PCI P2PE モジュラーアプローチによる クレジットカードセキュリティ対策

2018/6/22

ネットムーブ株式会社

高田　理己

takada@netmove.co.jp

What‘s provided by NetMove?

SaAT Security&Assistant Tools

セキュリティサービス

決済サービス

https://www.saat.jp

PCI Security Standards Council

PCI Security Standards Council
POINT-TO-POINT ENCRYPTION™

- ✓ IC（EMV）化対応済み
- ✓ PCI P2PE 認定取得済み（国内初!!）

NetMove CORPORATION

本日のお話し

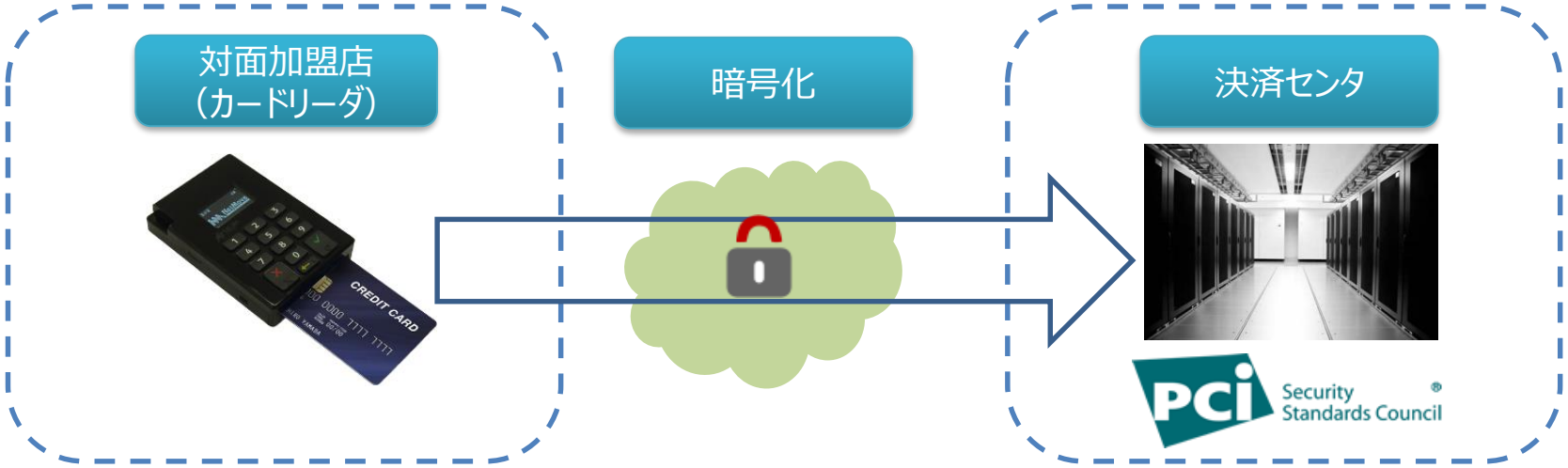
- ✓ PCI P2PE 概要
- ✓ PCI P2PE コンポーネントとソリューション管理
- ✓ PCI P2PE Key Management Technique

PCI P2PE について、まずは概要から..

PCI P2PE（Point To Point Encryption）とは？

SaAT Security&Assistant Tools

- ✓ 対面加盟店向けソリューション
- ✓ Point To Point でカード情報を暗号化



NetMove CORPORATION

Why do we need P2PE?

