cpl.thalesgroup.com

THALES
Building a future we can all trust

Data Protection on Demand (DPoD): Payment Services

Point to Point Encryption (P2PE)

Protecting payment transaction data in motion

P2PE is deployed to protect vulnerable zones or segments in the payments infrastructure. In point of sale (POS) environments, it protects data from the point of capture in the merchant environment to the next point of processing which is normally a payment gateway or acquirer. Traditional POS systems are increasingly adopting P2PE to avoid vulnerabilities relating to the cleartext transmission of magnetic stripe and chip card track data. Mobile point-of-sale (mPOS) solutions inherently deploy P2PE because they involve untrusted devices (mobile phones or tablets) and untrusted networks (the internet) and the risk of mobile malware having access to cleartext account data is unacceptably high.

P2PE encrypts data at the point of capture (i.e. at the POS terminal or mPOS reader) and this data is maintained in an encrypted state thereafter and is only ever able to be decrypted inside the secure compound of a Hardware Security Module (HSM), leveraged typically by a service provider or gateway in the transaction processing value chain. The key benefit to using P2PE is that the merchant cannot decrypt the data without authorized access to the cryptographic keys.

Benefits of P2PE

Security

- Use encryption to secure payment card data while in transit between the terminal and acquirer as part of a POS transaction

Compliance

- P2PE deployment significantly reduces the scope and cost of PCI compliance for merchants

Brand protection

- Inherently reduce the risk of a payment data breach, which would likely cause considerable damage to reputation and brand

Efficiency

- Simple to deploy, easy to scale, highly secure in use and transparent to merchants

Leading payment security innovation

For 30+ years, Thales has led innovation in the global payment ecosystem

- Personalization services for cards and mobile secure elements
- Digital banking and payment services
- Largest provider of payment HSMs globally
- Strong participation in standards bodies
- Integrations with all major payment applications

Working from our deep roots in the payment processing industry, Thales recognized the growing need for payment in the cloud services, and has added a P2PE service as part our flagship Data Protection on Demand (DPoD) platform. The P2PE Service is available with the free 30-day evaluation of DPoD.

DPoD is a cloud-based platform that provides a wide range of on-demand Luna Cloud HSM, CipherTrust Key Management, and now Payment services through a simple online marketplace. With DPoD, security is made simpler, more cost effective and easier to manage because there is no hardware to buy, deploy and maintain. Click and deploy the protection you need, provision services, add security policies and get usage reporting.

Leveraging HSMs for P2PE

The PCI Security Standards Council P2PE requirements call for the use of hardware security modules (HSMs) with an appropriate security rating to protect access to the master keys. The P2PE Service utilizes a FIPS 140-2 Level 3 Luna Cloud HSM that protects the Base Derivation Key (BDK) master keys and enables a PCI P2PE compliant decryption environment to be established.

The P2PE Service uses cloud-based hardware security to perform two critical functions of the overall P2PE payment transaction process.

Base Derivation Key (BDK) management

Every payment network uses its own BDK encryption keys and all payment terminal using that network needs the relevant BDK in place before it can start to process transactions. The keys used to encrypt payment data are derived from the BDK and typically change for each transaction.

The service enables P2PE solution providers to use the keys generated for subsequent injection into the payment terminals as the initial BDK as part of the commissioning process.

Payment data decryption

Card data is encrypted at the point of card acceptance and remains in that state as it travels to the payment gateway and the processor. Interception of the data will be of no value to an attacker since the keys to decrypt are not accessible.

Once the data reaches the secure confines of the DPoD P2PE service, the data is decrypted and passed to the bank or processor for authorization.

Features and benefits

Security and Protection

- Protects data in transit and blocks malware that "sniffs" and "captures"
- BDK master key management – generation, distribution & storage
- DPoD uses FIPS 140-2 Level 3 certified hardware for its cryptographic operations to ensure no cleartext exposure of keys or sensitive data
- ISO 27001 and SOC 2 certified

Easy to Integrate

- Container (which runs on customer premises) provides a REST service that communicates with the cloud service
- Assists with the certification of the overall PCI P2PE solution managed by the solution provider

Easy to Manage

- No upfront investment
- Subscription service with 99.95% SLA
- Managed by Thales, no need for specialist in-house security skillset
- Scale up or down to meet dynamic workload requirements

© Thales - Septmeber 2022 • RMv7