HOW ONE GERMAN FEDERAL AGENCY HAS KILLED THE PASSWORD AND IMPROVED SECURITY AND USER EXPERIENCE BY
MOVING TO STRONG PASSWORDLESS AUTHENTICATION

A German Federal Institute, which forms part of a collection of federal agencies consulting the German national government, recognized the need to evolve its workforce authentication. The organization had identified its password-based approach as a low-security solution that was delivering a poor user experience for its employees. A strong multi-factor authentication solution was required as the organization looked to ensure its employees could access government systems simply and securely.

THE CHALLENGE

With login and passwords still in use, the agency recognized that there was a need to step up the organization's security and provide a better system for its IT teams and employees.

Strong two-factor authentication (2FA) using the cryptographic security of public key infrastructure (PKI) was identified as the most secure solution. As proven technology that is simple to use and familiar to employees, smart cards were the chosen form factor that the agency wanted their 2FA to be based on. This meant employees would log in to an IT system using a combination of their credentialed smart card plus a PIN.

The federal agency was looking for an on-premise solution that would sit within their existing Windows Server network and enable their IT teams to issue digital identities to their employees' smart cards, set user policies, manage the x.509 certificates and integrate into the agency's Microsoft Active Directory. A software solution that would integrate with the internal Microsoft PKI certificate authority (CA) was essential, as was the scope for employees to self-serve when reactivating a blocked smart card or setting a new smart card up for use.

Furthermore, the agency required installation on-site in Hannover by a German-speaker.

THE SOLUTION

CRYPTAS Deutschland GmbH was the chosen organization to deliver the 2FA solution. The CRYPTAS solution offered a combination of smart cards for employees to use crypto-backed authentication into IT resources and a feature-rich credential management software solution in Intercede's MyID for issuing and managing digital identities across the agency's employees. MyID also presented a user-friendly solution for the organization's IT teams to manage the 2FA deployment and self-service options for employees to selfmanage their smart cards.

In line with the agency's requirements, MyID was installed on-premise by CRYPTAS to the existing Windows Server 2019.

cryptas

we protect identities.

This provided the agency with a fully functional credential management system without connection to any cloud services or requirements for permanent internet connectivity.

The agency establishes compliance to "IT-Grundschutz" within their IT network, using the Microsoft AppLocker service. The administration of all agency computers and user accounts takes place in a Windows domain, using Active Directory (AD). The configuration of MyID ensures that AD information is usable within the credential management system, with AD accessed via LDAPS.

The self-service elements of MyID ensure that agency employees can reactivate their smart card should it become blocked. Employees are also able to update existing smart cards and can only see features within MyID that they can use.

CRYPTAS delivered the integration and smart card setup on time at the agency's Hannover base, all managed on-site by CRYPTAS' native German-speaking team from its Düsseldorf office.

With the initial rollout complete across all employees, the agency is now working with CRYPTAS to extend the deployment across a further two federal agencies.

THE RESULTS

Improved Security
The threat of data breach has been minimized by the agency moving from passwords to 2FA using strong authentication.

Improved Usability
Employees no longer have extensive passwords to remember and update and can log in simply with their CRYPTAS smart card and a PIN.

Reduced Helpdesk Demand
Employees can now self-serve using MyID to reset PINs and update their smart cards, reducing demands on IT teams.

Seamless Integration
The flexibility of MyID to integrate with the agency's existing IT infrastructure, together with onsite installation by CRYPTAS, ensured a smooth transition to the new deployment.

Futureproofed identity solution
The proven integration between MyID and CRYPTAS smart cards ensures the federal agency has a solution that can grow in line with their requirements. The additional flexibility of MyID to issue and manage credentials to virtual smart card technology, USB security keys, and mobile devices means that the agency has a futureproof identity management solution.

Easy deployment
The expertise and experience of the CRYPTAS team ensured the deployment was simple and without hidden complexities and costs. The end-to-end approach offered by CRYPTAS ensured everything from hardware, software, installation, and support was managed in line with the agency's requirements, timescales, and budget.

Find out more about CRYPTAS and MyID

https://www.cryptas.com/
https://www.intercede.com/