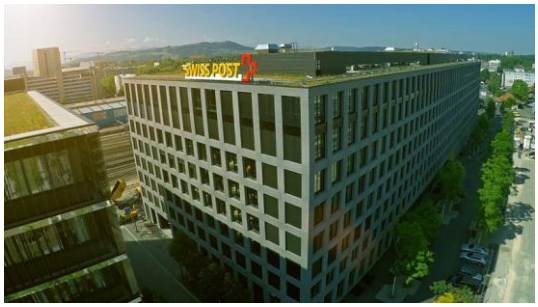
SECARDEO

Anwenderbericht

Absolut zuverlässig: Post CH AG optimiert Autoenrollment digitaler Zertifikate mit Secardeo GmbH

certEP übernimmt als Autoenrollment Proxy die Vermittlung zwischen Windows Clients und externer Zertifizierungsstelle

Post CH AG
In sechs Geschäftssparten, PostMail, Swiss Post Solutions, PostNetz, PostLogistics, PostFinance und PostAuto, ist die Post CH AG mit über 58.000 MitarbeiterInnen eine der größten Arbeitgeberinnen der Schweiz. Neben der Sicherung der postalischen Grundversorgung arbeitet das Unternehmen konsequent an der Umsetzung ihrer physisch-digitalen Transformationsstrategie. Die Post CH AG hat es sich zum Ziel gesetzt, durch Kundenfokus, als Systemanbieter und unter dem Kredo der Einfachheit die physische und digitale Welt zu verbinden und mit ihren Produkten und Systemlösungen neue Maßstäbe zu setzen.



Herausforderung und Zielsetzung
Um im internen und externen Datenaustausch sensible Inhalte effektiv zu schützen sowie den Kommunikationspartner verlässlich zu identifizieren, sind digitale Zertifikate innerhalb einer PKI (Public Key Infrastructure) das Mittel der Wahl. Es gilt Identitäten vor Fälschung und Missbrauch zu schützen und zentral zu verwalten.

Während die Zertifikatsprüfung durch die üblichen Programme wie Thunderbird oder MS Outlook für signierte E-Mails oder Firefox oder Internet Explorer für SSL-Zertifikate automatisch erfolgt, liegt ein Problemfeld im automatisierten Zertifikatsmanagement. Sollte nur eine geringe Menge an Zertifikaten im Einsatz sein, ist ein manuelles Management noch vorstellbar; bei einer größeren Anzahl bedarf es einer Lösung, die mehr leistet als das schlichte Bereitstellen der Zertifikate. Neben der Laufzeit der Zertifikate ist auch der Lebenszyklus der Identitäten zu überwachen und Zertifikate zu revozieren – also ungültig zu machen – wenn Mitarbeiter beispielsweise das Unternehmen verlassen oder sich Berechtigungen ändern.

Die Komplexität der Aufgabe steigt auf technischer Seite zudem, wenn, wie im Fall der Post CH AG, zur Ausstellung von Zertifikaten für Windows Clients in einer Active Directory Umgebung eine nicht-Microsoft CA (Certificate Authority) verwendet wird. Hier empfiehlt sich der Einsatz eines Proxys, der die automatische Zertifikatregistrierung, das Autoenrollment, übernimmt. Ein solcher Proxy vereinfacht und beschleunigt Prozesse zur Verteilung und Verwaltung digitaler Zertifikate, erhöht damit die IT-Sicherheit und Zuverlässigkeit und hilft Kosten zu sparen.

Absolut zuverlässig: Post CH AG optimiert Autoenrollment digitaler Zertifikate mit Secardeo GmbH

Vor der Zusammenarbeit mit der Secardeo GmbH hatte man bei Post CH AG einen selbst entwickelten Autoenrollment Proxy im Einsatz. Diese Lösung wies jedoch einige Schwächen auf, da sie beispielsweise nicht zuverlässig erkannte wenn bereits Zertifikate installiert waren und so teilweise bis zu sechs oder sieben Zertifikate für den gleichen Zweck oder den gleichen Nutzer vergeben wurden, was aus finanziellen und organisatorischen Gesichtspunkten nicht tragbar war. Man entschied sich also am Markt nach einem Autoenrollment Proxy zu suchen, wobei die absolute Zuverlässigkeit der Lösung höchstes Gewicht bei der Entscheidung hatte.

Anforderungen

Bei der Auswahl der passenden Lösung achteten die Mitarbeiter der Fachabteilung der Post CH AG unter Leitung von Walter Enkerli insbesondere darauf, dass das Produkt schnell einsatzfähig sein konnte und beispielsweise keine Softwareverteilung auf die Clients erforderlich war. Zudem wünschte man sich eine nahtlose Integration des Autoenrollment Proxys mit Windows Active Directory sowie die Verwendung von Zertifikatsvorlagen (sowohl Standard-Vorlagen als auch kundenspezifischer Templates). Auch sollte die Lösung eigenständig zu betreiben sein, um im Unternehmen vorhandene Windows AD & PKI Skills zu nutzen.

Die Lösung

Die Entscheidung fiel auf certEP der in Ismaning bei München ansässigen Secardeo GmbH. Der certEP vermittelt zwischen den Windows Clients und der externen Zertifizierungsstelle. Dabei agiert er unabhängig von einer Microsoft CA und ist in der Lage eine Reihe von Zertifizierungsstellen über anpassbare Schnittstellen einzubinden.

> *„certEP hat alle Anforderungen und Ziele, die wir an das Produkt hatten, erfüllt. Auch das Team der Secardeo GmbH war sehr professionell. Heute ist es ideal wie es jetzt ist, wir haben keinerlei Probleme.“*
>
> *Walter Enkerli*
> *Informatik, Post CH AG*

Zugleich unterstützt certEP native Microsoft PKI Protokolle, so dass keine Client-Softwareverteilung nötig ist. certEP verwendet einen etablierten Managed PKI Service, dank dessen die Private Key Infrastructure innerhalb weniger Stunden einsatzfähig ist. Durch ihren hohen Automatisierungsgrad werden PKI Betriebskosten minimiert. Zusätzlichen Schutz vor Bedrohungen bietet die Isolierung der CA aus dem Produktions-Netzwerk.