Security Standards in Payment Systems

Edgar González Fernández
Dr. Guillermo Morales Luna
Dr. Feliú Sagols Troncoso

Department of Computer Science
CINVESTAV-IPN

August 9, 2017

1. Payment Card Industry
   - Involved parties and payment lifecycle
   - Standards
2. Approved Cryptographic Primitives
3. Secure cryptographic devices
   - Security levels
   - Device management and lifecycle
   - Key Management and lifecycle
   - Controls and audit
4. Public Key Infrastructure
   - Certificate management
   - Key management
5. Smart cards
   - Chip card and POS communication
6. Mexican regulations

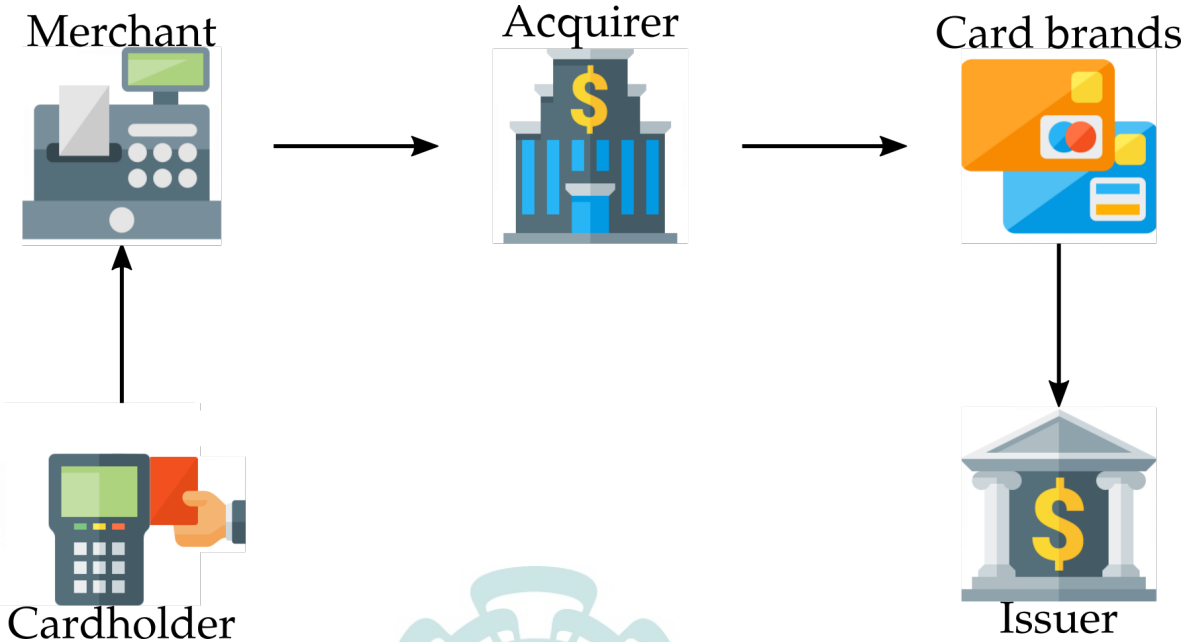
Cardholder: Holds cards, pays receipts, keep PIN secret

Merchant: Accepts processes, transmits and possibly stores sensitive user data

Issuer: Responsible of card physical security, check available funds, bills the user

Acquirer: Authorizes payment, regulates fees, settles transactions with issuer

Card brands: Maintain connection between acquirer and issuer



Cardholder: Holds cards, pays receipts, keep PIN secret

Merchant: Accepts processes, transmits and possibly stores sensitive user data

Issuer: Responsible of card physical security, check available funds, bills the user

Acquirer: Authorizes payment, regulates fees, settles transactions with issuer

Card brands: Maintain connection between acquirer and issuer

Processor: Routes transactions to acquirer, may provide reporting and security services

Gateway: Sends transaction to processor or acquirer, may offer additional reporting and security services

Software vendors

Hardware manufacturers

Cardholder: Holds cards, pays receipts, keep PIN secret

Merchant: Accepts processes, transmits and possibly stores sensitive user data

Issuer: Responsible of card physical security, check available funds, bills the user

Acquirer: Authorizes payment, regulates fees, settles transactions with issuer

Card brands: Maintain connection between acquirer and issuer

Processor: Routes transactions to acquirer, may provide reporting and security services

Gateway: Sends transaction to processor or acquirer, may offer additional reporting and security services

Software vendors

Hardware manufacturers

Cardholder: Holds cards, pays receipts, keep PIN secret

Merchant: Accepts processes, transmits and possibly stores sensitive user data

Issuer: Responsible of card physical security, check available funds, bills the user

