COMFORTE DATA PROTECTION FOR ACI RETAIL PAYMENTS SOLUTIONS

SEAMLESS SECURITY FOR PCI DSS V4.0 COMPLIANCE AND BEYOND

SOLUTION AT A GLANCE

- Comprehensive PAN protection through field-level tokenization and encryption
- Compliance with PCI DSS v4.0 security mandates for data at rest via field-level tokenization
- Seamless integration with BASE24-eps applications endorsed by ACI for secure transaction processing
- Native support for BASE24-eps on AIX and Linux platforms
- Simplified auditing and reporting to support PCI scope reduction using data-centric security
- Ability to enable secure analytics on tokenized data

INTRODUCTION

Payment processors, merchants, acquirers, and other financial services organizations face growing challenges in safeguarding sensitive payment data from advanced cyber threats, while also striving to meet stricter privacy regulations. ACI Worldwide partners with comforte AG to support payments security and PCI DSS v4.0 compliance for ACI's Retail Payments Solutions (RPS) using BASE24-eps payment switches on AIX and Linux systems. By integrating comforte's advanced tokenization and encryption, ACI RPS users effectively secure all sensitive payment data at rest and ensure adequate PCI DSS v4.0 compliance while maintaining performance, scalability, and uninterrupted operations in high-transaction environments.

COMPLIANCE AND SECURITY CHALLENGES

PCI DSS v4.0—mandatory by March 31, 2025—introduces stricter requirements for securing PANs and other sensitive payment data at rest. Non-compliance with PCI DSS brings numerous risks, with examples like financial penalties reaching $100,000 monthly, potential exclusion from payment card networks, and tarnished brand image. Traditional methods like disk-level encryption now fall short under PCI DSS v4.0 requirements for field-level protection, as it leaves decrypted data exposed after processing. For example, transparent data encryption (TDE) only protects data on disks, which increases vulnerabilities and exposes payment systems to insider threats and breaches.

High-transaction volumes in BASE24-eps environments face added challenges since real-time encryption often introduces high latency, which degrades payment system performance and user experience. Additionally, legacy security technologies hinder modern analytics by requiring decryption for fraud detection, insights, and reporting processes—ultimately creating bottlenecks and scalability issues with large datasets and real-time operations.

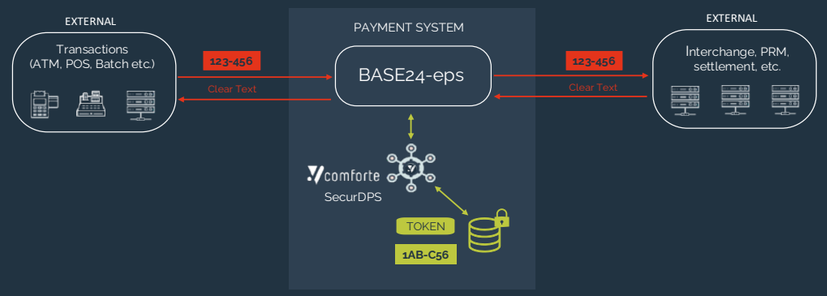
DATA-CENTRIC SECURITY DESIGNED FOR BASE24 ON AIX AND LINUX

Comforte offers the only ACI Worldwide-endorsed solution for securing data at rest in ACI RPS products with BASE24-eps payment switches on AIX and Linux systems. Rigorously tested and optimized for ACI's architecture, comforte Data Protection (SecurDPS) enables ACI RPS customers to implement robust security measures, without the inefficiencies and financial impact of compensating controls or unapproved third-party solutions. This native integration capability delivers a data-centric approach that exceeds PCI DSS v4.0 requirements for data at rest. Tokenizing sensitive data within BASE24-eps workflows renders PANs unreadable to unauthorized parties while ensuring compatibility with other payment processes, reducing PCI compliance costs, and simplifying audit processes. The collaboration between ACI and comforte ensures minimal implementation schedules plus proven solutions for a large variety of configuration and operational scenarios.

