EMV: Integrated Circuit Card Specifications for Payment Systems

Jan Krhovják

Faculty of Informatics, Masaryk University

Outline

- Introduction to EMV
- Offline data authentication
  - Static data authentication
  - Dynamic data authentication
- User authentication
  - Signature based
  - PIN based
- Automatic risk management
  - Terminal risk management
  - Terminal action analysis
  - Card action analysis
- Conclusion

Introduction to EMV

- EMV 4.1 specifications consist of four books (786 pages)
  - Application Independent ICC to Terminal Interface Requirements
  - Security and Key Management
  - Application Specification
  - Cardholder, Attendant, and Acquirer Interface Requirements
- Basic terminology
  - Merchant, payee
  - Cardholder, customer, payer, or simply user
  - Card issuer, cardholder's bank, or simply bank
    - ⋆ No distinguishing (for this presentation) between issuer or acquirer bank
  - Fraud, a deception made for a personal gain
    - ⋆ All parties should be protected against the fraud
    - ⋆ Unauthorized and illegal use of a credit card to purchase property
  - ICC, an acronym for integrated circuit(s) card

Introduction to EMV

- EMV 4.1 specifications consist of four books (786 pages)
  - Application Independent ICC to Terminal Interface Requirements
  - Security and Key Management
  - Application Specification
  - Cardholder, Attendant, and Acquirer Interface Requirements
- Basic terminology
  - Merchant, payee
  - Cardholder, customer, payer, or simply user
  - Card issuer, cardholder's bank, or simply bank
    - ★ No distinguishing (for this presentation) between issuer or acquirer bank
  - Fraud, a deception made for a personal gain
    - ★ All parties should be protected against the fraud
    - ★ Unauthorized and illegal use of a credit card to purchase property
  - ICC, an acronym for integrated circuit(s) card

Basic Principles of Offline Data Authentication

- The goal is offline detection of fake (altered/duplicated) cards
  - Based on asymmetric cryptography (namely on RSA)
    - ★ RSA public key must be always 3 or $2^{16} - 1$
  - Existence of a certification authority (CA) is required
    - ★ Integrity of transmitted public keys must be secured
  - Each EMV terminal must contain actual CA public key
- Supported mechanisms
  - Static data authentication (SDA)
  - Dynamic data authentication (DDA)
  - Combined DDA and application cryptogram generation (CDA)

Basic Principles of Offline Data Authentication

- The goal is offline detection of fake (altered/duplicated) cards
  - Based on asymmetric cryptography (namely on RSA)
    - ★ RSA public key must be always 3 or $2^{16} - 1$
  - Existence of a certification authority (CA) is required
    - ★ Integrity of transmitted public keys must be secured
  - Each EMV terminal must contain actual CA public key
- Supported mechanisms
  - Static data authentication (SDA)
  - Dynamic data authentication (DDA)
  - Combined DDA and application cryptogram generation (CDA)

SDA: Static Data Authentication I

- Basics of SDA
  - Performed by terminal
  - Confirms legitimacy of critical ICC-resident static data
  - Detects unauthorized alteration of data after personalization
- Settings and process of SDA
  - Public key of CA is stored in each terminal
  - Public key of issuer bank is certified by CA and stored on ICC
  - Static application data are signed by issuer bank and stored on ICC
- Security of SDA
  - Based on secrecy of private RSA keys
  - Counterfeiting/duplication not solved

