yubico

Herning Kommune

Industry

Local government

Healthcare

Benefits

Secures access to protected health information

Meets eIDAS and NSIS requirements

Preferred 2FA factor for 90% of deployed users

Provides user-based logging for medication audits

Protocols

FIDO2/WebAuthn

Products

Security Key C NFC by Yubico

Deployment info

All nurses and nursing assistants

1,500+ initial deployment

Plans to double healthcare deployment to all employees

Herning Kommune secures patient data with the YubiKey

Danish municipality secures medical data and critical health logs with easy-to-use, phishing-resistant MFA

Herning Kommune needed to meet NSIS requirements

Like many municipal governments across Europe, Denmark's Herning Kommune provides comprehensive public services including child care, health and elderly care. Representing one of 98 municipalities in Denmark, Herning Kommune's public services employ over 10,000 people, or roughly one-ninth of the municipality's population.

As a public sector organisation operating within the European Union (EU), Herning Kommune is subject to the requirements of eIDAS, the regulation on Electronic Identification, Authentication and Trust Services, as well as its Danish implementation, the National Standard for the Security Level of Identities (NSIS). These regulations provide a framework for secure electronic identification and authentication of users accessing public and private services—access which is destined to be supported cross-border with the establishment of a new EU Digital Identity Wallet (EUDI).

Patrick Grud Kristensen, IT Systems Specialist at Herning Kommune and

> " We have stronger security because of eIDAS and NSIS. We have had to rethink many areas, from privileged access to log collection. All of it has been a journey."

Patrick Grud Kristensen |
IT Systems Specialist | Herning Kommune

responsible for managing its hardware and software systems, worked on the technical team responsible for ensuring NSIS and eIDAS compliance. Requirements included implementing least-privileged user access controls as well as stronger two-factor authentication for privileged access by certain user groups, including employees working with medical information. For these users, Kristensen had to evaluate which methods of authentication met the levels of assurance (LOA) requirements of NSIS and eIDAS, which included the use of one of the following: an electronic identification credential (eID, locally referred to as mitID), an authenticator app (computer or phone) or a hardware security key.

In choosing authenticators, the team considered both the technical scope of

implementation as well as gaps where device-based or mobile authentication would not work or were not an option. For example, some users lack or choose not to use personal devices. Further, employees working in medical or elderly care often use shared devices (tablets), which cannot securely store personalised credentials. These employees have the choice to use their mitID, but the use of personal eIDs for work cannot be required. With this in mind, Herning Kommune sought a hardware security key that supported the global FIDO2 authentication standard, meeting the highest LOA requirements of eIDAS.

Modern security and strong phishing-resistant MFA for healthcare with the YubiKey

Herning Kommune's network partner NetIP recommended the YubiKey, a hardware security key that provides phishing-resistant two-factor, multi-factor and passwordless authentication leveraging FIDO2/WebAuthn. Working through distributor Infinigate, the team chose the Security Key C NFC by Yubico for both USB and NFC support, adding a tap-n-go second factor for secure and easy two-factor authentication.

Prior to the implementation of eIDAS and NSIS requirements, Herning Kommune only relied on single-factor username and password for authentication to all government systems, including those that stored sensitive personal or medical information. The first YubiKey deployment targeted employees in Health and Senior Services, as well as Disability and Psychiatry.

The largest deployment of YubiKeys has been to 1,000 nurses and nurse assistants who work in the 30 health units across Herning Kommune, as well as those who provide roaming health services to citizens in the field. These employees use shared tablets, iPhones and Samsung devices to access health and workplace systems.

Cost-effective YubiKeys secure at scale with a 90% adoption rate

The team felt that not only did the YubiKey prove a cost-effective option at scale, often a top consideration in the public sector, but it also outperformed other options in terms of usability. Although employees were given the choice to use their mitID, the YubiKey has seen a 90% adoption rate due to its ease of use and to minimise the risk that personal phones will be lost or broken during the day.

