HYPERFORM achieves its first milestone in quantum-safe data protection

The French cybersecurity consortium's demonstrator secures data at rest and in transit

# CYBERSECURITY

POSTED ON 01.29.26

The HYPERFORM consortium, a collaborative effort led by IDEMIA Secure Transactions, in partnership with five leading French cybersecurity partners (CryptoNext Security, PRIM'X, Synacktiv, CEA, INRIA) and the French National Cybersecurity Agency (ANSSI), has successfully showcased its quantum-safe data-protection prototype. This achievement represents a significant advancement in securing Europe's sensitive data, paving the way for a quantum-resilient future.

Advancing cybersecurity sovereignty in Europe

With the objective of developing France's first reference platform, the HYPERFORM consortium, funded by France 2030 and the European Union, focuses on real-world use cases for evaluating, testing, and demonstrating post-quantum cryptographic solutions, ranging from electronic identity document verification and secure banking transactions to long-term archiving of secret documents, collaborative work on confidential data, and sovereign cloud data backup. Beyond use case implementation, the project includes proactive security analysis and development of countermeasures to ensure that the solution will ultimately be resilient not only against quantum computers but also against sophisticated, contemporary attacks.

With its first prototype, the HYPERFORM consortium effectively showcases an encryption solution that protects confidential data throughout its entire lifecycle, from creation (data in transit) to long-term storage (data at rest). This involves replacing long-term data protection keys with quantum-safe hybrid keys and integrating algorithms based on NIST standards in a collaborative environment.

The success of this demonstration marks a major step towards securing data exchanges in critical workspaces and enabling long-term archiving of confidential data. By providing immediate and long-term protection, this solution directly addresses the critical "harvest now, decrypt later" threat.

Demonstrating post-quantum interoperability

A critical success of the demonstration is proving seamless interoperability between core components. The project validated that IDEMIA Sphere cryptographic libraries (running in the secure element) can communicate flawlessly with the CryptoNext Security library (used for PKI and integrated to PRIM'X encryption software). This is a vital step, as it shows that a robust, multi-vendor ecosystem is possible, preventing vendor lock-in and ensuring broad market applicability. The next steps of the project will see the development of a next-generation quantum-safe secure element, as well as the implementation of an alternative post-quantum cryptographic family and a crypto-agility demonstration.

Putting all the pieces together for quantum-safe data encryption

The HYPERFORM demonstration builds upon leading European data encryption software combined with robust key storage in secure elements and advanced encryption techniques.

- PRIM'X enhanced **two encryption software products** to support hybrid post-quantum cryptography for the demonstration: ZONECENTRAL, which encrypts the user's workstation and ensures only authorized users can access confidential data, and ZED! which protects collaboration between two users via encrypted containers.
- IDEMIA Secure Transactions provided **a quantum-safe secure element** featuring hardware accelerators specifically designed for post-quantum cryptography. It protects the solution's long-term keys and integrates the IDEMIA Sphere cryptographic library to enable quantum-safe cryptographic functionalities.
- CryptoNext Security's **cryptographic software library i**ncludes constant-time, side-channel-hardened implementations of ML-KEM and ML-DSA, among others, and has been certified by Synacktiv within the HYPERFORM project framework. It is used by the different software solutions of the project for data protection and PKIs when there is no need to use a physical secure element.

The strategic importance of projects such as HYPERFORM for Europe lies in developing sovereign quantum-safe solutions to safeguard critical data such as strategic archives, sovereign data, and industrial secrets. These solutions will be crucial for building digital trust in the post-quantum era and maintaining European independence in cybersecurity.