

Yubico Extends Passkeys Beyond Trusted Authentication to Verified Authorization with Launch of YubiKey 5.8

YubiKey 5.8 extends hardware-backed assurance from authentication into emerging digital signature, wallet, payment and agentic approval workflows

STOCKHOLM & SANTA CLARA, Calif. & SINGAPORE--([BUSINESS WIRE](#))-- Regulatory News:

[Yubico](#) (NASDAQ STOCKHOLM: YUBICO), the pioneer of phishing-resistant authentication and creator of the original passkey, the [YubiKey](#), today announced the general availability of its [YubiKey 5.8](#) – marking an expansion of the role of the passkey from secure authentication to include verifiable, hardware-backed authorization. The new firmware delivers a foundation for secure enterprise workflows across identity wallets, document signing, and AI-driven approvals, while also providing developers with the critical capabilities needed to test, design and deploy these next-generation security features early.

As generative and agentic AI mature to drive rapid, automated cyberattacks, traditional multi-factor authentication (MFA) is failing to keep pace. Security leaders now face a challenge globally: securing not just who logs into a system, but exactly what actions a user or autonomous AI agent can perform. While the YubiKey has long delivered industry-leading defense against phishing, YubiKey 5.8 addresses the needs of complex, multi-environment enterprises – going beyond trusted logins to provide a secure, hardware-backed foundation for verifiable digital actions in the age of AI.

"YubiKey 5.8 represents one of the most significant architectural updates to the modern authentication ecosystem by expanding phishing resistance into the workflows themselves," said Albert Biketi, chief product and technology officer at Yubico. "In an era where AI agents execute high-consequence business workflows, organizations must enable dynamic verification of human intent. YubiKey 5.8 bridges that gap, bringing hardware-backed phishing resistance directly into digital signatures, enterprise credential management, and human-in-the-loop validation workflows – without requiring costly custom cryptographic rollouts."

Simplifying the Usability and Scalability of Hardware-backed Passkeys Through Open Standards

The new firmware introduces support for the [CTAP 2.3](#) standard while offering preview support for the emerging WebAuthn signing extension. Developers can now use familiar standards and APIs to build secure, privacy-preserving workflows without relying on expensive backend key management systems or custom cryptographic infrastructure. This significantly lowers the barrier to building trusted digital workflows, allowing developers to integrate high assurance signatures into web applications, digital wallets and AI-driven workflow approval systems with greater speed and less complexity.

The YubiKey 5.8 delivers substantial technical upgrades built directly for developers working across the modern enterprise identity control plane:

- **Support for cutting-edge use cases:** Enables hardware-backed digital signatures through standardized APIs – opening the door to document signing, identity wallets, workflow approvals, and other high-assurance transactions.
- **Better user experience and enterprise scale:** Expanded Enterprise Attestation support to 16 Relying Party (RP) IDs on a single key. This allows a single YubiKey to be simultaneously uniquely identified down to an individual device across trusted development, testing, staging, and production environments across multiple identity providers without compromising user privacy.
- **Simplified developer integration:** Introduces [CTAP 2.3](#) support and preview support for the emerging WebAuthn signing extensions and more, making it easier for developers to integrate secure digital signatures using familiar standards.
- **Emerging initiatives secured:** Expands support for digital identity wallets, verifiable credentials with privacy enabling algorithms, and Secure Payment Confirmation (SPC) support for those developing hardware backed payment use cases on the web.
- **Streamlined user experience:** Persistent PIN/UV auth tokens allow apps to enable frictionless credential discovery and selection, with more autofill capabilities and less frequent PIN prompts for users.
- **Operational simplicity and lower overhead:** Introduces autofill-like credential discovery directly alongside software passkeys. This reduces user confusion, accelerates phishing-resistant passkey adoption, and minimizes IT helpdesk enrollment costs.

“The new signing capabilities of YubiKey 5.8 is a game changer for digital identity and credentials,” said Leif Johansson, executive director at SIROS Foundation. “In the last decade, FIDO authentication has become the industry gold standard for phishing-resistant authentication. By adding signatures, a whole range of new applications become possible without introducing platform lock-in. At SIROS, we are working to integrate the new signing capabilities into a seamless framework for secure phishing-resistant, digital identity credentials.”

YubiKey 5.8 is now shipping across all major YubiKey product lineups starting today. For organizations actively working on the next generation of use cases with a focus on hardware-backed signatures, digital wallet features, and AI-based workflows, YubiKey 5.8 enables acceleration of strong security for these scenarios. YubiKey 5.8 supports all of the capabilities of YubiKey 5.7.4 and expands the use of passkeys for enterprise use cases.

At this time, the YubiKey FIPS Series will remain on the newly validated FIPS 140-3 firmware 5.7.4 to maintain regulatory alignment. The YubiKey CCN Series will also remain on 5.7.4 while it is undergoing final re-certification.

For more details on YubiKey 5.8, visit the Yubico [blog post](#).

Contacts

For media inquiries:
Yubico Communications Team
press@yubico.com

Source: Yubico