Acquirer: Authorizes payment, regulates fees, settles transactions with issuer

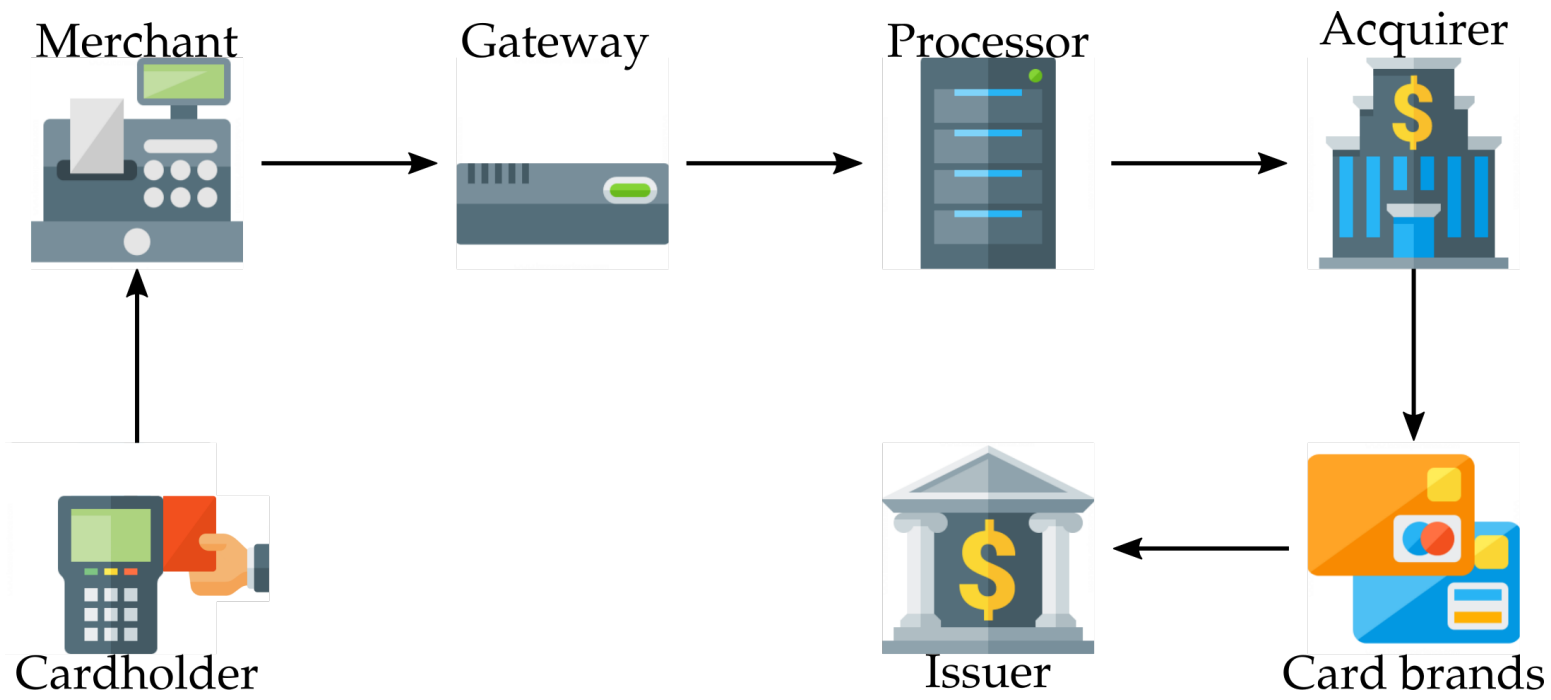
Card brands: Maintain connection between acquirer and issuer

Processor: Routes transactions to acquirer, may provide reporting and security services

Gateway: Sends transaction to processor or acquirer, may offer additional reporting and security services

Software vendors

Hardware manufacturers


Merchant
Gateway
Processor
Acquirer
Cardholder
Issuer
Card brands

- Card present transaction: ATMs withdrawal, point of sale. Cryptographic secure devices, ICC technology

- Card not present transaction: Online, phone, wallets. Secured with SSL/TLS

Weak points

- Application memory scraping using malware
- Retrieve sensitive information locally stored
- Use of network sniffers over unsecure or poorly secure communication
- Tamper application software configuration or updates
- Tamper or substitute hardware
- Disassemble application code
- Force offline authentication or downgrade security

Security measures:

- Do not store sensitive authentication data after authorization (even if encrypted)
- Secure sensitive data at any stage: in memory, at rest, in transit
- Use strong cryptographic algorithms and functions
- Verify applications and cryptographic material authenticity and integrity
- Avoid hard-coding sensitive or cryptographic information (when possible)