The YubiKey gives every employee a secure, reliable connection to health systems to ensure seamless care delivery. It requires no software installation, battery or mobile connection, making it ideal for shared device environments and for employees who are off-network working in the field or remotely. Users benefit from a frictionless authentication workflow, simply plugging the YubiKey into the USB port of a shared device and touching to authenticate.

"The YubiKey is easy and fast to use," notes Jonas Philipsen, an IT Consultant at Herning Kommune responsible for supporting the 2,000 employees and 800 devices across the Health and the Senior services. "Now our users can get back to what matters—patient care." The team at Herning Kommune supported YubiKey adoption with in-person education at each of the 30 facilities that received the first YubiKey deployment.

1500+

Number of users in initial deployment

Improving healthcare security with audit logs and the phishing-resistant YubiKey

The YubiKey has been a critical factor in increasing healthcare security at Herning Kommune. Usernames and passwords are easily hacked, being highly susceptible to phishing attacks and account takeovers that place patient information at risk.

> " We are taking care of people 24 hours a day, 365 days a year. It's critical that we have a reliable method to access healthcare systems anytime, anywhere. The YubiKey provides that for us."

Jonas Philipsen |
IT Consultant | Herning Kommune

The Yubikey provides phishing-resistant authentication, which requires both proof of possession and the presence of the user to log in or gain access to systems.

"We have to make sure the right person is coming into our systems," explains Philipsen. "The YubiKey helps ensure that hackers cannot enter systems or access patient information."

Independent research has shown that the YubiKey stops 100% of account takeovers. Furthermore, the YubiKey eliminates the insecure practice of password sharing, a common scenario in shared device environments where employees seek to save time or bypass having to reset forgotten passwords.

For Herning Kommune, the YubiKey also plays a critical role in supporting medication audits. When health employees access shared medicine carts with their YubiKey, that access is logged. In the event of a discrepancy, or if the wrong medicine were to be administered, this log would be critical to the investigative process. Previously, when passwords were shared between staff, these records would not have been reliable.

Seamless integration with Microsoft environment helps address growing number of systems and use cases

The initial deployment of YubiKeys at Herning Kommune focused on approximately 1,500 users, with a small buffer of extra keys to account for loss and employee turnover. The deployment in Health and Senior services will soon expand from 1,000 nurses and nurse assistants to extend to all 2,000 Health and Senior employees across the health system.

In addition to expanding the deployment of YubiKeys, Kristensen's team is working to expand YubiKey support across additional health and services systems. "Over time, we're making the YubiKey more agile by using it on a wider number of systems," continues Kristensen.

> **" **It is very important that we know who accessed the medicine cart to ensure that the right patient receives the right medication."

Jonas Philipsen |
IT Consultant | Herning Kommune

Sources

[1] European Commission, eIDAS Levels of Assurance (LoA), (2014)

[2] National Standard for Identity Assurance Levels (NSIS) Version 2.0.1a, (September 27, 2021)

[3] European Commission, Commission welcomes provisional political agreement on EU Digital Identity Wallet, Europe's first trusted and secure digital identity app, (June 29, 2023)

[4] European Commission, eIDAS Levels of Assurance (LoA), (2014)

Herning Kommune leverages Microsoft solutions for its work environment, both on-premise and in the cloud, including Microsoft Azure and Microsoft SQL. Herning Kommune is looking to continue modernising authentication across its departments, possibly incorporating a hybrid flow that allows for biometric platform authentication on Windows Hello for Business used in combination with or alongside the YubiKey.

Looking ahead with a future-proof MFA investment

Herning Kommune knows that today's rapidly changing compliance and security landscape requires an authentication solution that meets the most stringent security requirements and provides the flexibility for a wide variety of use cases, including emerging use cases around the use of electronic identifications across the EU. With the YubiKey, Herning Kommune has found a secure, phishing-resistant solution that users actually want to use.

Learn more   yubi.co/customers   yubi.co/contact

yubico