keyon

Migros-Genossenschafts-Bund (MGB)

Success Story

Automatisierte Ausgabe und Verwaltung von Benutzerzertifikaten

Nahtlose Integration in Identitätsmanagement Prozesse

Parallelintegration einer Microsoft CA und Public CA

Enterprise PKI

Der Migros-Genossenschafts-Bund setzt im Rahmen der Erneuerung der Windows Arbeitsplätze auf zertifikatsbasierte Authentisierung und Verschlüsselung. Im Fokus lag die vollständig automatisierte Ausgabe und Verwaltung der Benutzerzertifikate sowie ein rollenbasiertes Cockpit für Prozesse und Statusabfragen.

Bei der Erneuerung des unternehmensweiten Identitätsmanagements (IdM) sowie der Aktualisierung aller Windows Arbeitsplätze setzte das Grossunternehmen auf ein Optimum an Sicherheit, Verwaltung und Komfort. Kurz gesagt, „ein M besser“ in puncto Sicherheit und Komfort im Bereich der Zertifikatsverwaltung.

Ziel war es, alle Arbeitsstationen mit Authentisierungs- und Verschlüsselungszertifikaten automatisiert auszustatten. Dies erfolgte mit der true-Xtender Suite von Keyon sowie der Parallelintegration einer Microsoft CA und einer öffentlichen CA.

Keyon unterstützte den MGB bei der Konzipierung und Umsetzung der Lösung wie auch beim Support in der produktiven Nutzung.

Der Kunde

Der Migros-Genossenschafts-Bund mit Sitz in Zürich nimmt diverse Aufgaben innerhalb der Migros wahr. Er bildet gemeinsam mit den zehn Genossenschaften, der Eigenindustrie, den Dienstleistungsunternehmen sowie den weiteren zugehörigen oder nahe stehenden Betrieben, Organisationen und Stiftungen die Migros-Gruppe.

www.migros.ch

Anforderung

Mit der Einführung eines neuen, unternehmensweiten Identitätsmanagements sowie der Erneuerung aller Windows Arbeitsplätze des MGB sollte die bestehende PKI durch eine neue PKI abgelöst werden. Hierbei mussten die bestehenden Benutzerzertifikate automatisiert und sicher mit neuen Zertifikaten ersetzt werden, ohne dass die Benutzer in ihrer Arbeit beeinträchtigt werden. Die Benutzer sollten im gleichen Arbeitsschritt unternehmenseigene- wie auch öffentliche Zertifikate bereitgestellt bekommen. Zudem wurde ein umfangreiches Life-Cycle Management der Zertifikate sowie aussagekräftige Reports über Prozessfortschritte und Systemzustände gefordert.

Die Zertifikate sollten entsprechend von Active Directory Richtlinien und MGB-spezifischen Regeln automatisch ausgestellt, erneuert und revoziert werden. Ebenfalls soll der Prozess den Zertifikatsstatus im Falle von Namensänderungen, Abteilungswechseln, Austritten von Personen oder der Dekommissionierung von Geräten automatisch aktualisieren.

Lösung

Keyon war verantwortlich für die technische und organisatorische Umsetzung aller PKI basierten Prozesse. Auf Basis der true-Xtender Suite von Keyon wurde

- die alte Microsoft PKI des MGB mit einer neuen Microsoft PKI abgelöst;
- die Zertifikatsausgabe und -verwaltung über das Identitätsmanagement gesteuert;
- die öffentliche CA der QuoVadis Trustlink Schweiz AG parallel zu der Microsoft CA integriert;
- ein web-basiertes Cockpit bereitgestellt, das, abhängig von den jeweiligen Rollen, unterschiedliche administrative Tätigkeiten erlaubt oder Prozess-Stati anzeigt.

Keyon unterstützte den MGB mit technischem und organisatorischem Know-how bei der Spezifikation, Implementierung und Integration. Zudem stellte Keyon über fortwährenden Know-how Transfer und gezielten Schulungen sicher, dass die MGB die Lösung effizient und eigenständig betreiben kann.

Durch die Automatisierung der technischen Prozesse wurde der Aufwand für die Ausstellung und Verwaltung der Zertifikate auf ein Minimum reduziert. Die innovative Lösung wurde Kosten- und Termingerecht eingeführt. Sie zeichnet sich insbesondere durch folgende Eigenschaften aus:

- Full Certificate Life-Cycle

  Flexibles und dynamisches Microsoft Autoenrollment von öffentlichen- und internen Zertifikaten;

- Key History

  Automatische Verwaltung und Import der Key-History der Verschlüsselungszertifikate auf den Endgeräten;

- Integration des Quest One Identity Managers

  Regelwerk und Prozesssteuerung über das Identitätsmanagement;

- Umfangreiches Cockpit

  Web-basiertes Cockpit, über das rollenbasiert administrative Tätigkeiten oder Statusabfragen ausgeführt werden können.