keyon

Migros-Genossenschafts-Bund (MGB)

Automated issuance of user certificates

Seamless integration with identity management processes

Parallel integration of a Microsoft CA and public CA

Enterprise PKI

The Migros-Genossenschafts-Bund put the focus on certificate-based authentication and encryption as part of the renewal of all new Windows workstations. The goal was the fully automated issuance and management of user certificates, as well as a role-based cockpit for processes and status inquiries.

The large enterprise placed emphasis on safety, management and convenience in regards to the renewal of the company-wide identity management (IdM) and the upgrade of all Windows workstations. In short, "M as in more" in terms of security and convenience in the area of certificate management.

The aim was to automatically equip all workstations with authentication- and encryption certificates. This was realized with Keyon's true-Xtender Suite and the simultaneous integration of a Microsoft CA and a public CA.

Keyon assisted the MGB in the design and implementation of the solution as well as with the support in the productive use.

The customer

The Migros-Genossenschafts-Bund, headquartered in Zurich, takes on various tasks within Migros. It forms the Migros Group together with the ten cooperatives, the own industry, the service sector, and the other associated or related companies, organizations and foundations.

www.migros.ch

Requirement

Along with the implementation of a new, company-wide IdM, as well as the renewal of all MGBs Windows workstations, should the existing PKI be replaced with a new PKI. In so doing, the existing user certificates must be automated and safely replaced with new certificates without affecting the users in their work. Users should receive in the same step company-own certificates as well as public certificates. In addition, comprehensive lifecycle management of certificates and a conclusive report on the progress of a process and system states was demanded.

The certificates should be automatically issued, renewed and revoked in accordance with Active Directory guidelines and MGB-specific rules. The process should also automatically updated the certificate status in the case of name changes, change of department, the resignation of personnel or decommissioning of equipment.

Solution

Keyon was responsible for the technical and organizational implementation of all PKI-based processes. Based on Keyon's true-Xtender Suite

- the MGBs old Microsoft PKI has been replaced with a new Microsoft PKI;
- the issuance and management of certificates has been controlled via the IdM;
- the public CA from QuoVadis Trustlink Switzerland AG has been integrated parallel to the Microsoft CA;
- a web-based cockpit has been provided, that, depending on respective roles, allows different administrative activities or displays process statuses.

Keyon supported the MGB with technical and organizational know-how in the specification, implementation, and integration. Furthermore, Keyon ensured through ongoing know-how transfer and specific training that the MGB can operate the solution efficiently and independently.

The effort for issuance and management of certificates has been reduced to a minimum by automating technical processes. The innovative solution was implemented cost-effectively and on schedule. It is characterized in particular by the following properties:

- Full certificate lifecycle
  Flexible and dynamic Microsoft Autoenrollment of public and internal certificates;

- Key history
  Automated management and import of the key history of encrypted certificates on terminal devices;

- Integration of the Dell's Quest One Identity Manager
  Rules and process control through IdM;

- Comprehensive cockpit
  Web-based cockpit that allows role based administrative activities or status inquiries.