SDA: Static Data Authentication I

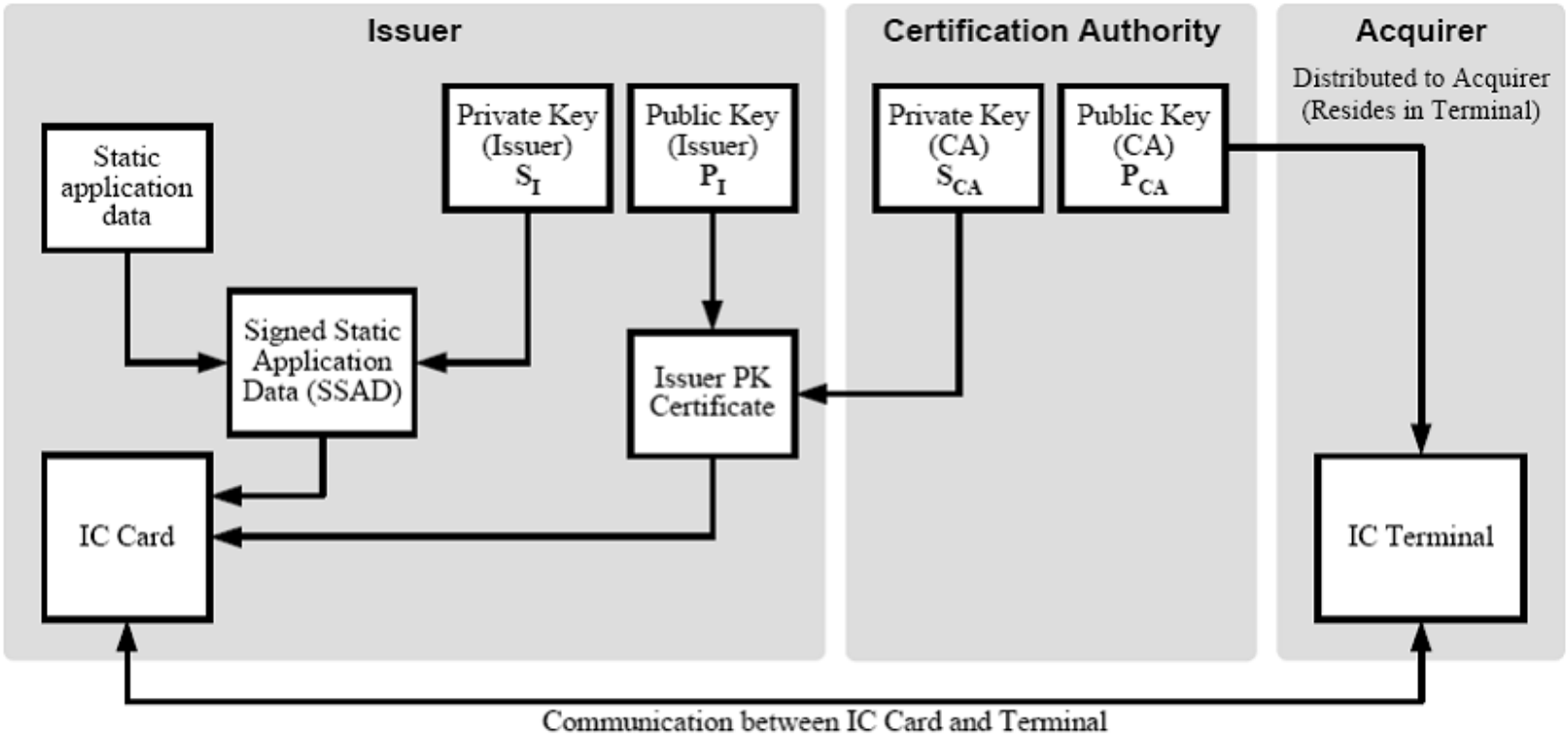
- Basics of SDA
  - Performed by terminal
  - Confirms legitimacy of critical ICC-resident static data
  - Detects unauthorized alteration of data after personalization
- Settings and process of SDA
  - Public key of CA is stored in each terminal
  - Public key of issuer bank is certified by CA and stored on ICC
  - Static application data are signed by issuer bank and stored on ICC
- Security of SDA
  - Based on secrecy of private RSA keys
  - Counterfeiting/duplication not solved

SDA: Static Data Authentication I

- Basics of SDA
  - Performed by terminal
  - Confirms legitimacy of critical ICC-resident static data
  - Detects unauthorized alteration of data after personalization
- Settings and process of SDA
  - Public key of CA is stored in each terminal
  - Public key of issuer bank is certified by CA and stored on ICC
  - Static application data are signed by issuer bank and stored on ICC
- Security of SDA
  - Based on secrecy of private RSA keys
  - Counterfeiting/duplication not solved

SDA: Static Data Authentication II

- Diagram of SDA (taken from the original specification)



Card provides to Terminal:

- Issuer PK Certificate (P_I certified by the CA)
- Signed Static Application Data (SSAD) (signed by the Issuer)