- **ISO, ISO/IEC**. International, application-independent. Financial services
- **ANSI/ASC X9**. Financial services industry
- **NIST**. SP, FIPS PUBS. US federal government departments
- **IESG, IETF**. Internet standards and requests for comments (RFCs)
- **PKCS**. RSA Inc. Industry standards
- **EMVCo**. EMV standard for credit card and reader devices communication
- **PCI council**. PCI-DSS for credit card based transactions

- **Random number generators**: ISO 18031, SP800-90A-C
- **Hash functions**: ISO 10118-1,2, X9.31, FIPS 180
- **Block ciphers**: SP800 67, X9.52 (TDES), FIPS 197 (AES), ISO 18033-3.
- **Modes of Operation**: ISO 10116, SP800 38A
- **Message Authentication Codes**: ISO 9797, X9.52, FIPS 198, SP800 38B-D.
- **Asymmetric ciphers**: ISO 18033-3, PKCS1.
- **Digital signatures**: ISO 9796, X9.30,31,62, FIPS 186.

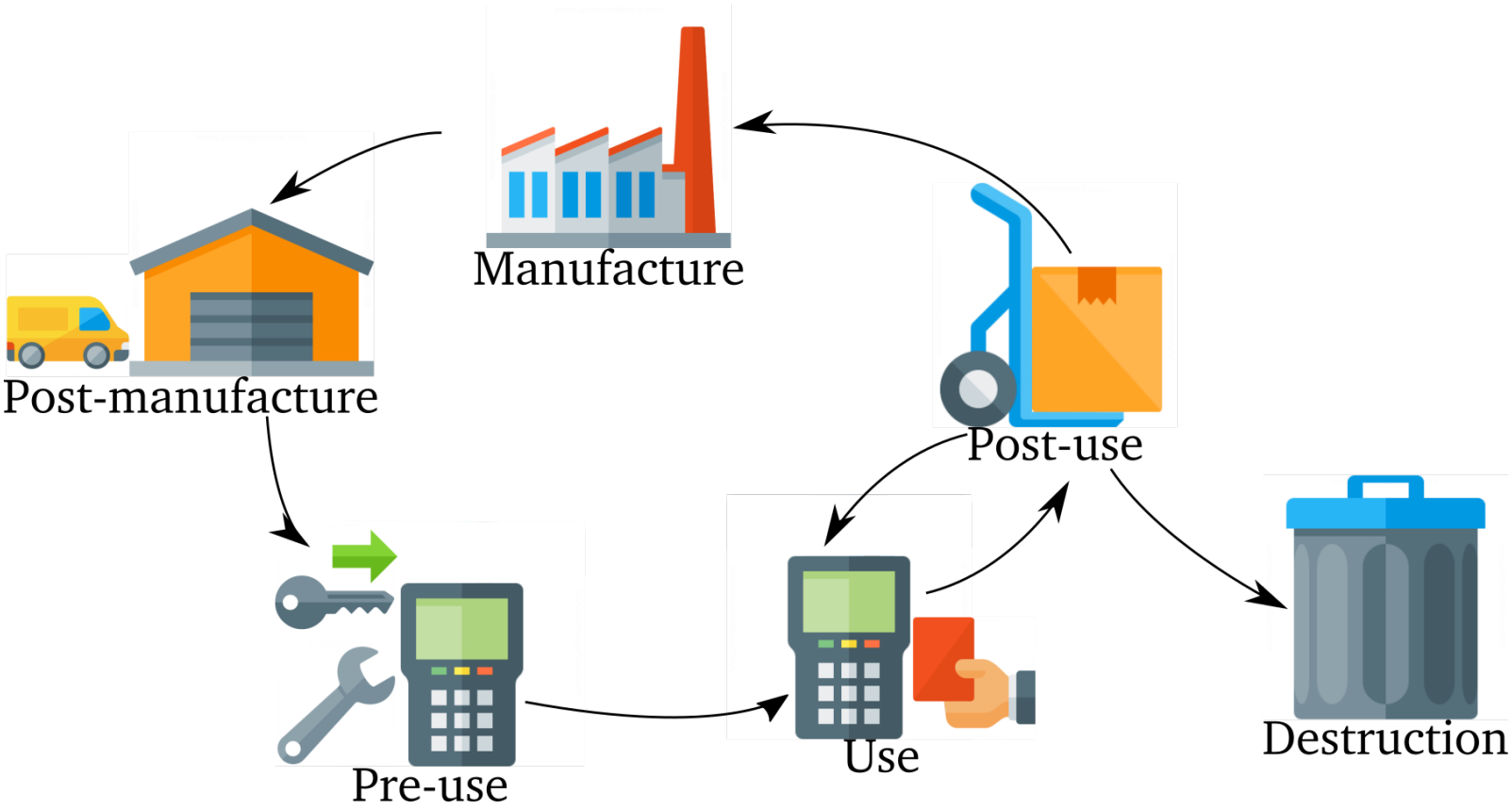
Secure cryptographic devices: ISO 13491, FIPS 140.