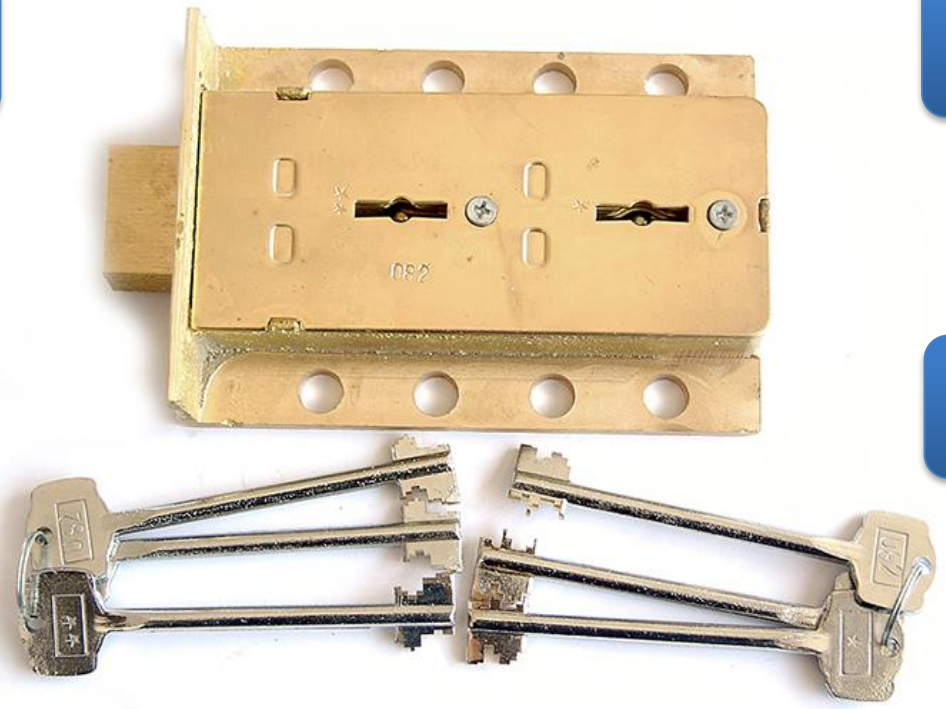
SaAT Security&Assistant Tools

暗号化方式

対称鍵
非対称鍵

アルゴリズム

3DES,AES,..etc
RSA, ECC, ..etc



鍵サイズ

128bit, 256bit,..
1024bit, 2048bit

暗号化モード

ECB, CBC, ..etc

定則

リプレイ攻撃対策、鍵自体の暗号化,..etc

PCI Security Standards Council®
POINT-TO-POINT ENCRYPTION™

NetMove CORPORATION

- To Be Created

実行計画2018年版からの引用

クレジットカード取引における

セキュリティ対策の強化に向けた実行計画

－２０１８－

（２）対面加盟店におけるカード情報の非保持化について

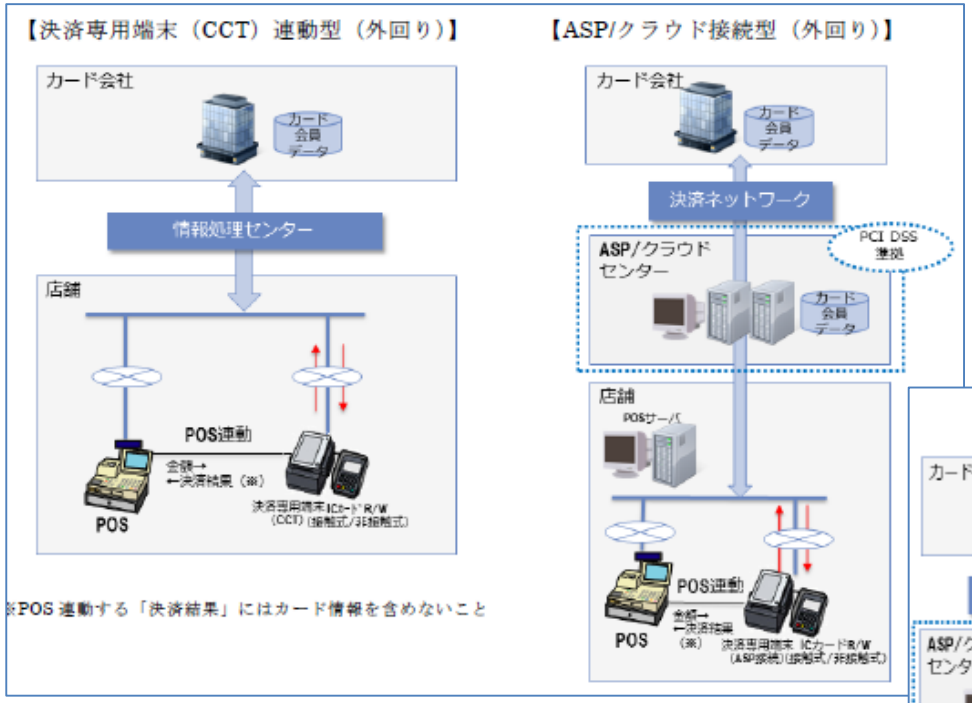
対面加盟店におけるカード情報の非保持化の推進は、特に POS システムを導入している加盟店において課題となる。カード情報を電磁的情報で自社内に「通過」させないよう、POS の機能と決済機能を分離すること、IC 対応した決済専用端末からカード情報を電磁的情報で自社内に取り込まない外回り方式（決済専用端末連動型・ASP/クラウド接続型（外回り方式））を導入することにより、カード情報の非保持化を実現することが可能となる。また、カード番号を特定できない状態とし、自社内で復号できない仕組みとすれば、仮に窃取されてもカード情報として不正に利用することは極めて困難であるため、PCI P2PE 認定ソリューションの導入又は本協議会において取りまとめた技術要件に適合するセキュリティ基準（11 項目）[9]を満たすことにより、非保持と同等/相当のセキュリティ措置を実現することが可能となる（この場合には、PCI DSS 準拠までは求めないこととする。）。

