yubico

CASE STUDY

KAUNO MIESTO POLIKLINIKA

Industry

Healthcare

Protocols

FIDO2 (Passkeys)

At a glance

- Largest outpatient healthcare institution in Lithuania
- Serves 160,000 residents
- Employs 1,700 professionals across 14 branches

Key results

- 80% drop in password resets, freeing up IT resources
- Significantly reduced phishing risk, resulting in zero data leaks
- Compliance with GDPR and NIS2
- Faster, more reliable logins on shared workstations

Yubico solutions deployed

YubiKey 5 NFC USB-A

Kaunas City Polyclinic Secures Patient Data and Achieves NIS2 Compliance with YubiKeys

Lithuania's largest public sector outpatient healthcare institution enables passwordless, phishing-resistant single sign-on to Microsoft accounts

> "YubiKeys strengthened security, boosted efficiency and enhanced our reputation as a modern healthcare provider."

Marius Sinkevičius
Head IT Department (CTO) | Kaunas City Polyclinic

Securing healthcare operations for 160,000 patients

Kaunas City Polyclinic is the largest public sector outpatient healthcare institution in Lithuania, serving over 160,000 residents and employing approximately 1,700 professionals. Kaunas City Polyclinic's laboratories perform over 1.6 million tests annually, with 95% of results delivered within 24 hours. Their smart call center answers 90% of patient calls immediately, ensuring patients receive timely access to services.

The clinic's digital transformation and security strategy are overseen by Marius Sinkevičius, Head of the IT Department (CTO). As a CISO-certified professional, he is responsible for the development and implementation of digital solutions that support healthcare operations, data management and cybersecurity.

"We pride ourselves on patient-centered care," says Sinkevičius, "with a strong emphasis on accessibility and responsiveness—and continuously upgrade our technologies to ensure precision, efficiency and patient safety."

> "A successful cyberattack could lead to financial losses, reputational damage and disruption of healthcare services."

Marius Sinkevičius
Head IT Department (CTO) | Kaunas City Polyclinic

“We moved to phishing-resistant MFA with YubiKeys to prevent future incidents before they happen.”

Marius Sinkevičius
Head IT Department (CTO) | Kaunas City Polyclinic

Vulnerability of passwords highlighted urgent need for phishing-resistant authentication

The healthcare sector globally faces increased risks due to the sensitivity of patient data and the reliance on legacy systems. Lithuania’s location means that critical infrastructure, including healthcare, also faces heightened geopolitical risks. Any successful cyberattack could disrupt critical healthcare services and lead to financial and reputational damage.

The EU’s NIS2 directive intensified the clinic’s cybersecurity efforts, driving the team to update risk plans and implement stronger tools. While Kaunas City Polyclinic had never experienced an external security breach, access to internal systems relied solely on passwords. “AI-powered phishing has made my job significantly harder,” said Sinkevičius. “Attacks are now highly personalized and convincing, making them difficult to detect. We’ve had to strengthen our defenses, train staff more intensively and stay constantly alert”.

The turning point for the organisation’s leadership was a simulated phishing test where several staff members unknowingly clicked on a fake link. This exposed the vulnerability of their password-only system, making it clear that phishing-resistant multi-factor authentication (MFA) was essential to protect sensitive healthcare data.

Legacy MFA methods threatened workflow disruptions

Kaunas City Polyclinic’s challenge was balancing strong security with operational ease of use. Doctors and nurses focus on providing speedy patient care, and are reluctant to be bogged down by extra security steps. With the help of Hermitage Solutions, the clinic’s long-time partner in IT infrastructure, the team evaluated options such as 2FA apps and SMS authentication but found they added complexity and disrupted existing workflows. Their search led them to passkeys, which offered a strong, phishing-resistant alternative with minimal workflow disruption.

Decision to deploy the most secure passkeys

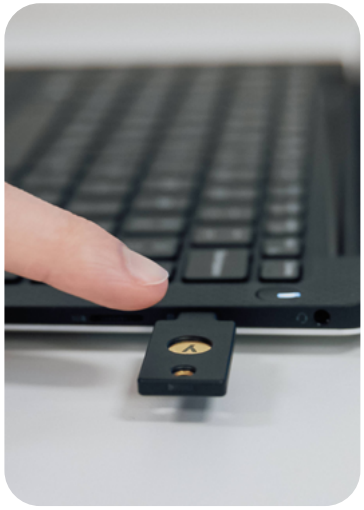
Synced passkeys are stored in the cloud and synced across multiple devices, offering convenience but introducing potential risks if the cloud account is compromised. For increased security, passkeys can also be restricted to a single hardware security key, like a YubiKey. For Sinkevičius, this was important: “device-bound passkeys give us stronger control over identity verification and reduce the risk of unauthorized access”.

The YubiKey requires a physical touch or tap to authenticate, blocking man-in-the-middle attacks. Manufactured in Sweden with a secure European manufacturing process and supply chain, a single YubiKey can store 100 passkeys, as well as Smart Card credentials and more.

Kaunas City Polyclinic opted to purchase the YubiKey 5 NFC, to enable phishing-resistant, passwordless login for medical staff to access internal systems via single sign-on (SSO).

“For medical staff, ease of use is critical since their priority is patient care, not IT tools. YubiKeys stood out as the fastest, most secure and user-friendly solution that fit seamlessly into daily routines.”