Terminal:

- Uses P_{CA} to verify that the Issuer's P_I was certified by the CA
- Uses P_I to verify that the Card's SSAD was signed by the Issuer

DDA: Dynamic Data Authentication I

- Basics of DDA
  - Performed by terminal&card (ICC with coprocessor required)
  - Confirms legitimacy of critical ICC-resident/generated data and data received from terminal
  - Detects counterfeited/duplicated cards
- Settings and process of DDA
  - Similar as for SDA
  - New unique ICC RSA key pair is stored on each card
    - ICC private key is securely stored (can not leave the card)
    - ICC public key is signed & stored together with static application data
  - Terminal sends random challenge to be signed by ICC private key
- Security of DDA
  - Based on secrecy of private RSA keys
  - The chip card must be able to protect ICC private key

DDA: Dynamic Data Authentication I

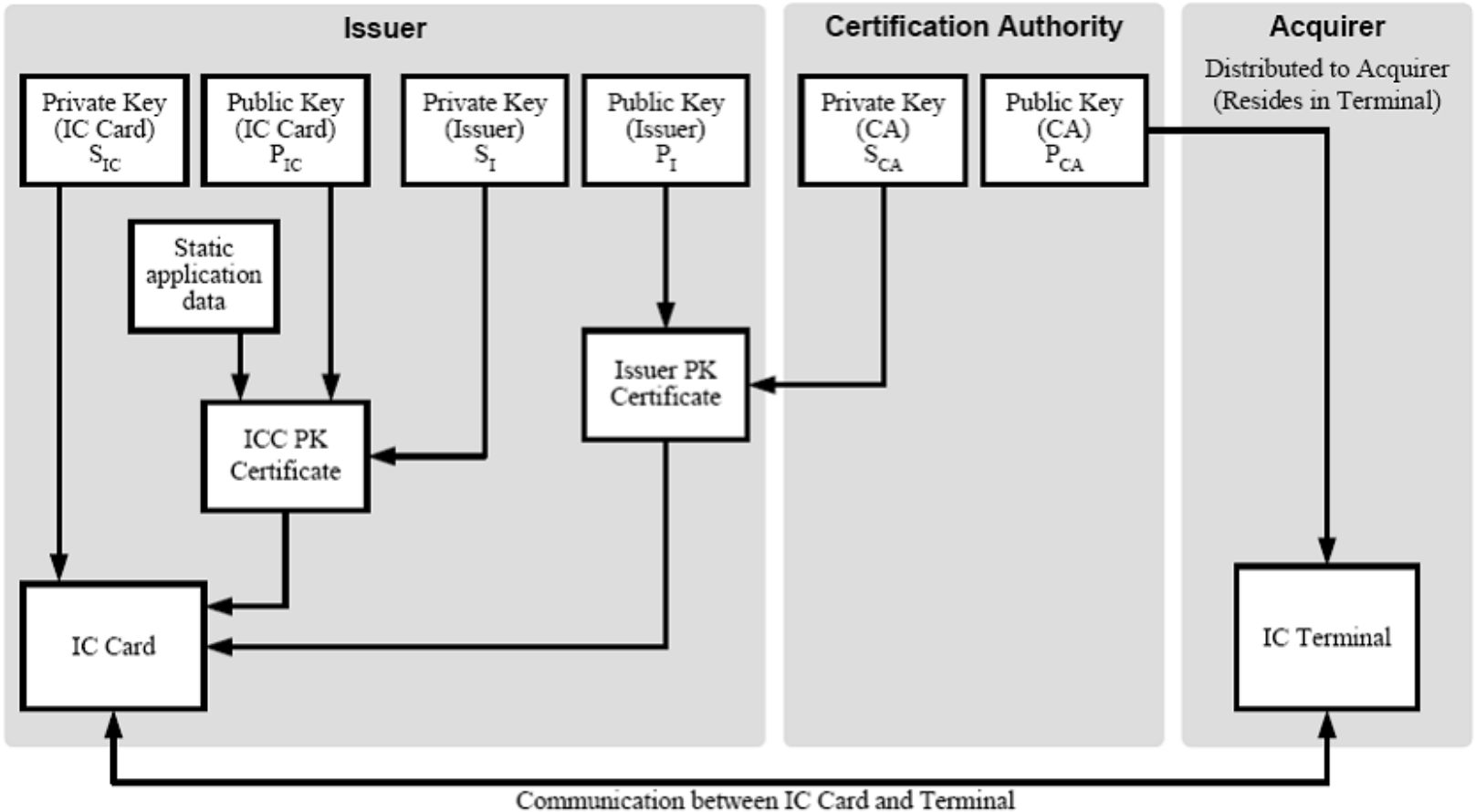
- Basics of DDA
  - Performed by terminal&card (ICC with coprocessor required)
  - Confirms legitimacy of critical ICC-resident/generated data and data received from terminal
  - Detects counterfeited/duplicated cards
- Settings and process of DDA
  - Similar as for SDA
  - New unique ICC RSA key pair is stored on each card
    - ICC private key is securely stored (can not leave the card)
    - ICC public key is signed & stored together with static application data
  - Terminal sends random challenge to be signed by ICC private key
- Security of DDA
  - Based on secrecy of private RSA keys
  - The chip card must be able to protect ICC private key