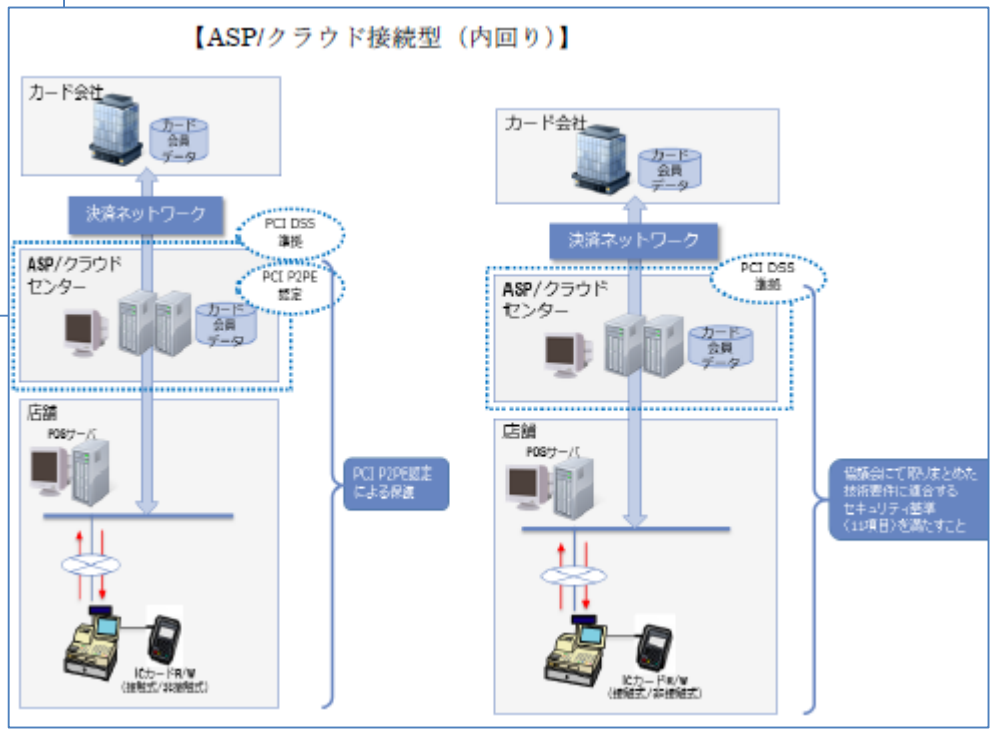
ただし、カード会社や ASP/クラウドセンター等を運営する事業者より、カード情報の還元を受け自社で保有する機器・ネットワークにおいて「保存」、「処理」、「通過」している場合（決済以外の目的の場合も含む）には、カード情報を保持している扱いとなる。