- Integrated chip circuits: Cardholder data
- Card readers: magnetic stripes, chip, contactless
- Electronic cashiers: transmission of data over card network
- Servers: Receive data, return responses
- One time password devices: Two factor authentication
- Key loader devices: Injects cryptographic keys or material into secure devices
- Hardware Secure Modules (HSM): Generate, store and derive keys. May implement cryptographic primitives and financial facilities

Hardware Security Module
Source: `wikipedia.org/wiki/Hardware_security_module`

One Time Passwords
Source: `wikipedia.org/wiki/Multi-factor_authentication`

1. At least 1 approved algorithm or security function. No physical-network security required. Software can be run on a general purpose computer system on unevaluated operating systems.
2. Tamper evidence or pick-resistant locks. Role-based authentication. Run on a general purpose computing system with access controls and audit mechanisms.
3. Tamper detect and response. Plaintext data destruction. Identity-based authentication. Input-output through physically separated ports or logically separated interfaces.
4. Two-factor authentication, protection against environmental conditions. Resistance to timing and diferential power analysis attacks and against fluctuation in the production environment.



Manufacture and post-manufacture: Beware of tamper proof and hardware substitution

Pre-use: Avoid use of compromised keys

Use: Prevent substitution or modification of keys or applications

Post-use: Key and application erasure or compromise detection

Key management: ISO 11568, SP800 57
A single key should be used for a single purpose and must have a limited lifetime (cryptoperiod).
Data types:

- Secret: PIN, passwords, keys, PAN, CVV, Expiration Date
- Key material: Passwords, seeds, IVs, components, shared secrets
- Authentication: Certificates, MACs, nonces

Key types:

- Key, PIN, Data encipherment keys.
- MAC Keys.
- Key derivation, generating keys.
- Master keys (Issuer, terminal).

