

Qanapi Flow - Key Management Service FAQs

Thank you for your interest
in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V, TIPS, Software Solutions and Services - OMNIA Partners, Public Sector and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Qanapi, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/QanapiResources



Join Events & Webinars:
carah.io/QanapiEvents



Discover Technology Solutions:
carah.io/Qanapi



Learn About Procurement:
carah.io/QanapiContracts



Connect With Our Team:
Qanapi@carahsoft.com
571-591-6210

Key Management Service **FAQs**

What is client-side encryption?

Client-side encryption (CSE) allows organizations to encrypt their data stored on Google Workspace products before it ever reaches Google's servers.

How does a Key Management Service assist with Google Workspace CSE?

A Key Management Service (KMS) separates encryption keys from the data stored in Google Workspace. This enables organizations to maintain full control over their data and ensure that sensitive information remains inaccessible to Google.

How much does Qanapi Flow's Key Management Service cost?

\$15 per user per month — no hidden costs or usage-based variables. Email sales@qanapi.com for more information.

What level of support does Qanapi offer?

Support is available 24/7. Your mission's success is our priority — contact us anytime at support@qanapi.com.

Which Google Workspace products does Qanapi Flow integrate with?

Organizations can enable client-side encryption on Google Drive, Docs, Sheets, Slides, Calendar, and Meet. Qanapi Flow integrates seamlessly to store and manage encryption keys across any of these Google Cloud solutions.

Does a KMS help my organization meet regulatory compliance requirements?

Yes, a KMS provides organizations with control over their encryption keys for data stored with a cloud provider. Regulations and frameworks such as HIPAA, CJIS, CMMC, PCI DSS, DoD IL, ITAR, and FedRAMP call for controls like key rotation reporting, which can be provided by Qanapi.

Are data residency and sovereignty controls included in Qanapi Flow's KMS solution?

Yes, we ensure that your encryption keys are stored within the continental United States to meet data residency requirements.

What is Qanapi's data protection strategy?

We utilize the latest data encryption strategies, the same ones used by the U.S. government and military. Our KMS employs a quantum-resistant, FIPS 140-2 Level 1 encryption service to manage your organization's encryption keys — crypto-agile by design.

Which cloud environments are supported by Qanapi?

Organizations can operate in multi-tenant or private cloud environments on Google Cloud. Teams using Qanapi Flow can package and deploy any cluster of U.S. government-approved cloud services as a private cloud.

Does Qanapi support any identity providers (IdPs) for client-side encryption?

Yes, we support Google's Identity Service, along with giving teams the ability to configure Qanapi Flow for any preferred IdP that is supported by OpenID Connect.