２０１８年３月１日

クレジット取引セキュリティ対策協議会

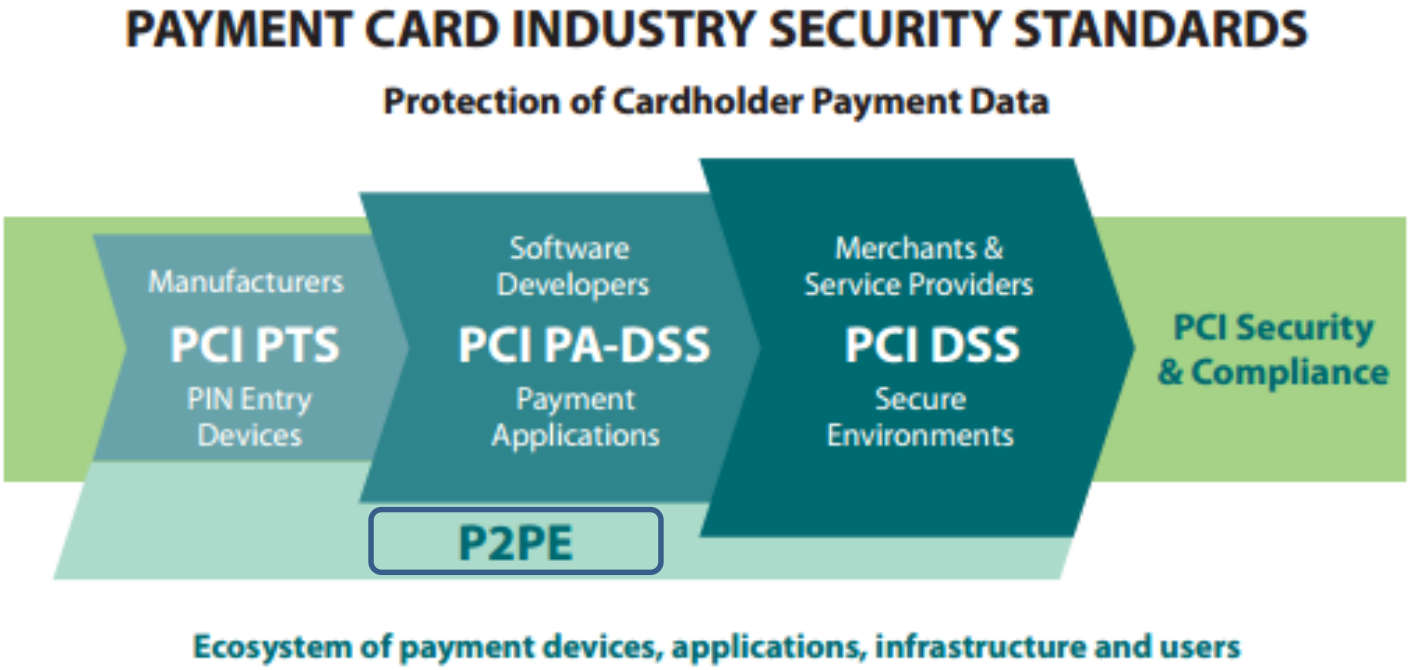
実行計画2018年版からの引用





PCI P2PE Overview（PCI SSC サイト引用）

- Only Council-listed P2PE solutions are recognized as meeting the requirements necessary for **merchants to reduce the scope of their cardholder data environment** through use of a P2PE solution. (PCI P2PE FAQ)



