DEPLOYING STRONG AUTHENTICATION IN THE ENERGY AND UTILITIES SECTOR

A US diversified energy company, supplying millions of customers with electric utility and natural gas utility, required a solution that would secure their workforce's access into their corporate systems and facilities.

With 12,000 employees geographically spread, the organisation required a solution that would ensure only the right people had access to highly secure environments, including a nuclear power plant, and IT systemsand resources across the corporate network.

THE CHALLENGE

Responsible for keeping millions of lights on and homes warm, the energy provider continuously strives to minimise any risk to the reliability of their services. With a growing cybersecurity threat posed to US utilities, the energy provider recognised a need to mitigate this risk by ensuring they were using best practices to secure their workforce authentication.

As a utility provider, the company has a large and diverse workforce with different access requirements, both from a physical and logical access perspective. Key to any solution was the capacity to make secure access user-friendly and not create onerous barriers that would hinder employees' ability to do their jobs. Ease of use was fundamental, as was the need to limit the devices needed for employees to authenticate. The energy provider did not want a solution where employees would need multiple devices to enter different facilities or for logical access into their corporate network.

The energy provider also wanted a solution that would be simple to integrate into their existing IT infrastructure, minimising the need to invest in further hardware and software, and speeding up the time to deploy.

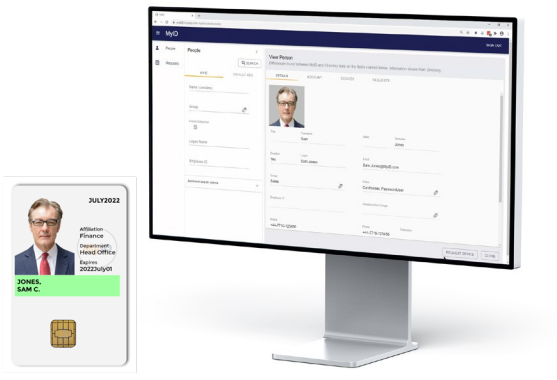
One cohesive system to manage their workforce authentication deployment was a must. As was a system that made the deployment manageable for a small number of system administrators and system operators across their 12,000 employees.

Lastly, as a US energy provider, best practice authentication in line with National Institute of Standards and Technology (NIST) guidelines was important.

THE SOLUTION

Intercede partner, CertiPath demonstrated the optimum solution to the energy provider with their combination of a logical access system and credential management, using MyID.

The solution offered a facility-wide PACs system for employees to access the facilities they were approved to with a smart card. That same smart card would also enable employees to access their corporate systems and networks securely, whether working from an office or remotely.



Fundamental to the solution was public key infrastructure (PKI), delivering best practice strong authentication that minimises the cybersecurity threat posed to the energy provider and adheres to the standards set by U.S. Government.

This meant that MyID would issue a credential to each employee's smart card. Cryptographically protected, at the

point of authentication an employee would present their smart card to a reader and a crypto-backed handshake would occur between the private key on the smart card and a public key from the energy provider's certificate authority. The employee would also be required to enter a PIN for two-factor authentication.

For access into secure buildings, employees would simply use their smart card on an external door reader and be granted access.

For the lifecycle management of employees' smart cards, a small number of system administrators and system operators have access to MyID. MyID is used by system admins to set security policies, define user groups and associated access rights, and access the system's audit and reporting functionality. System operators are also able to login to MyID to revoke and replace employee smart cards, issue new smart cards, and update existing smart cards should an employee's personal details or role change.

The deployment of MyID has meant the energy provider has a robust, centralised system to issue and lifecycle manage their employees' smart cards, ensuring organisation-wide use of strong multi-factor authentication to access digital systems. An approach that removes the threat of system breaches fom social engineering and phishing attempts. Fundamentally, the energy provider knows that only the right people are able to access their facilities, systems and networks.

THE RESULTS

SECURE
All employees now use strong multi-factor authentication to access corporate systems and networks.

EASY TO MANAGE
MyID centralises the management of the energy provider's 12,000 employees and provides the framework for system administrators and system operators to manage the deployment across their workforce in a simple, manageable way.

USER-FRIENDLY
High security doesn't have to mean poor user experience. All employees have a single smart card that they are able to use for both physical and logical access. For buildings a simple insertion or touch of the card using external card readers, and for computer systems it's just the matter of inserting the card into an in-built card reader and entering a PIN for two-factor authentication.

BEST PRACTICE
The presence of MyID credential management software, as part of the NIST National Cybersecurity Center of Excellence's lab set up for best practice personal identity verification (PIV) solution, was further testament to the solution meeting the security and management needs of the energy provider.

SIMPLE TO DEPLOY
Vendor neutral, MyID integrates with a wide variety of certificate authorities, hardware security modules, smart cards and other devices. The flexibility of MyID ensured the energy provider didn't have to make changes to their existing IT infrastructure, making the deployment simpler and quicker.

FUTUREPROOF
MyID is continuously updated on a quarterly release cycle, ensuring the system integrates with the technologies the energy provider wants to use. The energy provider has the technology to embrace alternative end user devices, from iOS and Android OS devices, to alternative smart cards and USB tokens. MyID also supports FIDO alongside PKI based authentication.

CONTACT EXPISOFT TO FIND OUT MORE

Contact us now to discover what MyID has to offer your organisation:

sales@expisoft.com **+46 8-41 00 79 00**