DDA: Dynamic Data Authentication I

- Basics of DDA
  - Performed by terminal&card (ICC with coprocessor required)
  - Confirms legitimacy of critical ICC-resident/generated data and data received from terminal
  - Detects counterfeited/duplicated cards
- Settings and process of DDA
  - Similar as for SDA
  - New unique ICC RSA key pair is stored on each card
    - ICC private key is securely stored (can not leave the card)
    - ICC public key is signed & stored together with static application data
  - Terminal sends random challenge to be signed by ICC private key
- Security of DDA
  - Based on secrecy of private RSA keys
  - The chip card must be able to protect ICC private key

DDA: Dynamic Data Authentication II

- Diagram of DDA (taken from the original specification)



Card provides to Terminal:

- Issuer PK Certificate (P_I certified by the CA)
- ICC PK Certificate (P_{IC} and static application data signed by the Issuer)
- Card and terminal dynamic data signed by the Card

Terminal:

- Uses P_{CA} to verify that the Issuer's P_I was certified by the CA
- Uses P_I to verify that the Card's P_{IC} and static application data were certified by the Issuer
- Uses P_{IC} to verify that the dynamic data was signed by the Card

CDA: Combined DDA and Application Cryptogram (AC) Generation

- Basics of CDA
  - Performed by terminal&card in parallel with card action analysis
- Settings and process of CDA
  - Similar as for DDA
  - Random challenge is a part of request for AC
  - Signed AC contains this random challenge
- Security of CDA
  - Extra security for AC
  - Advantage if secure communication between terminal and ICC can not be guaranteed

CDA: Combined DDA and Application Cryptogram (AC) Generation

- Basics of CDA
  - Performed by terminal&card in parallel with card action analysis
- Settings and process of CDA
  - Similar as for DDA
  - Random challenge is a part of request for AC
  - Signed AC contains this random challenge
- Security of CDA
  - Extra security for AC
  - Advantage if secure communication between terminal and ICC can not be guaranteed

CDA: Combined DDA and Application Cryptogram (AC) Generation

- Basics of CDA
  - Performed by terminal&card in parallel with card action analysis
- Settings and process of CDA
  - Similar as for DDA
  - Random challenge is a part of request for AC
  - Signed AC contains this random challenge
- Security of CDA
  - Extra security for AC
  - Advantage if secure communication between terminal and ICC can not be guaranteed

Negotiation of authentication method

- Supported methods
  - Signature-based (handwritten)
  - PIN-based (offline/online, plaintext/encrypted)
  - Several combinations
- Priority list of card-supported methods stored on ICC
  - Terminal selects the first terminal-supported method from this list
    - Selected method is dependent on the terminal type
    - One supported method can be "no cardholder verification required"
  - Successful verification
    - At least one metod is successfully performed
    - The list is exhausted

Negotiation of authentication method

- Supported methods
  - Signature-based (handwritten)
  - PIN-based (offline/online, plaintext/encrypted)
  - Several combinations
- Priority list of card-supported methods stored on ICC
  - Terminal selects the first terminal-supported method from this list
    - ★ Selected method is dependent on the terminal type
    - ★ One supported method can be "no cardholder verification required"
  - Successful verification
    - ★ At least one metod is successfully performed
    - ★ The list is exhausted