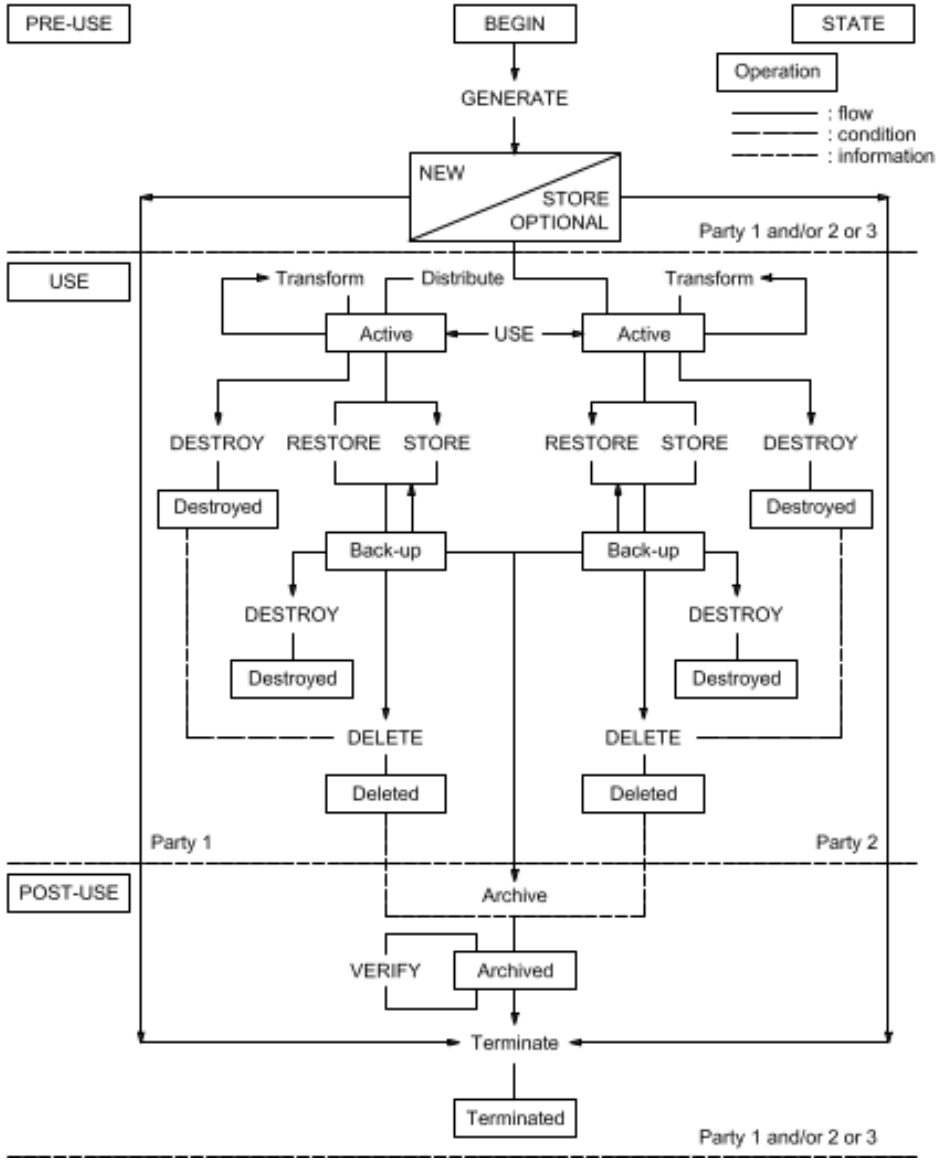
Techniques for key management services

- Encryption or key wrapping: $E_{KEK}(K)$
- Variants: $K_i = K \oplus C_i$ (key of type i).
- Derivation: $K_D = F(K, Id)$
- Transformation: Original key must be destroyed
- Offsetting: $K_O = F(K, ctr)$
- Tagging: $E_{KEK}(K \oplus T_i)$
- Verification: $KVC = E_K(\overline{0})[0 : k]$ (Key Check Value)
- Integrity: Hash functions.

Generation: repeatable (PRNG) or non-repeatable (derivation, transformation) processes
Storage:

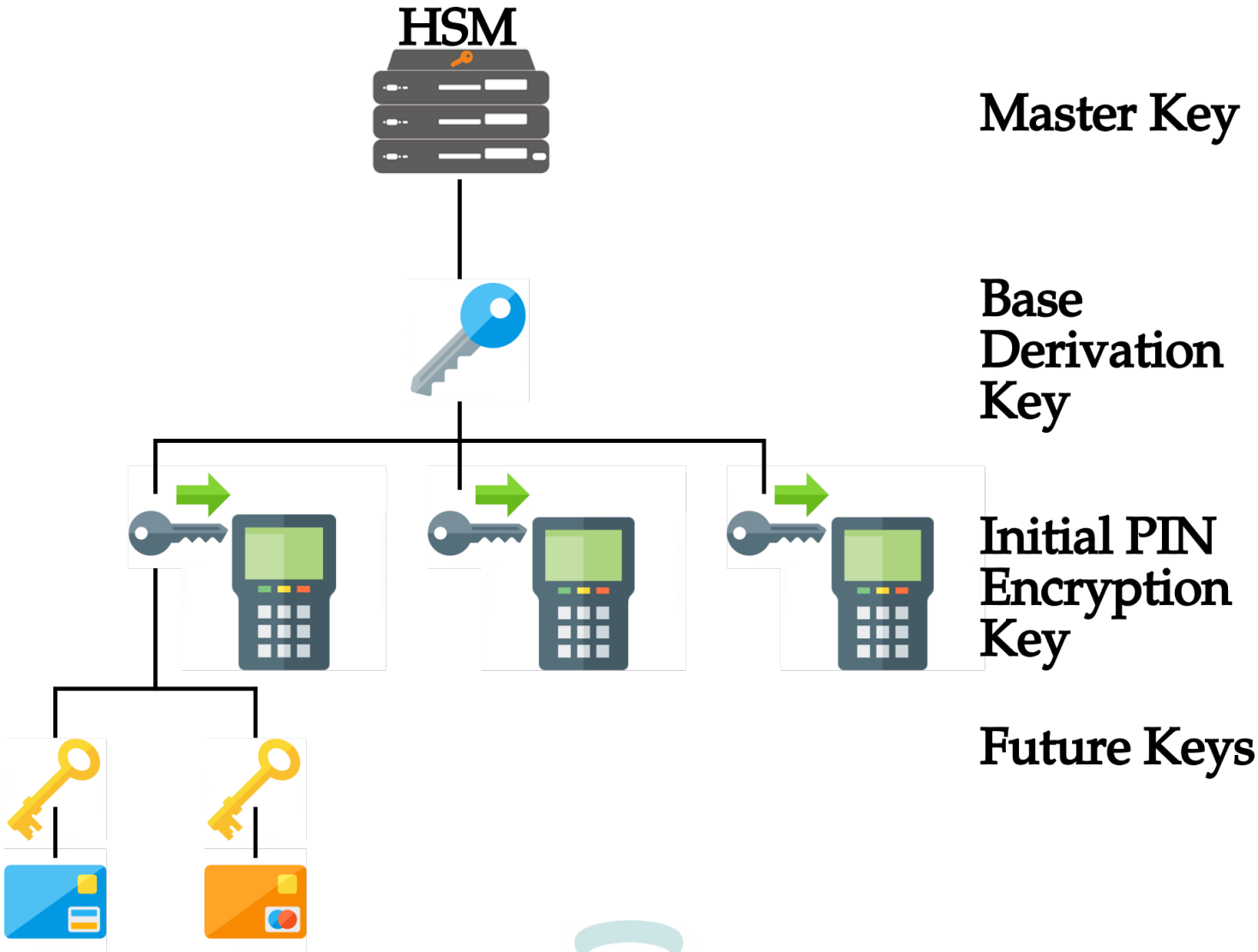
- Plaintext (tamper proof dev)
- Key components
- Encrypted

