Hewlett Packard Enterprise

Case Study

bankart

Slovenian payment processor ensures PCI compliance with HPE ESKM and HPE NonStop

Protects PII/PAN with volume-level encryption and integrated key management

Objective
Ensure PCI compliance for processing tens of millions of payment authorizations per month

Approach
Deploy HPE Enterprise Secure Key Manager (ESKM) to enable automated key management for encrypted data-at-rest volumes on HPE NonStop servers

IT Matters
- Automatically generates and protects 88 business-critical encryption keys
- Greatly reduces risk by automating daily backup of encryption keys instead of the previous monthly manual process
- Maximizes protection by regenerating 6 keys daily for encrypted backups
- Enables policy-based controls that automate key replication, load-balancing, fail-over and provides digitally-signed logs for audits

Business Matters
- Ensures PCI compliance for 25 million transactions per month with volume-level encryption and FIPS-140-2, level 2 validation for key management
- Streamlines PCI audits, providing clear proof that sensitive PII/PAN data is protected
- Provides secure payment authorizations for 25 financial institutions across eastern Europe
- Helps maintain compliance with regulatory mandates, & reduces operational costs with a central management approach

Securing production and backup data

People buy things with a credit card or use their debit card to withdraw money from an ATM all the time. But does anyone ever think about what happens "behind the box"? Few people do, and that's good. It means the myriad systems and processes to authenticate identity, verify funds, and approve the transaction are working. Most important, they're working securely to protect your personally identifiable information (PII) and primary account number (PAN).

For dozens of leading banks and other financial institutions throughout Slovenia and across many parts of Bosnia-Herzegovina, Kosovo, Macedonia, and Serbia, secure payment transactions are handled by one company: Bankart. This trusted financial clearing house processes 25 million payment transactions per month generated by the full gamut of payment systems, including ATM and point-of-sale (POS).

Like all financial institutions, Bankart must comply with strict European regulatory requirements and the Payment Card Industry Data Security Standard (PCI DSS). PCI dictates

> "For volume-level encryption, HPE ESKM is really the only choice to provide key management. With ESKM, we have an efficient and secure solution because we centrally manage all encryption keys, including those for our encrypted backups."
>
> — Igor Šilc, Systems Engineer and NonStop Administrator, Bankart

that all data-at-rest, whether on production systems or backups, must be encrypted to protect PII and PAN information.

Bankart's payment infrastructure is built on the ACI Worldwide BASE24 suite of applications. However, BASE24 does not provide native encryption. To meet PCI DSS requirements and ensure continuous availability of its mission-critical BASE24 applications, Bankart deployed HPE NonStop servers with volume-level encryption (VLE) for approximately 1 terabyte of production data. Equally important was finding a solution to generate and securely manage the encryption keys for all disk volumes on NonStop, as well as the company's secure backup environment, BackBox. For this, the company chose HPE Enterprise Secure Key Manager (ESKM), which provides centralized key management with FIPS-140-2 Level 2 validation.

Igor Šilc, a systems engineer and NonStop administrator at Bankart, notes, "For volume-level encryption, HPE ESKM is really the only choice to provide key management. ESKM was also ideal for Bankart because we could use it with our BackBox solution. In the past we did some encryption on backup tapes, but the keys were stored in a flat file, which was not very secure. With ESKM, we have an efficient and secure solution because we centrally manage all encryption keys, including those for our encrypted backups."

Prevents security vulnerabilities

Bankart deployed two ESKM appliances, one for each of its production NonStop servers, as well as a third ESKM appliance for a test and development NonStop server. BackBox uses keys stored on the NonStop storage subsystem that are also managed by ESKM. Recently, Bankart upgraded to the latest version of ESKM with additional security capabilities, including support for advanced cryptographic protocols such as transport layer security (TLS).

Robert Bolha, also a systems engineer and NonStop administrator for Bankart, remarks, "It's very important for Bankart to stay current with all the latest ciphers, including new versions of SSL and TLS. Upgrading ESKM strengthens our protection against security vulnerabilities in our environment."

He adds, "The latest ESKM also allows us to schedule daily backups of the encryption keys. Previously that was a manual process, so we only backed up the keys once per month. If anything ever went wrong with the keys, we would have a gap of several weeks between backups. Now, since we have backups every day, there's only a gap of a few hours, which reduced our risk significantly."

HPE Security professional services provided guidance and assistance throughout the ESKM upgrade. In particular, Bankart took advantage of the HPE Security, Data Security Quick Start Services, which provides an onsite Data Security Services Delivery Manager to ensure a smooth and stable ESKM deployment. The Delivery Manager performed a series of health checks to validate the installation and all integration points, and shared best practices with Bankart IT staff on how to manage ESKM for maximum availability and efficiency.

"We were very happy with the knowledge and experience of HPE services," says Bolha. "We learned a lot and everything went very smoothly, without any problems. The knowledge and best practices we gained were essential to helping us achieve the highest possible compliance levels and realizing the full benefits of ESKM."

Instant, automated key generation

Bankart configured each production NonStop server with 20 logical volumes, fully encrypted using NonStop's native VLE capabilities. Because each logical volume comprises two mirrored physical disks to ensure continuous availability, the two NonStop servers contain 80 disks, and the company generates an encryption key for each disk. With the two production NonStop servers, plus eight disks on the test and development system, ESKM manages a total of 88 encryption keys.

In addition, Bankart generates one encryption key for each backup—six per day. ESKM automatically generates new keys for each backup every day. Also, any time the company performs maintenance on a NonStop disk, ESKM regenerates an encryption key. And once per year, Bankart creates a whole new set of encryption keys for the encrypted disks on NonStop.

"All we do is issue a simple command on NonStop to encrypt the disk and the server requests a new key, which ESKM generates automatically," Bolha explains. "Encrypting each disk takes about 30 minutes, but the key generation is instantaneous. Because we encrypt one disk at a time, the entire process is completely transparent to our users."

Case study
Bankart d.o.o.

Industry
Financial services

Customer at a glance

Application
- Mission-critical payment processing for ATM, point-of-sale (POS), SEPA, and e-invoice transactions generated by 25 banks and financial institutions across Eastern Europe

Hardware
- HPE NonStop
- HPE Enterprise Secure Key Manager (ESKM)

Software
- ACI Worldwide BASE24

Services
- HPE Security – Data Security Quick Start Services
- HPE Technology Support – Health Check for NonStop

PCI-compliant protection for sensitive data

One of the most important benefits of ESKM is that it helps Bankart ensure PCI compliance without requiring day-to-day administration. This streamlines regulatory audits and frees up IT staff to focus on other value-added projects for the business.

Šilc comments, "The combination of volume-level encryption on the NonStop servers and ESKM helps us prove to PCI auditors that Bankart is serious about compliance—that we are doing all we can to secure our sensitive data-at-rest. Any time the auditors come in we have to show them how the disks are encrypted and the keys managed. With ESKM and NonStop VLE, it's very easy to demonstrate that we satisfy PCI requirements."

Bolha concludes, "ESKM is a very stable product and everything is automated—all we do is check to make sure the systems are working properly. We've never had any problems with the ESKM appliances. They just do their job, so we are very happy."

Learn more at
hpe.com/software/datasecurity

Sign up for updates

Hewlett Packard Enterprise

4AA4-1203ENW, August 2016, Rev. 2