PCI DSS Quick Reference Guide Understanding PCI DSS v3.0

SAQ Validation Type P2PE

v3.2 SAQ Validation Type	Eligibility Criteria*	ASV Scan Required	Penetration Test Required
A Of Questions:22	Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage	No	No
D-MER Of Questions:331	All other SAQ-eligible merchants	Yes	Yes
P2PE Of Questions:33	Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage	No	No

PCIP2PE Solution Provider Service
利用時は自己問診33項目で加盟店は
PCIDSS準拠相当とみなされる

Self-Assessment Questionnaire P2PE（参考）

Payment Card Industry (PCI)
Data Security Standard

Self-Assessment Questionnaire P2PE and Attestation of Compliance

Merchants using Hardware Payment Terminals in a PCI SSC-Listed P2PE Solution Only – No Electronic Cardholder Data Storage

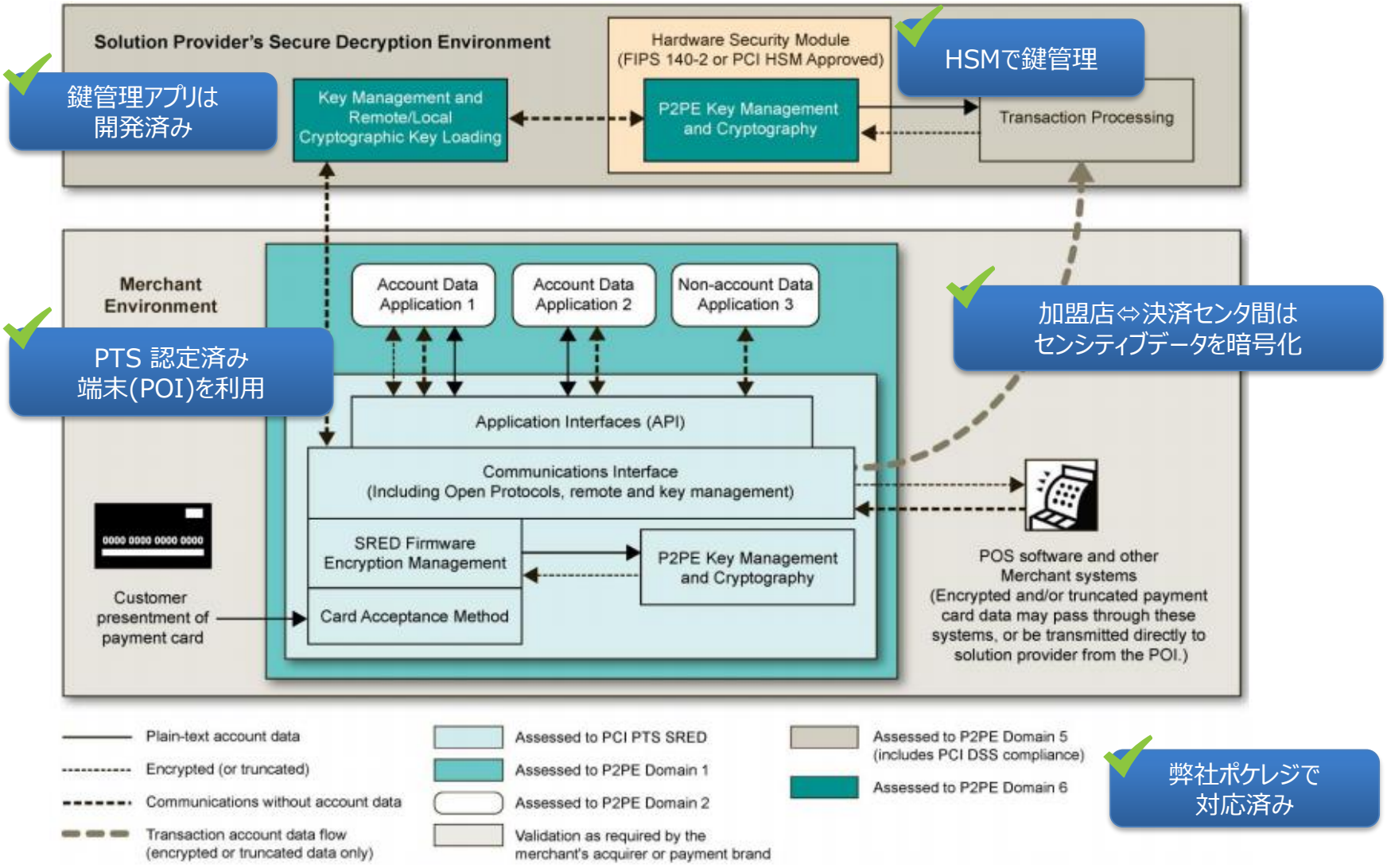
For use with PCI DSS Version 3.2

Revision 1.1

January 2017

続いて、P2PE において構成される コンポネントとソリューション全体の管理 について

PCI P2PE Components



鍵管理アプリは
開発済み

HSMで鍵管理

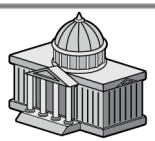
PTS 認定済み
端末(POI)を利用

加盟店⇔決済センタ間は
センシティブデータを暗号化

弊社ポケレジで
対応済み

Example P2PE Implementation at a Glance

PCI P2PE Domains (High Level Summary of Six P2PE Domains)

Domain 1 – Security requirements for the 暗号化端末 アプリ管理	MIURA SYSTEMS  ロジスティクス  NetMove CORPORATION
暗号化アプリ セキュリティ	MIURA SYSTEMS
Domain 3 – For P2PE solution management P2PEソリューション 管理	NetMove CORPORATION
加盟店管理 ソリューション	N/A(Not Applicable)
