Solution Brief

Thales Quantum Resistant Solutions for Google Workspace

Enhanced Privacy and Confidentiality using Google Workspace Client-side Encryption for a Post-Quantum World

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Overview of Customer Challenges

In today's era of digital transformation and cloud-based applications, enterprises and cloud providers are increasingly seeking stronger cloud security and compliance measures. The challenge lies in ensuring enhanced privacy and confidentiality while maintaining control over encryption keys. This is particularly critical as quantum computing poses a significant threat to existing cryptographic technologies, making it imperative to adopt solutions that are quantum resilient.

Joint Solution by Google and Thales

To address these challenges, Google Workspace and Thales Cybersecurity Products offer enhanced privacy and confidentiality through Client-side Encryption. This solution empowers enterprise customers with full control over their encryption keys using Thales SafeNet Trusted Access and Thales CipherTrust Cloud Key Management.

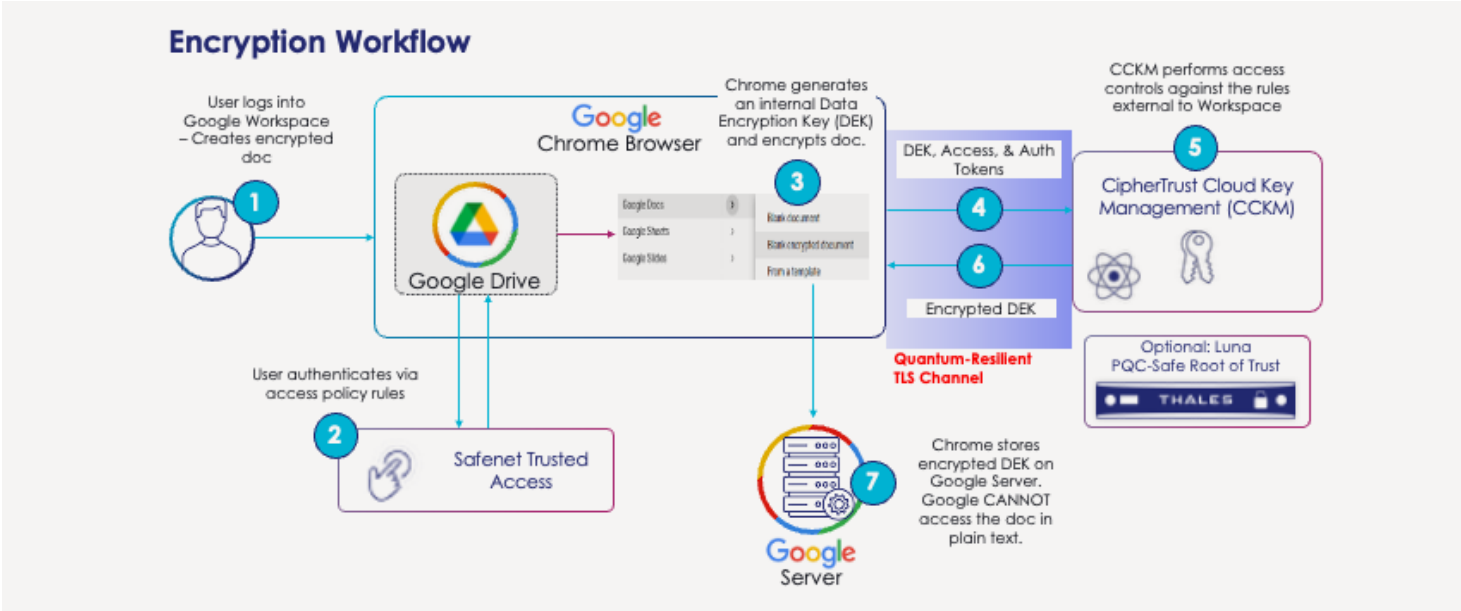
Why Security for Post-Quantum Computing?

The quantum resilient CipherTrust Cloud Key Management solution is fully integrated with Google Client-Side Encryption. This integration allows customers using Google Workspace Client-Side Encryption to achieve stronger security and lower deployment overhead by benefiting from Thales' end-to-end solution that protects identities and controls encryption keys separately from their sensitive data in the cloud. Luna HSMs can also be integrated with CCKM as a FIPS 140-3 Level 3 quantum-safe solution for an optional root of trust.

Thales has demonstrated leadership in post-quantum cryptography (PQC) with the co-development of the FN-DSA Algorithm (formerly known as Falcon) one of four selected by NIST for standardization, including two for digital signatures, a new PQC standard for digital signatures. Thales Luna Hardware Security Modules (HSMs) and Thales High Speed Encryptors (HSE) network encryption solutions already offer quantum-safe capabilities built into current product offerings, including native support for PQC algorithms, and Thales actively collaborates with technology partners to showcase its readiness for the PQC era.

How the Joint Solution Works

- Client-Side Encryption: Protects user privacy by enabling service providers to host encrypted data without decrypting it. Authenticated users can retrieve and decrypt their files using customer-provided data encryption keys.
- External Key Management: Google Workspace supports integrating with an EKM to wrap the Data Encryption Key (DEK) with a Key Encryption Key (KEK), ensuring secure key management.
- Quantum-Resilient TLS Channel: Thales has upgraded the TLS connection between CipherTrust Cloud Key Management and Google Chrome to be quantum-resilient, using the Hybrid X25519 Kyber768 algorithm for key encapsulation.



Summary of Benefits

The integrated solution from Thales offers several tangible benefits:

- Enhanced Security: Reduces the risk of data breaches and penalties by allowing organizations to own their access security and key management.
- Smooth Deployment: Single vendor integration with Google Workspace ensures quick and smooth deployment.
- Quantum Resilience: Provides protection against quantum attacks without changing the user experience.

Flexible Deployment Options

CCKM for Google CSE can be deployed in the cloud, on premises, across hybrid environments, and as a service. To enable a free trial, please visit the Community Edition from Google Cloud Marketplace or CCKM as a service from the Thales DPoD Marketplace.

Take a self-guided product tour of Thales cloud key management solutions for Google.

Environmental, Social, and Governance (ESG) Commitment

Thales is dedicated to reducing its carbon footprint, power consumption, and operating costs through eco-design, aligning with Thales' ESG commitment to a greener, safer world.

About Thales

Thales is a global leader in cybersecurity, helping trusted organizations protect critical applications, data, identities, and software at scale. Through Thales' integrated platforms, customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

About Google Workspace Client-side Encryption

Google Workspace Client-side encryption helps customers strengthen data confidentiality and address data sovereignty and compliance requirements. Customers have direct control of encryption keys and the identity service they choose to access those keys. Customer data remains indecipherable to Google, while users can continue to collaborate, access content on mobile devices, and share encrypted files externally.

About Google Workspace

Google Workspace is a unified collaboration and communications platform that provides companies of all sizes with everything they need to connect, create, and collaborate. Google Workspace includes apps such as Gmail, Google Meet, Calendar, Drive, Docs, Sheets, Slides, and more. Learn more at workspace.google.com