Distribution: manual, electronic injection, network download
Replacement: Repeat generation process or apply transformation
Destruction: ISO 9564-1
Archive: plain, encrypted, components



Symmetric key life cycle
Source: ISO 11568-2:2005

Key hierarchy. Confidentiality of certain keys is dependent upon the confidentiality of keys in upper levels



Key hierarchy for DUKPT (X9.24)

Controls and audit:

- Detect the disclosure of a key
- Detect the substitution of a disclosed key for a legitimate key

Key disclosure can be detected by:

- Audits and controls imposed on those individuals who manage keys and/or cryptographic devices
- Periodic inspection of and control over interfaces through which unenciphered keys or key components are transferred
- Control and auditing of cryptographic devices that contain keys, to detect any lost or stolen devices.

Public Key Infrastructure ISO 21188, SP800-32, RFC 5758 Core functional components:

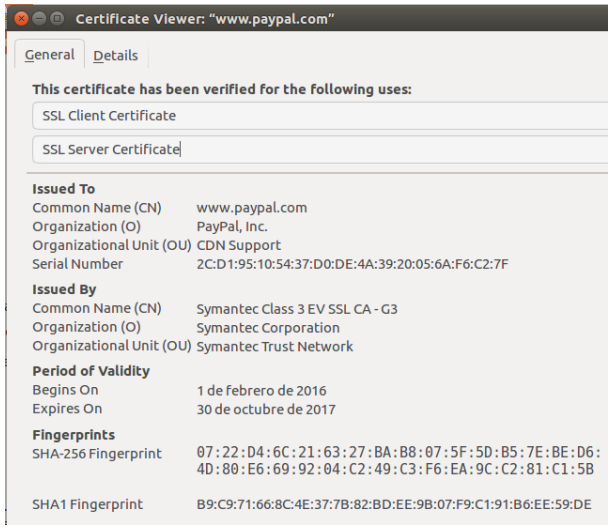
- Certification Authorities
- Registration Authorities
- Repository for keys, certificates and Certificate Revocation Lists (CRLs)
- Management function

Functions:

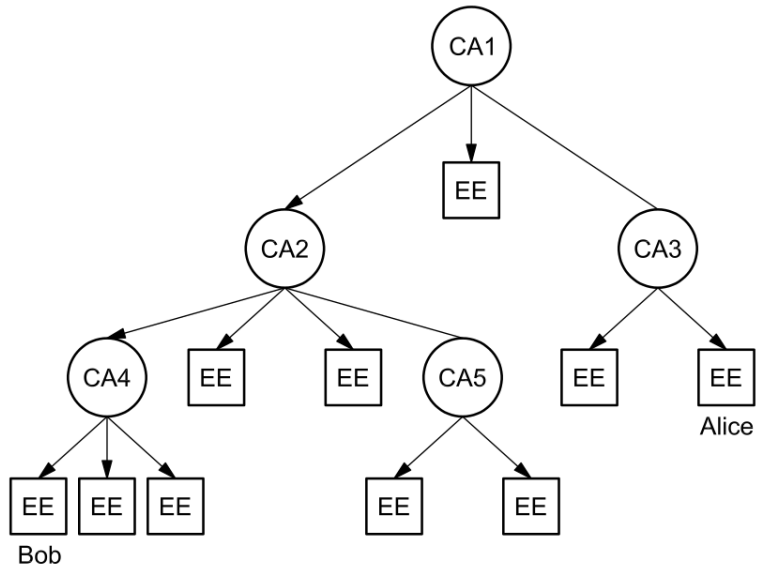
- User registration
- Issuing, validating and revoking certificates
- Creating and publishing CRLs
- Storing and retrieving certificates and CRLs
- Key lifecycle management

Data structures: ISO 15782-x, ISO/DIS 21188, ANSI X9.55, X9.57, ITU-T X.509

- X.509 Public Key Certificates
- Certificate Revocation Lists (CRLs)
- Attribute Certificates
- Certificate extensions

