Bit4id erweitert elektronisches ID-Kartensystem im Nahen Osten mit eIDAS-konformem digitalem Online-ID-System mit Entrust HSMs

Bit4id entwickelt einfache, sichere und standardisierte Technologien für Authentifizierung, digitale Signaturen und Kryptographie. Der Hauptsitz des Unternehmens ist in Italien, mit Niederlassungen in Ecuador, Indien, Macao, Peru, Portugal, Spanien und dem Vereinigten Königreich.

Das Bit4id-Konzept: So wie die physische Identität einer Person einzigartig und universell erkennbar ist, sollte auch die digitale Identität dieser Person einzigartig sein und sie in Computernetzwerken und im Internet sicher repräsentieren können. Außerdem können digitale Identitätsprogramme nur dann erfolgreich sein, wenn sie einfach, sicher und natürlich zu bedienen sind – sowohl für die Unternehmen, die sie verwalten, als auch für die Personen, die sie nutzen.

> **„Entrust nShield HSMs sind der weltweite Standard. Wir entwickeln Projekte aufgrund der herausragenden Zuverlässigkeit und Verfügbarkeit von Entrust nShield HSMs und integrieren sie in alle unsere Produkte. Wir vertrauen sowohl der Marke Entrust als auch ihren Produkten vorbehaltlos."**
>
> – Pierluigi Pilla, ID Systems and PKI Unit Director bei Bit4id

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Bit4id

GESCHÄFTLICHE PROBLEMSTELLUNG

Im Rahmen einer Arbeitsgemeinschaft von Systemintegratoren wurde Bit4id vom Informationsministerium (MIT) eines Landes im Nahen Osten beauftragt, eine mobile digitale Identitätslösung für die gesamte Bevölkerung, einschließlich der Bürger und Nicht-Bürger des Landes, bereitzustellen. Das Land verfügte bereits über ein elektronisches ID-Karten-(Mikrochip-) System, doch das MIT wollte dieses System durch eine IT-Infrastruktur ergänzen, um digitale IDs im Cyberspace zu erzeugen und zu verwalten – nach dem Vorbild und in Übereinstimmung mit der Verordnung der Europäischen Union (EU) über elektronische Identifizierungs- und Vertrauensdienste (eIDAS). Die Verwendung des eIDAS-Modells würde nicht nur einen Best-Practice-Ansatz gewährleisten, sondern auch den Handel mit der EU und anderen Ländern, die diesen Standard einhalten, ermöglichen.

TECHNISCHE PROBLEMSTELLUNG

PKIs, digitale Zertifikate und digitale Identitäten

Die öffentliche Schlüsselinfrastruktur (public key infrastructure, PKI) ermöglicht die Identifizierung von Personen, Geräten und Diensten, sodass der kontrollierte Zugriff auf Systeme und Ressourcen, der Schutz von Daten und die Rechenschaftspflicht bei Online-Transaktionen gewährleistet sind. Die PKI ist die Basis für die Verwendung von Technologien wie digitale Signaturen und Verschlüsselung in großen Benutzergruppen. Folglich sind PKIs für sichere und vertrauenswürdige Regierungstransaktionen und den elektronischen Handel unerlässlich.

Digitale Zertifikate

Digitale Zertifikate bilden die Credentials, welche die Überprüfung der Identitäten zwischen Benutzern in einer Transaktion erleichtern. Ähnlich wie ein Reisepass die Identität einer Person als Bürger eines Landes bescheinigt, stellt das digitale Zertifikat die Identität der Benutzer innerhalb des Ökosystems fest. Da digitale Zertifikate zur Verifizierung der Identität des Unterzeichners von Informationen verwendet werden, ist der Schutz der Authentizität und Integrität des Zertifikats unerlässlich, um die Vertrauenswürdigkeit des Systems aufrechtzuerhalten.

Zertifizierungsstellen

Eine Zertifizierungsstelle (Certificate Authority, CA) ist die wichtigste Komponente einer PKI, die für den Aufbau einer hierarchischen Vertrauenskette zuständig ist. CAs stellen die digitalen Berechtigungsnachweise aus, die zur Zertifizierung der Identität von Benutzern und zur Gewährleistung der Sicherheit einer PKI und der von ihnen unterstützten Dienste verwendet werden. Die physischen und logischen Kontrollen und Abwehrmechanismen eines Hardware-Sicherheitsmoduls (HSM) gewährleisten die Integrität einer PKI und mindern das Risiko eines Angriffs.

eIDAS

eIDAS ist eine EU-Verordnung, die Standards für elektronische Identitäten, Authentifizierung und Signaturen festlegt. Sie bezieht sich auf Regierungsstellen und Unternehmen, die Online-Dienste für europäische Bürger anbieten und die Identitäten, Authentifizierung oder Signaturen erkennen oder verwenden. eIDAS erfordert auch die Verwendung von nach Common Criteria EAL4+ (AVA_VAN.5) zertifizierten HSMs, um digitale Zertifikate, digitale Signaturen, Zeitstempel und andere Transaktionsdaten auszustellen.

