Europol Report Outlines Transition to Post-Quantum Cryptography for Financial Institutions

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Cornelia Riehle

On 21 January 2026, Europol and its partners published a joint report entitled "Prioritising Post-Quantum Cryptography Migration Activities in Financial Services". The report offers financial institutions a structured, risk-based approach to preparing for the transition to post-quantum cryptography (PQC). This involves using encryption methods that are designed to remain secure even against attacks from quantum computers. As advances in quantum computing are expected to compromise the long-term security of current encryption standards, financial institutions should start preparing for these future risks by transitioning to more secure cryptographic methods. They should plan the shift to quantum-safe security, determining priorities based on system vulnerability (quantum risk) and the time required for upgrades (migration time). This information can then be used to prioritise actions and implement changes step by step.

AUTHOR
Cornelia Riehle
Deputy Head of Section
Academy of European Law

Preprint eucrim 2026, Vol. 21(1)
ISSN: 1862-6947
https://eucrim.eu

According to the report, a critical first step is to identify all business use cases that rely on public key cryptography. This inventory enables the development of a prioritised transition roadmap, with the quantum risk of each use case being assessed based on three parameters:

- "Shelf life of protected data", which refers to how long the data remains sensitive;
- "Exposure", which indicates the extent to which data is accessible to potential attackers;
- "Severity", which reflects the business impact of a potential compromise.

When the quantum risk is assessed, organisations can prioritise actions based on the migration time of each use case, i.e., the complexity and timeline required to achieve quantum safety for a particular use case. The report explains how to assess risk using a Quantum Risk Score, set up a Migration Time Score, and determine migration priorities. It also provides example use cases to demonstrate the methodology and warns against cryptographic antipatterns in cybersecurity. These are commonly used but flawed practices that can increase vulnerabilities, operational risk, and long-term technical debt, particularly in financial institutions. Identifying and addressing them early on can strengthen security, improve cryptographic maturity, and support faster and more flexible migration to future-ready systems.

The report concludes that the transition to quantum-safe cryptography is not merely a technical upgrade. It is a strategic imperative that demands foresight, coordination, and disciplined execution across the entire ecosystem, and is necessary for businesses to position themselves as leaders in secure digital innovation for the quantum era.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by the European Union