –management konnte das komplexe Projekt innert Jahresfrist umgesetzt werden. Mit dieser ersten Implementierung für PostFinance sind ideale Voraussetzungen geschaffen worden, um auch weitere Organisationen der Post erfolgreich integrieren zu können.

Die Vorteile der Multifunktionskarte liegen auf der Hand:

- Die Multifunktionskarte kann beliebig ausgebaut werden. Beim Projekt wurde von Anfang an darauf geachtet, dass gängige Standards eingebaut werden. Auch für eine Ausweitung der Maschinenzertifikate auf weitere Endgeräte der Post (Telefone, Handscanner etc.) sind alle Voraussetzungen geschaffen worden.
- Neben der Vereinfachung des Arbeitsprozesses für die Mitarbeitenden gibt die Kombination von Zutrittsbadge, Zugang zu Workstation und Vending-Funktionalität der Karte einen hohen psychologischen Wert: Denn ohne sie läuft nichts mehr.
- Die verwendeten Zertifikate von SwissSign bürgen für höchste Qualität. Sie sind öffentlich und durch ihren hohen Standard in allen gängigen Browsern eingebaut. Daher ist auch ein sicherer Datenverkehr mit Kunden und Partnern ausserhalb der PKI möglich. Das ist ein grosser Vorteil für sichere E-Mail-Kommunikation und Signaturen.

DIE MULTI-FUNKTIONS-KARTE

Die Karte kann mittels Smartcard-Reader in jeden Computer eingelesen werden. Die Karte selbst ist mit einem PIN vor unbefugter Verwendung geschützt (analog Postcard, EC etc.). Die Multifunktionskarte vereint gleichzeitig Personalausweis, Zutrittskontrolle, starke Authentifizierung für Windows-Login, Zeiterfassung, Bargeld für den Kaffeeautomaten und Garagenbenutzung. Sie ist beliebig ausbaubar.

Das Konto auf der Karte kann am Automaten mit Münzen/Noten oder bargeldlos am Verkaufspunkt (EFT/POS) wieder aufgeladen werden.

QUOTES

Urs Brunner, Post: „Die erarbeitete Lösung ist so auf dem Markt nicht zu finden. Wir sind stolz, als erste unseren Mitarbeitern nicht nur eine vielseitige Multifunktionskarte anzubieten, sondern auch höchste Sicherheitsstandards zu erfüllen.“

Stefan Beyeler, Trivadis: „Als Gesamtprojektleiter bin ich auf ein motiviertes und professionelles Projektteam, auf eine optimale Projektorganisation und auf die Unterstützung des Auftraggebers angewiesen. Dank der ausgezeichneten Zusammenarbeit aller Beteiligten konnte ich das Projekt erfolgreich zum Abschluss bringen.“

Gion Manetsch, Informationstechnologie Post: „Die Schwierigkeit einer internen Zertifizierungsstelle liegt nicht in der Ausstellung von Zertifikaten, sondern in der Anpassung der internen Prozesse an geforderte Qualitätsstandards. SwissSign überzeugt als CA-Anbieterin nicht nur mit kurzfristiger Programmierung und Anpassung von Softwareapplikationen, sondern auch mit hoher Fachkompetenz.“

Mike Doujak, SwissSign: „Die gemeinsam mit Informationstechnologie Post und Trivadis entwickelte Lösung ist einzigartig und trotzdem einfach auf jede Firma anzuwenden.“

PROJEKTFAKTEN

- Auftraggeber (Übersicht): PostFinance ist ein eigenständiger Geschäftsbereich der Schweizerischen Post und erbringt seit 1906 den flächendeckenden Zahlungsverkehr in der Schweiz. Seit 1997 hat sich PostFinance von der Nummer eins im Schweizer Zahlungsverkehr zum umfassenden Finanzinstitut entwickelt.
- Projektziel: Realisation einer Smartcard mit starker Authentisierung für PostFinance und einer internen Public-Key-Infrastructure
- Involvierte Partner:
 - Trivadis: Trivadis entwickelt praxisgerechte und massgeschneiderte Sicherheitslösungen. Trivadis unterstützt sowohl bei der Sicherheitsstrategie und der dazugehörigen Prozesse als auch im Design, der Implementierung und der Evaluation von Sicherheitstechnologien.
 - Informationstechnologie Post: Der Bereich Informationstechnologie sorgt für den wirtschaftlichen Betrieb der Informatik-Infrastruktur. Als innovativer Partner entwickelt und realisiert er konzernweit massgeschneiderte IT-Lösungen mit dem Ziel die Kunden im IT-Bereich umfassend, nachhaltig und wirkungsvoll zu unterstützen.
- SwissSign: SwissSign, ein Unternehmen der Schweizerischen Post, macht kompromisslose Sicherheits- und Identitätstechnologie made in Switzerland anwendbar für den täglichen Gebrauch.
- Leistung: PKI-Consulting, Lieferant CA, Customizing CA Services
- Projektdauer: Das Projekt wurde im September 2007 initialisiert und dauerte bis Ende September 2008.
- Eingesetzte Technologie:
 - Trivadis: Microsoft .Net Framework 3.5, Spring Framework 1.1.0.2, BouncyCastle.Crypto 1.3.0.0, Novell.directory.Idap Version 2.1.10.0
 - SwissSign: Open Source (Linux, Apache, SQL, OpenSSL, Openend-Up) und Eigenentwicklungen
 - Informationstechnologie Post: Chip: Java Chip Philips, Middleware: AET, SCMS: BlueX (AET), Kartenleser: Omnikey (Desktop), Laptops (Gemplus) bereits eingebaut

www.trivadis.com, info@trivadis.com, Info-Tel. 0800 874 823 47