Domain 5 – Security 復号化環境	 gemalto security to be free macnica networks NetMove CORPORATION
Domain 6 – P2PE Key 鍵管理 運用全般	MIURA SYSTEMS    NetMove CORPORATION

NetMove CORPORATION

PCI P2PE Component Provider

Added new diagram to explain relationships between P2PE solution providers, **P2PE component providers**, and other third parties.(Summary of Change P2PE 1.1 to 2.0)

https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_components

POINT-TO-POINT ENCRYPTION COMPONENTS

This listing is a resource for use by PCI P2PE Solution Providers or for merchants implementing their own Merchant Managed Solution – MMS.

For information regarding the PCI P2PE program, please click here for our document library.

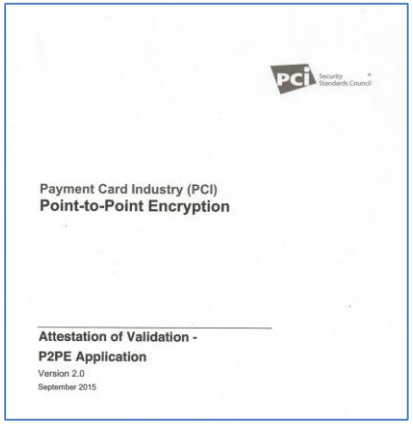
Miura System Ltd			
Component Name: Miura Certificate Authority Reference #: 2016-001071.001	P2PE v2	Foregenix Ltd.	21 Sep 2019
Description Provided by Vendor: The Miura Certificate Authority is the heart of a trust model that enables the secure and remote distribution of encryption keys to Miura MPOS devices. The secure Certificate Authority facility provides state-of-the-art digital signature services that form the foundation of trust between solution providers cryptographic equipment and Miura MPOS POI devices.			
NetMove Corporation			
Component Name: SaAT Managed Terminal Service Reference #: 2017-01147.002 Component Details	P2PE v2	Foregenix Ltd.	31 Oct 2020

