EASY YET SECURE ENCRYPTION IN GOOGLE WORKSPACE

Use of i4p's Google Client-Side Encryption module with the Trident HSM on premise provides a higher level of protection for your data stored in the Google Workspace, without interrupting the user experience.

The challenge: data security in Google Workspace

Google Workspace is used by many companies around the world. It offers a reasonable ROI and meets the requirements of most companies. It is flexible, scalable, and easy to use. It allows users to collaborate in real-time and store, share and access files in the cloud from any device, enhancing productivity.

However, there is one concern about this service: privacy. Google is one of the "Big Brothers". You know what it's like when you mention something in a chat or email, and half an hour later the related product comes up in Google ads in your browser...

Data protection is important in the life of a company from several aspects. Confidential business information, such as information about patented technology or contracts, cannot be leaked, and customers' and employees' personal data is just as valuable information. Protecting this information properly is not only in the company's own well-conceived interest, but it is also required by regulations such as the GDPR. Companies receive significant fines if their systems are breached, and their data is leaked.

According to the GDPR, the controller of the data shall "implement appropriate technical and organizational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".

This is binding for all companies in the EU, just like the "cookie consent" that pops up on every website. The "necessary safeguards" are more difficult to check, but if it is discovered during an audit, the company can be fined for not storing the data in accordance with the regulations.

GDPR is one of the strictest privacy regulations in the world, but similar regulations are being passed around the world. An analysis by Gartner predicts that by 2023, 65% of the world population will have its personal data covered under modern privacy regulations. Certain organizations are subject to even stricter regulations, if they operate in a highly regulated industry, like aerospace, defense, financial services, or government, for example.

The solution: Google Client-Side Encryption

The Google Client-Side Encryption (CSE) module with the Trident HSM can help companies in meeting regulations and enhancing the protection of their data. With CSE you have direct control of encryption keys, helping you strengthen the confidentiality of your sensitive or regulated data. Currently, Google enables the Client-Side Encryption feature for the customers who chose the Google Workspace for Education Plus or the Google Workspace for Enterprise pricing plan, but this option may be extended to other customers in the future.

CSE can be used on the data you store in Google Drive, including files created with Google Docs Editors (documents, spreadsheets, presentations) and uploaded files, like PDFs and Microsoft Office files. You can use CSE for Google Meet audio and video streams, including screen sharing, and the data transmitted between meeting participants and Google. Google Calendar data can be encrypted with CSE in beta mode currently, including event description, attached Drive files, and Meet audio and video. Google started the CSE beta for its Gmail service and CSE will be introduced for other Google services in a later release.

However, it is very important not to just use the encryption, but to carefully guard the keys used for encryption afterwards. **i4p's CSE module with Trident HSM offers a high level of protection for these keys.** The effectiveness and reliability of the Trident HSM is verified by its Common Criteria EAL4+ certificate, the international security certificate recognized worldwide.

With its Secure Multi-Party Computation capability, the Trident HSM can offer even more than an "ordinary" HSM. It can organize multiple HSM devices into a distributed cluster and manage the cryptographic keys in a distributed way within the cluster. This means that the key data cannot be identified independently on each of the devices, so even if one of them is taken physically, the information obtained is worthless. Due to this revolutionary innovation, Trident HSM offers the highest level of protection required in the world of business.

With our solution, you have the option to choose from several types of algorithms for the encryption. For the encryption of your most sensitive data, you can pick the symmetric AES

or the new asymmetric Kyber algorithm that are both quantum-resistant. This is important because according to the experts of the field, quantum computers might become so advanced within a few years that they will be able to decrypt information that has been encrypted with one of currently used algorithms. However, some algorithms are already quantum-resistant, and will provide proper protection for your data not only now but in the future, too.

Results: secure encryption with the click of a button

CSE with Trident HSM is easy to deploy, and after the short deployment process, your users will be able to turn on the encryption in the Google services with one click to encrypt the Google Drive and Google Calendar data as well as Google Meet audio and video streams. The CSE function enables the web browser to encrypt the information before sending it to Google, guaranteeing end-to-end protection of sensitive data.

This keeps your data safe and hidden from Google and online attackers: if your data is encrypted and the encryption keys are stored safely, the attackers cannot access sensitive information even if they manage to infiltrate your Google systems and steal your (encrypted) data.

This solution provides you a convenient way to address all your data sovereignty and compliance requirements. It gives you control over your encryption keys while letting you leverage the processing capabilities and power of Google Workspace, without interrupting the user experience.