Systemanforderungen

Das MIT verfügte bereits über eine PKI, um seinen Bürgern elektronische Ausweise auszustellen. Bit4id hatte die Aufgabe, zusätzliche Leistungsmerkmale in die PKI zu integrieren:

- Bürger sollten die Möglichkeit haben, Transaktionen und Dokumente sowohl von Desktop- als auch von mobilen Geräten wie digitalen Notebooks, Tablets und Smartphones aus digital zu unterzeichnen

Bit4id

- Einfache Skalierung
- Ausstellung von Zertifikaten für Millionen von Benutzern
- Verarbeitung von Tausenden von Transaktionen pro Sekunde

LÖSUNG

Ein wichtiger Grund, warum das MIT dieses Projekt an Bit4id vergab, war deren Vorschlag, Mobilzertifikate in einem Entrust nShield® HSM zu speichern, das nach Common Criteria EAL4+ zertifiziert ist, und nicht auf dem Gerät selbst, wie etwa einem Mobiltelefon. Dies würde den eIDAS-Bestimmungen bezüglich digitaler Fern-Zugangsdaten entsprechen. Da Bit4id in Sachen eIDAS-Konformität sehr versiert ist, wusste das Unternehmen, wie man das System zum Laufen bringt.

Das eigens vom Unternehmen entwickelte digitale Identitätssystem erleichtert den Verkehr zwischen der nationalen PKI, den Entrust nShield HSMs und den Einwohnern des Landes im Nahen Osten, das das System nutzt. Das System verwaltet die sichere Ausstellung von Zertifikaten durch die nationale PKI an das HSM, regelt die Verwendung von Zertifikaten vom HSM für Benutzer und steuert die Verwaltung des Lebenszyklus von Zertifikaten (z. B. Aussetzung, Widerruf, Erneuerung). Zertifikate sind erforderlich, um die Benutzer innerhalb des Systems zu identifizieren und zu authentifizieren und dann Dokumente in verschiedenen staatlichen Anwendungen zu unterzeichnen, wie z. B. bei der Eröffnung eines Unternehmens, der elektronischen Einreichung der Einkommenssteuer oder beim Unterzeichnen und Hochladen von Dokumenten für die juristische Korrespondenz.

Bei der Bereitstellung wird derzeit die SignCloud-Lösung von Bit4id zusammen mit der ergänzenden Middleware-Anwendung Universal Key Chain und insgesamt vier nShield Connect XC HSMs verwendet: eines für die Entwicklung, eines für Tests und zwei für die Produktion, einschließlich eines Failover-Mechanismus. Dies sorgt für hohe Verfügbarkeit und Lastausgleich für einen reibungslosen Ablauf. Bit4id machte sich auch die einzigartige Security World-Architektur von Entrust zunutze, die es ermöglicht, Schlüssel als verschlüsselte und geschützte Dateien außerhalb der physischen Grenzen des HSM zu speichern. Dies bietet praktisch unbegrenzten Schlüsselspeicher.

Das derzeitige digitale ID-System wird in erster Linie für behördliche Anträge für Bürger verwendet. Allerdings ist geplant, den derzeitigen Einsatzbereich zu replizieren, um weitere Anwendungsfälle zu ermöglichen, bei denen digitale Signaturen in Anwendungen von Regierung zu Unternehmen und von Regierung zu Regierung eingesetzt werden.

„Bit4id arbeitet seit vielen Jahren mit Entrust und verwendet deren nShield HSMs“, sagt Pierluigi Pilla, ID Systems and PKI Unit Director bei Bit4id. „Entrust HSMs sind der weltweite Standard. Wir entwickeln Projekte aufgrund der herausragenden Zuverlässigkeit und Verfügbarkeit von Entrust nShield HSMs und integrieren sie in alle unsere Produkte. Wir vertrauen sowohl der Marke Entrust als auch ihren Produkten vorbehaltlos.“

Bit4id

Geschäftliche Anforderungen

Erstellung eines digitalen Online-ID-Systems, das ein bestehendes elektronisches Ausweissystem ergänzt und mit eIDAS kompatibel ist

Technische Anforderungen

Integration zusätzlicher Infrastruktur in die bestehende PKI, die Folgendes ermöglicht:

- Bürgern die Option bieten, von Desktop- und Mobilgeräten wie digitalen Notebooks, Tablets und Smartphones aus digital zu unterschreiben
- Einfache Skalierung
- Ausstellung von Zertifikaten für Millionen von Benutzern
- Verarbeitung von Tausenden von Transaktionen pro Sekunde

Lösungen

Benutzerdefinierte Gestaltung eines digitalen ID-Systems mit:

- Bit4id SignCloud
- Bit4id Universal Key Chain
- Entrust nShield Connect HSM
- nShield Security-World-Architektur

Ergebnisse

- Aufbau eines nationalen mobilen digitalen ID-Systems
- Erfüllt die geschäftlichen, technologischen und Sicherheitsanforderungen des Kunden
- Solides System, das demnächst dupliziert und auf andere Anwendungsfälle erweitert wird

ERGEBNISSE

Bit4id entwickelte ein eIDAS-kompatibles mobiles digitales ID-System, das das bestehende elektronische Ausweissystem des Nahost-Landes ergänzt. Das System:

- Ermöglicht Bürgern digitale Signaturen sowohl von Desktop- als auch von mobilen Geräten
- Ermöglicht einfache Skalierung
- Ermöglicht die Ausstellung von Zertifikaten für Millionen von Benutzern
- Ermöglicht die Verarbeitung von Tausenden von Transaktionen pro Sekunde
- Soll dupliziert und auf Anwendungen von Regierung zu Unternehmen und von Regierung zu Regierung ausgeweitet werden

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com