PCI P2PE ソリューションプロバイダの責務

- ✓ P2PE 対応可能なコンポーネントの選定
- ✓ 責任、役割分担を明確に規定
- ✓ 運用体制の確立

PCI P2PE 監査提出証跡例

Approval



3rd Party Agreement

Manual

Logs

鍵生成プロセス

- To Be Created

端末デプロイプロセス

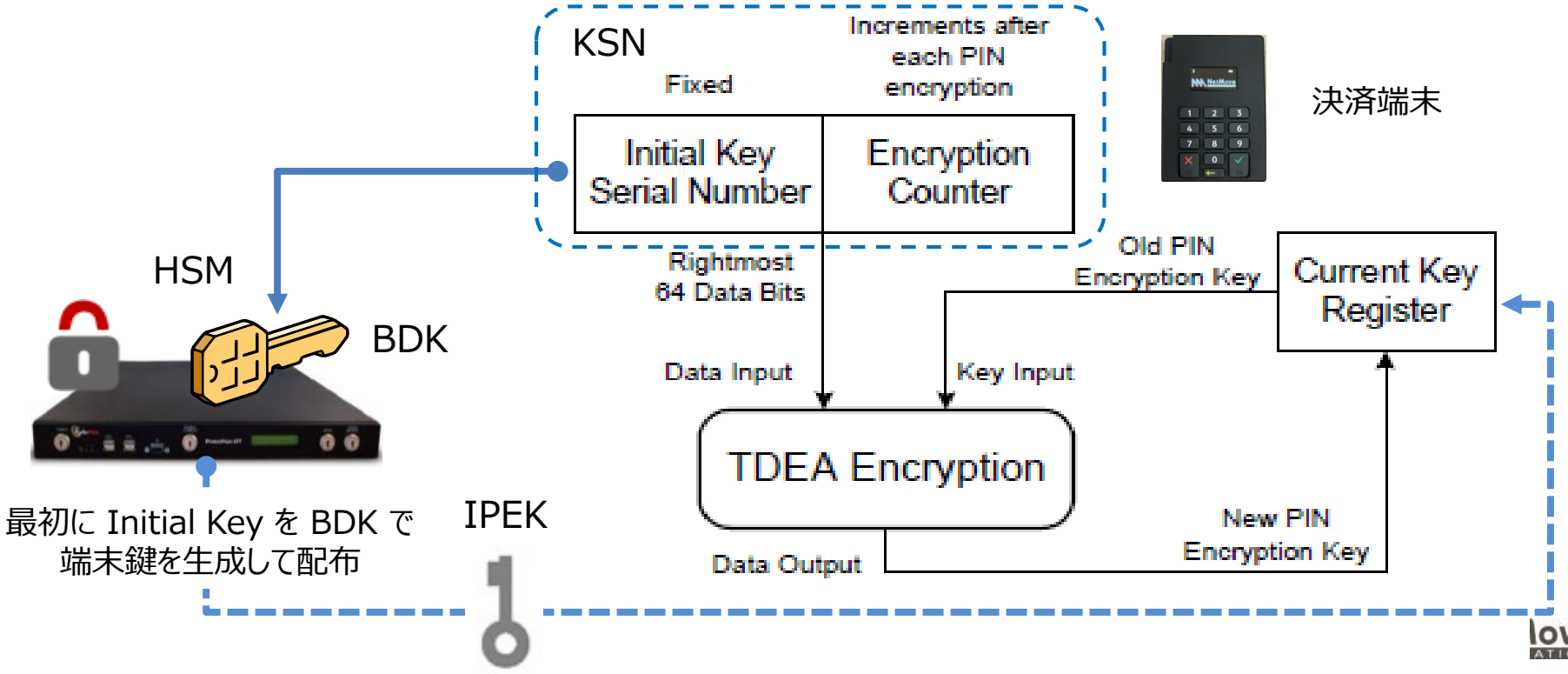
- To Be Created

PCI P2PE
Key Management Technique

What's "DUKPT"? (P2PE Core Key Management)

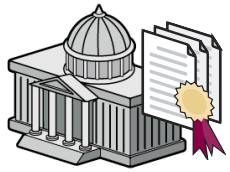
- Derived Unique Key Per Transaction
  - トランザクション毎に異なるユニークな暗号鍵を使うことで暗号鍵の危殆化を防止する仕組み

