cryptas

we protect identities.

CUSTOMER STORY

ENCRYPTING BUSINESS-CRITICAL AND SENSITIVE DATA

WHY A MAJOR EUROPEAN ENERGY PROVIDER ENCRYPTS ALL OF ITS CUSTOMERS' BUSINESS-CRITICAL AND SENSITIVE DATA, AND HOW IT IS DONE

CUSTOMER CHALLENGE

Major European energy providers, like most businesses in the world, rely on a state-of-the-art IT infrastructure to offer and deliver competitive services to their customers. A mix of cloud services from global suppliers such as Amazon Web Services (AWS), Google's Cloud Platform (GCP), Microsoft Azure, and Salesforce is a natural part of such an infrastructure. For both strategic and legacy reasons, a wide range of in-house IT systems is equally part of this type of IT infrastructure.

Such a heterogeneous and dynamic IT infrastructure brings challenges in terms of IT security: Regulatory requirements such as GDPR and Schrems II as well as the protection of critical digital assets against unauthorized access must be assured at all times, and for the entire infrasturcture which is constantly changing. Critical assets of an energy company include business intelligence data, financial planning, and power grid statistics as well as HR data.

GDPR & Schrems II

Under the European General Data Protection Regulation (EU2016/679, GDPR) companies are obligated to protect personal data. The Court of Justice of the European Union confirmed and clarified in its July 2020 judgment (ECLI:EU:C:2020:559) "Schrems II" that the unrestricted transfer of personal data to IT service providers outside the EU is illegal.

For EU-based companies, this means:

- Refraining from using foreign-owned cloud services to process and store their customers' personal data, or
- Encryption at source and uploading only encrypted data to the cloud while managing and storing the encryption keys securely within EU jurisdiction and permanently out of reach of foreign parties or governments.

THE STRATEGY

The energy provider has adopted a data security protection strategy that encrypts all data at rest, regardless of the storage location. Encryption must be seamless and automatic for end-users across all applications that generate, process, or store data on-premises and in the cloud. The encrypton must, of course, rely on robust and proven cryptography.

A key management service that generates and manages keys for encryption at rest forms the core of the data protection strategy. The key management service is to be protected by Hardware Security Modules (HSMs), and, as explained above, it must remain inaccessible to non-EU entities.

THE SOLUTION

To implement the data security protection strategy, the customer chose Thales CipherTrust Manager together with Transparent Encryption, Cloud Key Manager (CCKM), and Database Protection. This solution provides centralized key management for cloud application protection, data-at-rest encryption, and transparent database encryption, all with privileged user access control and detailed data access audit logging. "Bring your own key" and "hold your own key" schemes are also supported for large cloud platforms.

This allows digital assets to be protected wherever they reside, such as on-premises, across multiple clouds, and in Big Data and container environments. CRYPTAS was selected as an integrator to implement the solution at the customer site. The CipherTrust Key Management Service is provided and operated by CRYPTAS to ensure business continuity and high availability across all sites and applications. Entrust nShield Connect Hardware Security Modules are used as the root of trust.

CRYPTAS is also engaging in the consultation of each project and group at the customer on how to meet their regulatory duties and protect their critical assets. In each case, a standardized approach is followed between the CRYPTAS consultants and the responsible case team at the customer.