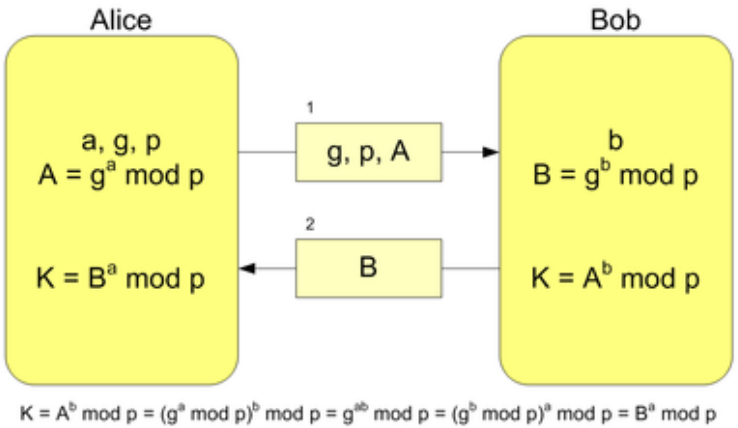


Paypal certificate

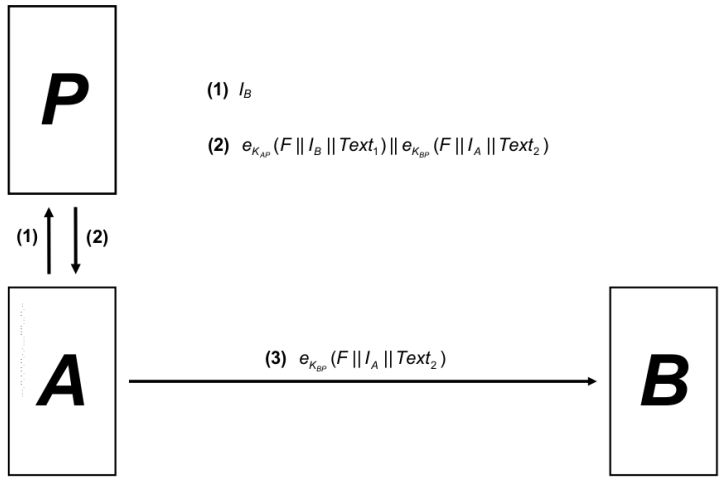


Hierarchy of certification authorities
Source:ISO 15782-1:2009

- Key establishment with symmetric techniques: point to point, key distribution centre, key translation centre
- Key establishment with asymmetric techniques: key agreement, key transport



Diffie-Hellman Key Exchange
Source: `wikipedia.org/wiki/Diffie-Hellman_key_exchange`



KDC Key Exchange
Source: `ISO/IEC11770-2:2008`

Smart cards: ISO 7816-x. EMV books

- Physical characteristics
- Communication protocols and commands for interoperability
- File system
- Offline and online authentication
- PIN encipherment for online and offline authentication
- Certificate hierarchy: CA, issuer, chip

According to EMV, different options are available for authentication

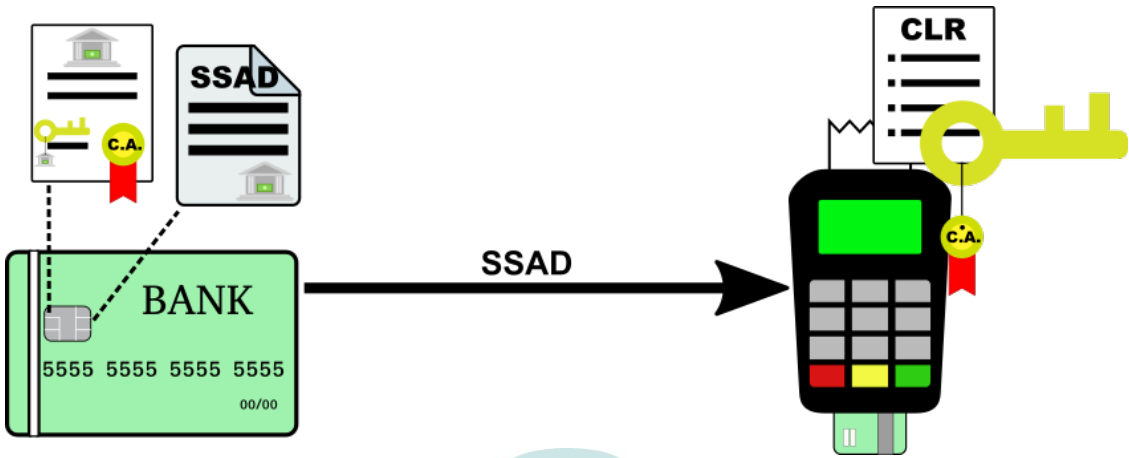
Static Data Authentication

Card provides to Terminal

- Issuer PK Certificate (signed by CA)
- Signed Static Application Data (SSAD) (signed and provided by the Issuer)

Terminal performs:

- Verification of Issuers certificate (additionally check against CRL)
- Verification of SSAD signature