- BDK（Base Derivation Key）を用いて端末毎に異なる鍵を生成
  - BDK が危殆化した際には決済システムの鍵が判別できてしまう
  - P2PE では BDK は HSM に格納して厳重に管理することが義務付けられている



Remote Key Injection

PCI P2PE Domain6 Annex A1
(Remote Key Distribution using Asymmetric Techniques)



Terminal + CA Cert

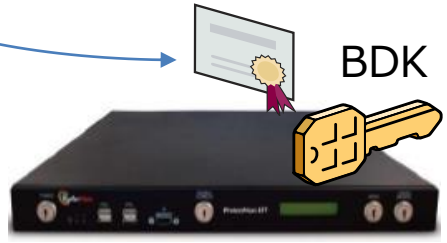
CA

HSM + CA Cert

Suggested IKSN

Terminal Cert

Verify



BDK

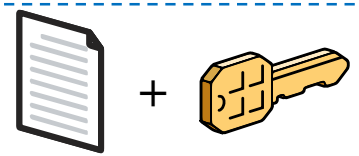
Inject

Decrypt

IPEK

TMK

Generate

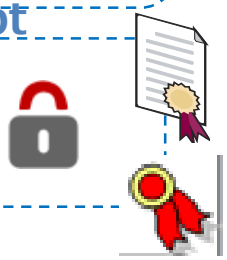


IPEK

TMK

Encrypt

Decrypt



Verify

Encrypt & Sign

NetMove CORPORATION

ご提供サービス形態イメージ(ご参考)

SaAT Security&Assistant Tools

PCI POINT-TO-POINT ENCRYPTION (P2PE)™ SOLUTIONS

This listing is a resource for merchants and acquirers to use in selecting a PCI Point-to-Point Encryption (P2PE) Solution.

For information regarding the PCI P2PE program, please click here for our document library.

Each PCI P2PE Solution has an associated P2PE Implementation Manual which is provided by the Solution Provider and contains details of all P2PE Applications and other software used in the Solution

Click here for the Application Listing and Component Listing.

Find Point-to-Point Encryption Solutions

COMPANY NAME | NetMove Corporation | SUBMIT | CLEAR

Results: 1

COMPANY	P2PE VERSION	P2PE ASSESSORS	REGIONS SERVED	REASSESSMENT DATE
NetMove Corporation				
Solution Name: SaAT PocketRegi				
Reference #: 2017-01147.001 Solution Details	P2PE v2.0	Foregenix Ltd.	Japan	31 Oct 2020

■PCI P2PE Solution Providers List
https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

POINT-TO-POINT ENCRYPTION COMPONENTS

This listing is a resource for use by PCI P2PE Solution Providers or for merchants implementing their own Merchant Managed Solution - MMS.

For information regarding the PCI P2PE program, please click here for our document library.

Click here for the Solutions Listing and Application Listing.

Find PCI P2PE Component Providers

COMPANY NAME | NetMove Corporation | SUBMIT | CLEAR

Page: 1

Certification/Registration Authorities | Decryption Management Services | Encryption Management Services | Key Injection Facilities

Results: 1

COMPANY	P2PE VERSION	P2PE ASSESSOR	REASSESSMENT DATE
NetMove Corporation			
Component Name: SaAT Managed Terminal Service Reference #: 2017-01147.002 Component Details	P2PE v2	Foregenix Ltd.	31 Oct 2020

■PCI P2PE Component Providers List
https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_components

NetMove CORPORATION

P2PE モジュラアプローチ 本日のまとめ

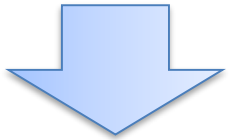
SaT Security&Assistant Tools

✓ 対面決済を Point To Point で暗号化

✓ モジュラ型アプローチによる管理の効率化

✓単に暗号化すれば良いというわけではない

- 適正な暗号鍵のキーマネジメント
- ソリューションとしての厳密な管理体制



✓セキュリティを担保しつつ、加盟店の負荷・責務は軽減

NetMove CORPORATION