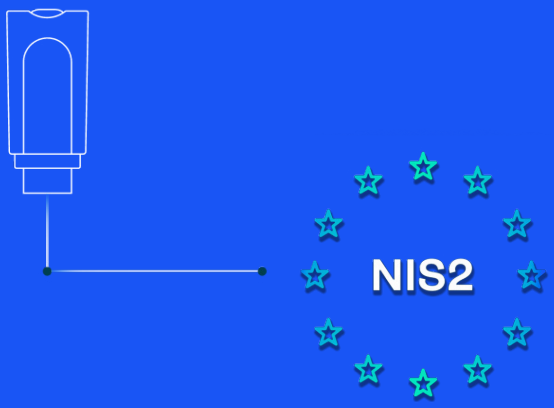
OneSpan

Digipass®

& NIS2 Compliance



Solution brief

Phishing-resistant authentication that complies and exceeds NIS2 requirements

The NIS2 Directive mandates strong, risk-based authentication to secure access to critical systems and sensitive data. Digipass® FX delivers phishing-resistant, device-bound security that empowers organizations to protect critical systems, secure their workforce, and meet NIS2 requirements with confidence.

As digital transformation deepens across critical infrastructure, the EU's NIS2 Directive raises the bar for cybersecurity resilience. Designed to improve the protection of essential services, NIS2 mandates robust risk management, incident reporting, and, crucially, multi-factor authentication (MFA) for workforce access to sensitive systems.

Digipass FX FIDO2 security keys offer organizations a phishing-resistant solution that meets and exceeds NIS2's MFA requirements. Unlike outdated methods such as SMS codes, Digipass FX FIDO2 security keys provide strong, cryptographic authentication that's resistant to interception, replay, and manipulation.

Understanding NIS2 and who must comply?

The Network and Information Security Directive 2 (NIS2) is the EU's updated cybersecurity framework, extending its scope to a wider range of sectors and organizations than its predecessor.
Entities in finance, energy, utilities, healthcare, digital infrastructure, transportation, and other critical domains must now adhere to its strict standards. Among the core mandates of NIS2 is a strong emphasis on risk-based governance, supply chain security, timely incident reporting, and, most notably, workforce authentication.

Article 21 of the directive specifically highlights multi-factor authentication as a foundational security measure, underscoring its role in protecting access to essential systems and sensitive data. By requiring stronger access controls, NIS2 aims to reduce the risk of unauthorized access and identity-based attacks. Non-compliance may lead to regulatory penalties, reputational damage, and greater exposure to cyber threats.

Strong authentication for the workforce

NIS2 requires covered entities to implement multi-factor or continuous authentication solutions as part of their overall security strategy. This ensures that only verified users can access sensitive systems, especially in remote or high-privilege scenarios. The directive does not prescribe specific authentication technologies but calls for security measures that are appropriate and proportionate to the associated risk, particularly when securing access to critical systems and sensitive data.

To help organizations interpret these requirements, the European Union Agency for Cybersecurity (ENISA) offers clear technical guidance on evaluating the strength of MFA methods.

ENISA categorizes MFA into three tiers: "strongest," "medium," and "last resort," and recommends aligning the chosen method with asscoiated risk. The strongest level, which includes phishing-resistant MFA such as FIDO-based security keys, is recommended for high-risk scenarios and access to critical systems. By contrast, legacy methods like SMS OTPs are considered less secure and more vulnerable to phishing and adversary-in-the-middle attacks.

FIDO2, developed by the FIDO Alliance, exemplifies this highest level of security. It uses public-key cryptography to eliminate vulnerabilities common to legacy MFA, such as phishing and credential theft. Built on this standard, Digipass FX security keys offer hardware-backed, phishing-resistant authentication that supports NIS2 compliance while strengthening overall access security.

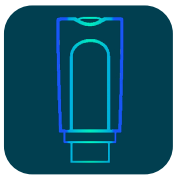
How Digipass FX helps organizations meet NIS2 compliance

Meeting NIS2 requirements isn't just about ticking boxes, it's about deploying security controls that work reliably at scale, across departments, devices, and user profiles. Digipass FX provides a modern, hardware-backed approach to authentication to stop phishing at the source by eliminating passwords. It's designed for ease of use, high assurance, and broad compatibility . From financial services and energy to public administration, any organization that falls under NIS2 can use Digipass FX FIDO2 security keys to secure employee access. Digipass FX is purpose-built for enterprise environments where phishing threats are real, and user experience matters. It bridges security and usability, making strong authentication practical to roll out and effortless to adopt. Here's how it helps organizations secure access, simplify compliance, and stay resilient:

Phishing-Resistant

Digipass FX replaces vulnerable passwords with public-key cryptography, ensuring that every authentication is uniquely signed and bound to the device. This eliminates phishing risks, credential reuse, and adversary-in-the-middle (AITM) attacks, key threat vectors that NIS2 aims to address.

Secure hardware



As a FIDO2-certified security key, Digipass FX establishes a secure, hardware-bound connection between the user and the service. Cryptographic keys are stored in a tamper-resistant enclave and never leave the device, ensuring authentication cannot be spoofed, even if the endpoint is compromised.

Authentication that scales to your needs

Digipass FX scales effortlessly with your business, whether you're securing a small team or a global workforce . The security keys are easy to roll out, quick to enroll, and fully compatible with major browsers, operating systems, IAM platforms, and any FIDO2-enabled service. This flexibility enables organizations to enforce strong, hardware-backed access controls across departments and geographies, without adding complexity to infrastructure.

Designed for everyday use

Digipass FX integrates seamlessly into everyday workflows, requiring no complex setup or user training. Authentication is fast and intuitive: users simply insert the key and tap, or use their fingerprint. With no passwords to remember or apps to manage, it delivers a frictionless experience that drives adoption and supports long-term compliance across the organization.

About OneSpan

OneSpan is a global leader in digital security, trusted by thousands of enterprises across 100+ countries—including more than 60% of the world's 100 largest banks—to safeguard digital accounts, secure financial transactions, and prevent fraud. Our award-winning solutions provide passwordless authentication, digital transaction security, and advanced mobile application protection, helping organizations meet the highest security standards and global compliance requirements. As cyber threats grow more sophisticated, OneSpan delivers cutting-edge technology to safeguard customers, mitigate risks, and ensure trust in every digital interaction.

Learn more at
OneSpan.com/security

Contact us at
OneSpan.com/contact-us