Verification processing

- Signature-based or online PIN-based authentication
  - Same process as used in the case of magnetic strip cards
    - ★ PIN is formatted into PIN-block, encrypted by using 3DES, ...
  - Chip card should provide extra security against skimming
- Offline encrypted PIN-based authentication
  - New own RSA key pair is associated with PIN encipherment
  - This key pair is stored/certified as the key for DDA
  - Original PIN necessary for verification is securely stored on ICC
  - PINpad/terminal must be physically/logically well secured

Verification processing

- Signature-based or online PIN-based authentication
  - Same process as used in the case of magnetic strip cards
    - ★ PIN is formatted into PIN-block, encrypted by using 3DES, ...
  - Chip card should provide extra security against skimming
- Offline encrypted PIN-based authentication
  - New own RSA key pair is associated with PIN encipherment
  - This key pair is stored/certified as the key for DDA
  - Original PIN necessary for verification is securely stored on ICC
  - PINpad/terminal must be physically/logically well secured

Automatic Risk Management

- Protects against offline undetectable threats
  - Decides if transaction should be:
    approved offline, declined offline, or transmitted online
- Terminal risk management
  - Floor limit checking
  - Random transaction selection
  - Velocity checking
- Terminal&card action analysis
  - T: reject transaction offline $\Rightarrow$
    C: reject offline
  - T: transaction should go online $\Rightarrow$
    C: go online $\vee$ reject offline
  - T: transaction might be completed offline $\Rightarrow$
    C: go online $\vee$ reject offline $\vee$ approve offline

Automatic Risk Management

- Protects against offline undetectable threats
  - Decides if transaction should be:
    approved offline, declined offline, or transmitted online
- Terminal risk management
  - Floor limit checking
  - Random transaction selection
  - Velocity checking
- Terminal&card action analysis
  - T: reject transaction offline $\Rightarrow$
    C: reject offline
  - T: transaction should go online $\Rightarrow$
    C: go online $\vee$ reject offline
  - T: transaction might be completed offline $\Rightarrow$
    C: go online $\vee$ reject offline $\vee$ approve offline

Automatic Risk Management

- Protects against offline undetectable threats
  - Decides if transaction should be:
    approved offline, declined offline, or transmitted online
- Terminal risk management
  - Floor limit checking
  - Random transaction selection
  - Velocity checking
- Terminal&card action analysis
  - T: reject transaction offline $\Rightarrow$
    C: reject offline
  - T: transaction should go online $\Rightarrow$
    C: go online $\vee$ reject offline
  - T: transaction might be completed offline $\Rightarrow$
    C: go online $\vee$ reject offline $\vee$ approve offline

Conclusion & References

- EMV introduces the Chip&PIN technology
  - Chip cards provide more secured storage for sensitive data
    - ★ If SDA is not used ...
  - PIN-based user authentication is more secure (for whom?)
    - ★ If the secure method is negotiated ...
- Several online references:
  - EMV 4.1 Specifications
    http://www.emvco.com/cgi_bin/detailspec.pl?id=5
  - EMV POS terminal interceptor
    http://www.cl.cam.ac.uk/~mkb23/interceptor/
  - Chip and SPIN webpage http://www.chipandspin.co.uk/ and article
    http://www.cl.cam.ac.uk/~mkb23/spin/spin.pdf

Conclusion & References

- EMV introduces the Chip&PIN technology
  - Chip cards provide more secured storage for sensitive data
    - ★ If SDA is not used ...
  - PIN-based user authentication is more secure (for whom?)
    - ★ If the secure method is negotiated ...
- Several online references:
  - EMV 4.1 Specifications
    http://www.emvco.com/cgi_bin/detailspec.pl?id=5
  - EMV POS terminal interceptor
    http://www.cl.cam.ac.uk/~mkb23/interceptor/
  - Chip and SPIN webpage http://www.chipandspin.co.uk/ and article
    http://www.cl.cam.ac.uk/~mkb23/spin/spin.pdf