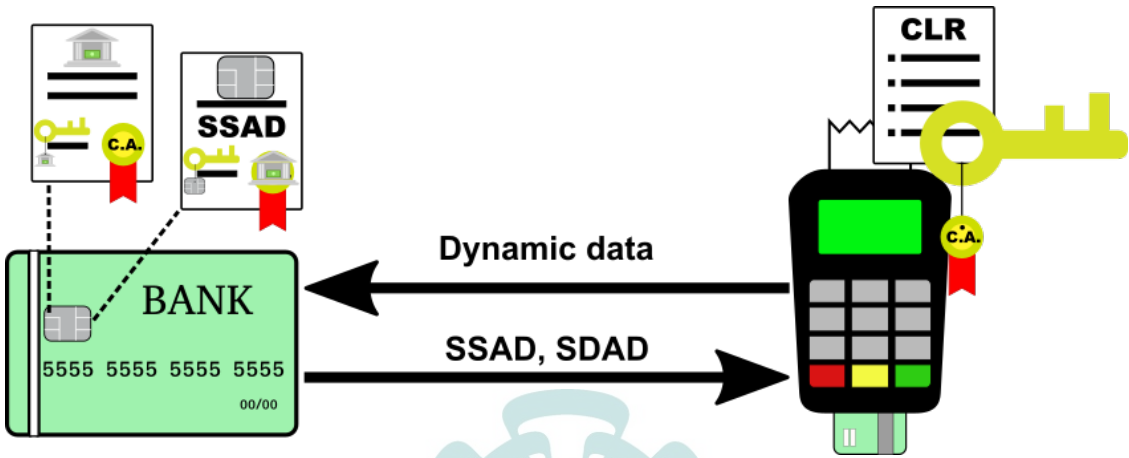
Offline Dynamic Data Authentication

Card provides to Terminal:

- Issuer PK Certificate
- ICC PK Certificate and SSAD (signed and provided by the Issuer)
- ICC Dynamic Application Data (SDAD) (signed and generated by the ICC)

Terminal performs:

- Verification of Issuers certificate (additionally check against CRL)
- Verification of ICC Certificate and SSAD signature
- Verification of ICC Dynamic Data signature



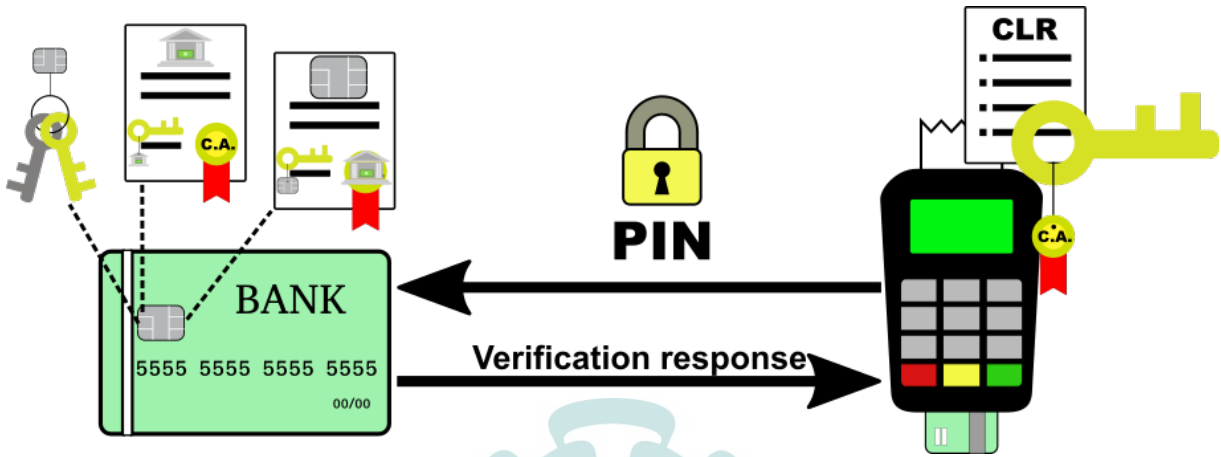
PIN encipherment and verification

Card provides to Terminal:

- Issuer PK Certificate (signed by CA)
- ICC PIN Key Certificate and Static Application Data (SSAD) (signed and provided by the Issuer)

Terminal performs:

- Verification that Issuers certificate was signed by the CA (additionally check against CRL)
- Verifies that the Cards SSAD was signed by the issuer
- Enciphers PIN with ICC Public Key



Comisión Nacional Bancaria y de Valores:
Capítulo X

- Multiple factor authentication for e-banking
- User and institution authentication
- Access management
- Use of ICC cards
- Security in data storage and transmission

Banco de México: Infraestructura Extendida de Seguridad (IES)

- Digital signatures
- Public keys and digital certificates structure

Norma Oficial Mexicana: PROY-NOM-151-SCFI-2015 for messages and digital documents

- ASN.1 format for messages
- Digital signatures

Thank you!

egonzalez@computacion.cs.cinvestav.mx