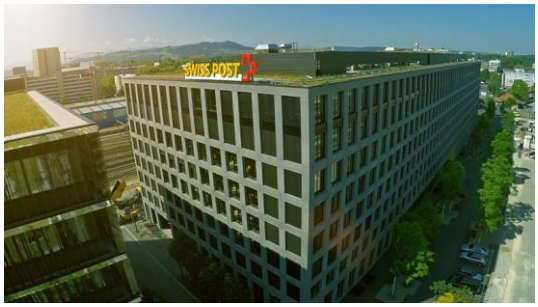
Absolutely Reliable: Post CH AG Optimizes Autoenrollment of Digital Certificates with SECARDEO

certEP acts as Autoenrollment Proxy and sits between the Windows Clients and an external Certificate Authority (CA)

Post CH AG
With 58,000 employees working in one of its six business units, PostMail, Swiss Post Solutions, PostNetz, PostPogistics, PostFinance and PostAuto, Post CH AG is one of the largest employers in Switzerland. Besides continuing to provide postal services to the Swiss public, the company is focused on delivering on its physical-digital transformation strategy. Post CH AG's goal is to combine the physical and digital world. As such, all of its products and system solutions are designed to set new standards in terms of customer focus and user friendliness.



Challenges and Objectives
Digital certificates as part of a PKI (Public Key Infrastructure) are the method of choice to secure the internal and external exchange of information, making it possible to reliably identify communication partners. It's critical to a company's security to centrally manage identities and protect them from being forged or misused.

While certificate verification is performed automatically by programs such as Thunderbird or MS Outlook for digitally signed e-mails and Firefox or Internet Explorer for SSL certificates, automatically managing the variety and increasing number of certificates used by an organization can prove to be problematic. If only a small number of certificates is being used, manual management is still feasible, else more advanced solutions that go beyond simply providing certificates are being called for. The validity period of each certificate has to be monitored as does the lifecycle of these digital IDs and making sure certificates are revoked – rendered invalid – for example if an employee leaves the organization or access rights change.

From a technical point of view it's becoming even more complex if a company – as is the case with Post CH AG – uses a non-Microsoft CA (Certificate Authority) to issue certificates for Windows Clients in an Active Directory environment. This set-up usually calls for a Proxy which can automatically handle certificate registration (autoenrollment). This Proxy will simplify and accelerate processes for certificate management and distribution, contribute to increased IT security and reliability and help reduce costs.

Absolutely Reliable: Post CH AG Optimizes Autoenrollment of Digital Certificates with SECARDEO

Before working with Secardeo GmbH, Post CH AG had developed and used its own Autoenrollment Proxy. This in-house developed solution, however, had some technical flaws. For example, it couldn't reliably tell if a certificate had already been installed leading to situations where one user received up to six or seven certificates for the same use case, which from a financial and operational point of view was not viable. Post CH AG decided to look for an industry-proven Autoenrollment Proxy on the market, putting utmost importance to its absolute reliability.

Requirements

In their decision making process, the team of experts at Post CH AG led by Walter Enkerli focused on number of criteria. The solution needed to deploy quickly and shouldn't require software to be installed on the Windows Clients. They also looked for an Autoenrollment Proxy which would seamlessly integrate with Windows Active Directory and offered both standard and customer-specific certificate templates. In addition, they wanted to be able fully and autonomously manage the Proxy themselves, thus continuing to use their Windows AD and PKI skills.

Solution

The decision was made to use certEP from Secardeo GmbH based in Ismaning, in close proximity to Munich. certEP sits between the Windows Clients and an external certification authority. It acts independently from a Microsoft CA and is able to interface with a number of CAs via open interfaces.

> *„certEP fulfilled all of our requirements and objectives which we had on this product. On top, the Secardeo team was extremely professional. Today we are highly satisfied with the solution we achieved, we don't have any problems at all."*
>
> *Walter Enkerli,*
> *Informatik, Post CH AG*

As certEP supports native Microsoft PKI protocols, no software has to be distributed and installed on the client machines. certEP leverages an established managed PKI service making it possible to have the private key infrastructure up and running in a matter of hours. Its high level of automation helps reduce operational cost of the PKI. Last but not least, isolating the CA from the production environment, helps to further protect the company from cyber threats.