Success Story

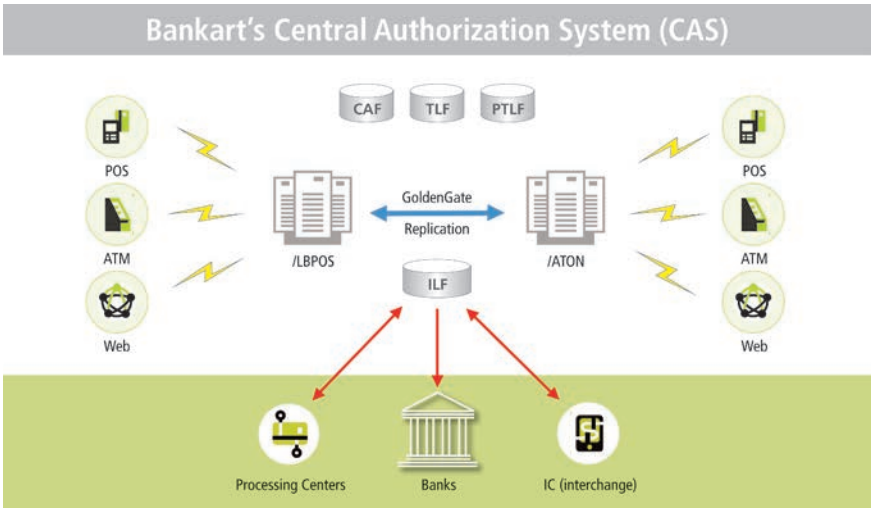
PCI and GDPR Data Protection Requirements Met With Zero Downtime on Payments Processing Network

Bankart is a card payments processing center headquartered in Slovenia that serves 23 banks and other institutions across six countries and in four different currencies. Bankart's mission is to provide reliable, secure and cost-effective transaction processing services involving various bank payment instruments to its customers.

With its Central Authorization System (CAS), Bankart processes over 30 million ATM, POS, internet, and mobile transactions every month on ACI's Base24 Classic. Bankart also controls and manages ATM and POS networks for most of their banks. In addition to payments processing and network management services, the CAS also h andles card validation, PIN verification and, in case a bank is experiencing technical issues and is unable to process an authorization, Bankart will conduct off-line authorizations for them.

Challenge: PCI and GDPR Compliant Data Protection

Since Bankart's Central Authorization System must be up and running 24/7, it is hosted on highly-available HPE NonStop servers in a dual site configuration working in active-active mode. Some of the data is being replicated to back office systems running on Windows servers. Both authorization servers are connected to the POS network, ATM network, and web interfaces for online transactions, all of which are routed to the banks that Bankart serves, other processing centers, and interchanges. To manage all of this, various databases, files, and logs with card holder data have to be maintained.



Quick Facts

- Payments processor handling over 30 million transactions per month.
- Now compliant with PCI and GDPR requirements.
- Highly flexible and scalable solution implemented quickly and easily.

Secure your Growth with comforte

With more than 20 years of experience in data protection on truly mission-critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: data. comforte's Data Protection Suite, SecurDPS, has been built from the ground up to best address data security in a world that is driven by digital business innovations, empowered customers, and continuous technology disruptions.

We are here to help secure your growth by providing expertise, an innovative technology suite, and local support.

To learn more, get in touch with a comforte representative today by visiting www.comforte.com/contact/.

"This entire process was carried out while the system was live with-out any of Bankart's partners or customers noticing any difference in service levels".
– Michael Deissner, CEO at comforte

Throughout Bankart's network, there are several files and databases that contain cardholder data, all of which need to be protected from both external threats and accidental exposure to unauthorized insiders. Bankart already employed Volume Level Encryption to protect cardholder data, however VLE is only useful when physical hard drives leave their premises. If a malicious actor infiltrates the system undetected, then the data is left in the clear and vulnerable. An additional level of protection was required so that the data would still be secured, even in the event of a breach.

Requirements

Given the complex network configuration and the high level of service that customers expect, Bankart had very high standards for the solution that would protect the cardholder data they manage:

1. **High Availability –** able to integrate on a live system with zero down-time and available 24/7
2. **Highly Configurable –** compatible with a diverse system on a file and record level
3. **Ease of integration –** little or no changes to applications or source code
4. **Scalability –** should be possible to extend the solution to other systems within the company
5. **PCI and GDPR compliance –** cardholder data must be rendered unreadable wherever it is stored

Solution

Bankart chose SecurDPS from comforte because it fulfilled all of the above requirements and more. It was easy to implement in its complex IT environment without any changes to source code or down time, it properly secured cardholder data in accordance with PCI and GDPR requirements, and it is a scalable, enterprise-wide solution that can later be expanded to other systems in the organization.

Data-Centric Security

SecurDPS reduces business risk as it replaces in-the-clear sensitive data with a token value that is meaningless if it is exposed. A data-centric security strategy protects the data itself so that even if all other security measures fail, the data at the core will still not be exploitable.This also fulfils the PCI and GDPR requirements for no sensitive data on core enterprise components. Furthermore, tokenized data is protected from accidental exposure to unauthorized insiders and third party vendors as it can only be accessed with proper authorisation. This helps reduce dependency on compensating controls as a temporary measure to pass security audits and fulfils the PCI and GDPR requirements that sensitive data only be accessible on a need-to-know basis.

Data Protection with a Light Footprint

Bankart processes on average 1.4 million transactions a day, so they needed a solution that could be implemented without interrupting the business or affecting service levels. Tokenisation offers protection without the performance pitfalls of classic encryption by preserving the format and utility of the protected data so that business applications and analytics can operate on tokens rather than sensitive data in the clear.

In addition, SecurDPS is highly flexible and scalable so it could be implemented without any changes to the source code. This meant that the solution could not only be implemented in a matter of a few months, it was also done without affecting service levels.

Benefits

The benefits of this project go beyond fulfilling PCI and GDPR requirements for data protection. In the unlikely event of a data breach, all sensitive data will be unreadable and have no exploitable value to hackers, which greatly reduces the impact of a potential breach.

Furthermore, tokenised data will help secure Bankart's growth as it is now much easier for them to exchange data with partners and customers while keeping sensitive data protected. Since they no longer rely on compensating controls and can do business much faster, they will be able to get the most out of the rapidly growing market and provide processing services to more customers than ever. As an added benefit, SecurDPS enabled Bankart to be more cost effective by making volume level encryption obsolete.

Thanks to the successful implementation of SecurDPS meeting all the project requirements, Bankart plans to extend the solution to other systems across the organization.