Marius Sinkevičius
Head IT Department (CTO) | Kaunas City Polyclinic



YubiKeys integrated seamlessly with Microsoft

Hermitage Solutions assisted with the deployment, beginning with a preparation phase during which the IT team designed security architecture and evaluated solutions, followed by a testing phase, where YubiKeys were piloted within the IT department.

Initial integrations focused on the core Microsoft environment, covering both Active Directory on-premises and cloud-based Microsoft 365.
Access to additional services, like the hospital information system (HIS), document management and finance platforms, was made possible through single sign-on, ensuring staff could use one YubiKey for all their common daily tasks.

This created a unified and simple authentication experience across the clinic's diverse digital environment, covering both modern cloud services and critical legacy infrastructure, allowing Kaunas City Polyclinic to upgrade its security posture without costly or disruptive system overhauls.

Rapid YubiKey deployment at speed and scale

The main rollout of YubiKeys to employees took two months—minimal training was required, but additional testing was provided for departments with complex workflows. Once 90% of employees had their keys, it was no longer possible to log into a workstation without a YubiKey. This requirement extends to mobile devices, where staff use the NFC capability of their YubiKey to access Microsoft email on their phones.

> “By implementing YubiKeys and SSO, we significantly reduced the risk of credential theft and improved both security and user experience.”
>
> **Marius Sinkevičius**
> Head IT Department (CTO) | Kaunas City Polyclinic

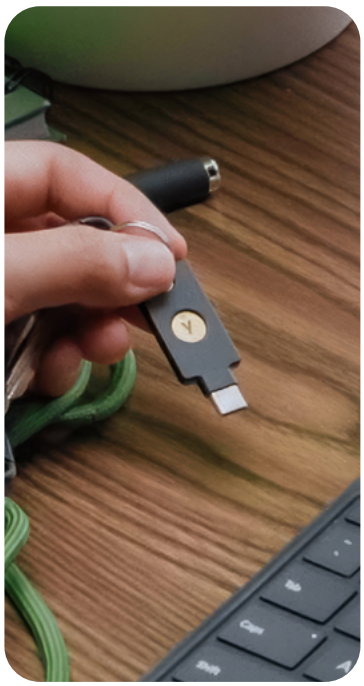
Password resets drop by 80% slashing support costs

While some staff saw the rollout as “another task from IT,” users quickly adapted and began to appreciate the benefits. Login became faster and more reliable, which is particularly crucial for medical staff using shared workstations. Since implementing YubiKeys, Kaunas City Polyclinic has seen major improvements across security, costs and daily operations. “Phishing risks have dropped significantly, helping us align with NIS2,” says Sinkevičius.

IT cost reduction was significant, reducing helpdesk workload dramatically as password reset requests decreased by over 80%. An in-house key management system provides operational control with full visibility over issuance, loss and replacements—guaranteeing that only one valid access token is active for each employee at any given time.

The deployment has also simplified GDPR compliance and data protection: previously, staff often neglected to lock their devices, which posed a privacy risk to patient data. Now this crucial step is automated, as removing the YubiKey instantly locks the computer screen.

> “Our primary focus was to provide a secure and efficient solution for medical staff. However, reducing password reset requests and IT workload was a clear added benefit. Support needs have dropped significantly.”
>
> **Marius Sinkevičius**
> Head IT Department (CTO) | Kaunas City Polyclinic



Partnering with Yubico to solve additional use cases—digital signing and more

The assurance provided by YubiKeys that the person logged into a workstation is the actual user allows Kaunas City Polyclinic to move forward with a new project: implementing a digital company stamp and secure signing process.

Lithuanian law currently requires every doctor to sign documents using a personal signature stored on a USB device. The clinic plans to upgrade this process by acquiring hardware security module (HSM) infrastructure, embedding the signing doctor's identity into the signature metadata, and requiring users to re-enter their YubiKey PIN before signing. This will further strengthen accountability and ensure every signature is securely tied to the correct individual.

> "When changes bring clear benefits—like introducing YubiKeys, eliminating the need for passwords across internal systems people become much more open to change. Showing value makes all the difference."
>
> **Marius Sinkevičius**
> Head IT Department (CTO) | Kaunas City Polyclinic

A blueprint for modern healthcare security

Kaunas City Polyclinic provides a clear model for other healthcare institutions facing similar challenges, demonstrating that it is possible to achieve the highest levels of security without compromising efficiency.

By implementing phishing-resistant MFA, the clinic dramatically reduced its cyber risk, aligned with stringent NIS2 and GDPR mandates and future-proofed its infrastructure for passwordless authentication. This transformation has not only benefited internal operations but also positioned Kaunas City Polyclinic as a leader in digital health assurance.

As threats to the healthcare sector intensify and digital services become increasingly critical to patient care, Kaunas City Polyclinic's dedication to robust, high-assurance authentication secures its vital operations, employees and the protected health information of Lithuanian residents.

> "Stronger security has reinforced patient and stakeholder confidence in our ability to protect sensitive health data."
>
> **Marius Sinkevičius**
> Head IT Department (CTO) | Kaunas City Polyclinic

Contact us
yubi.co/contact

Learn more
yubi.co/customers

yubico