COMFORTE DATA PROTECTION FOR ACI RPS

Comforte delivers advanced data-centric security solutions to safeguard cardholder data and other sensitive information throughout the entire transaction lifecycle. With full integration into ACI Retail Payments Solutions like BASE24-eps, comforte Data Protection simplifies compliance with PCI DSS v4.0 and strengthens overall payment system security posture through end-to-end protection with low latency—simultaneously preserving BASE24-eps performance. Using simple parameter files, ACI RPS customers can also extend data-centric security beyond PCI DSS v4.0 to address other regulatory compliance challenges and further protect additional cardholder data elements or sensitive payment information.

Comforte Protection Nodes are stateless and can be deployed near payment applications across on-premises, cloud, or hybrid environments and architectures. By securing data at the field level, format-preserving tokens retain the structure and length of sensitive PANs to ensure compatibility with legacy systems and mitigate disruption to processing logic. Comforte Data Protection is future-proof with new ACI RPS product versions and is built with a unique architecture optimized for high transaction volumes, while also including failover mechanisms to deliver enterprise scalability and ensure continuous, reliable payment system performance.



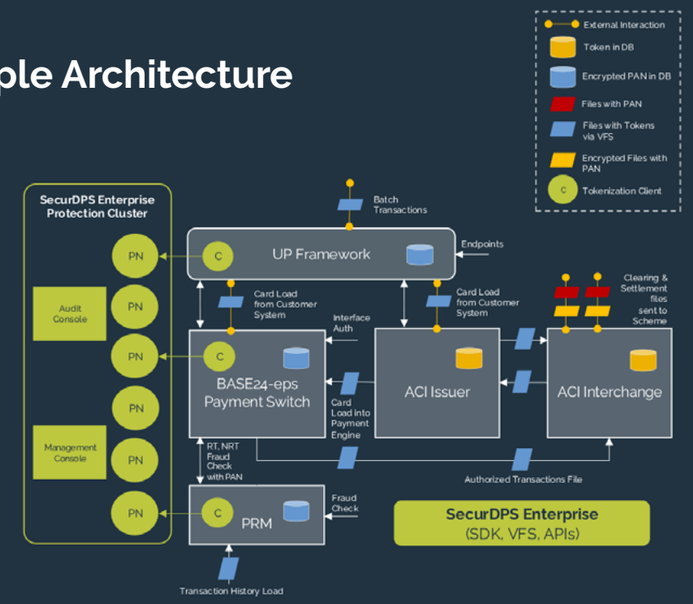
BENEFITS FOR ACI RPS CUSTOMERS

- **Compliance with PCI DSS v4.0:** PANs are replaced with valueless tokens that are unreadable in storage (Requirement 3) and all interactions are audited
- **Stronger Payment System Security:** PANs remain protected in the event of a data breach
- **Compatibility with Fraud Detection and Analytics:** Uninterrupted analysis of transaction patterns and customer behavior by external systems
- **Ease of Integration:** Native support for BASE24-eps on AIX and Linux for fast deployment with minimal changes to existing configurations, architectures, and workflows

IMPLEMENTATION

Comforte Data Protection integrates with BASE24-eps on AIX and Linux platforms through SmartAPIs, flexible language-specific SDKs, and Virtual File Systems (VFS) to deliver file-based tokenization—while also supporting integration into non-ACI applications if required. As a result, this enables real-time data protection with minimal impact on existing applications and workflows. In real-time integrations, comforte's Protection Cluster can be integrated to different payment system components like the BASE24-eps payment switch, UPF, PRM, and other ACI-supported product environments to tokenize all sensitive cardholder data elements before processing. In batch processing, the VFS module tokenizes sensitive cardholder data during file transfers moving to and from the payment switch. UPF tokenizes all incoming transactions—and can de-tokenize if necessary—before passing the data along to BASE24-eps applications. Since the clearing system can read protected cardholder data, tokenized transaction history can therefore be sent to fraud systems—like PRM—without any sensitive data exposure.

Sample Architecture



Secure Your Payment Systems

Meet PCI DSS v4.0 compliance and enhance your data security.

Request a Demo >>