John Beric and Mike Ward
February 1, 2012

MasterCard Worldwide

The practical application of cryptography to international card payments

EMV heuristics and standards

Colloquial expression of requirements

Consumer

- No unauthorised debits to their account
  - No modifications to an authorised transaction
  - No omissions of authorised transactions
  - Privacy
  - Audit and enquiry trail
  - Consumer protection checks and balances

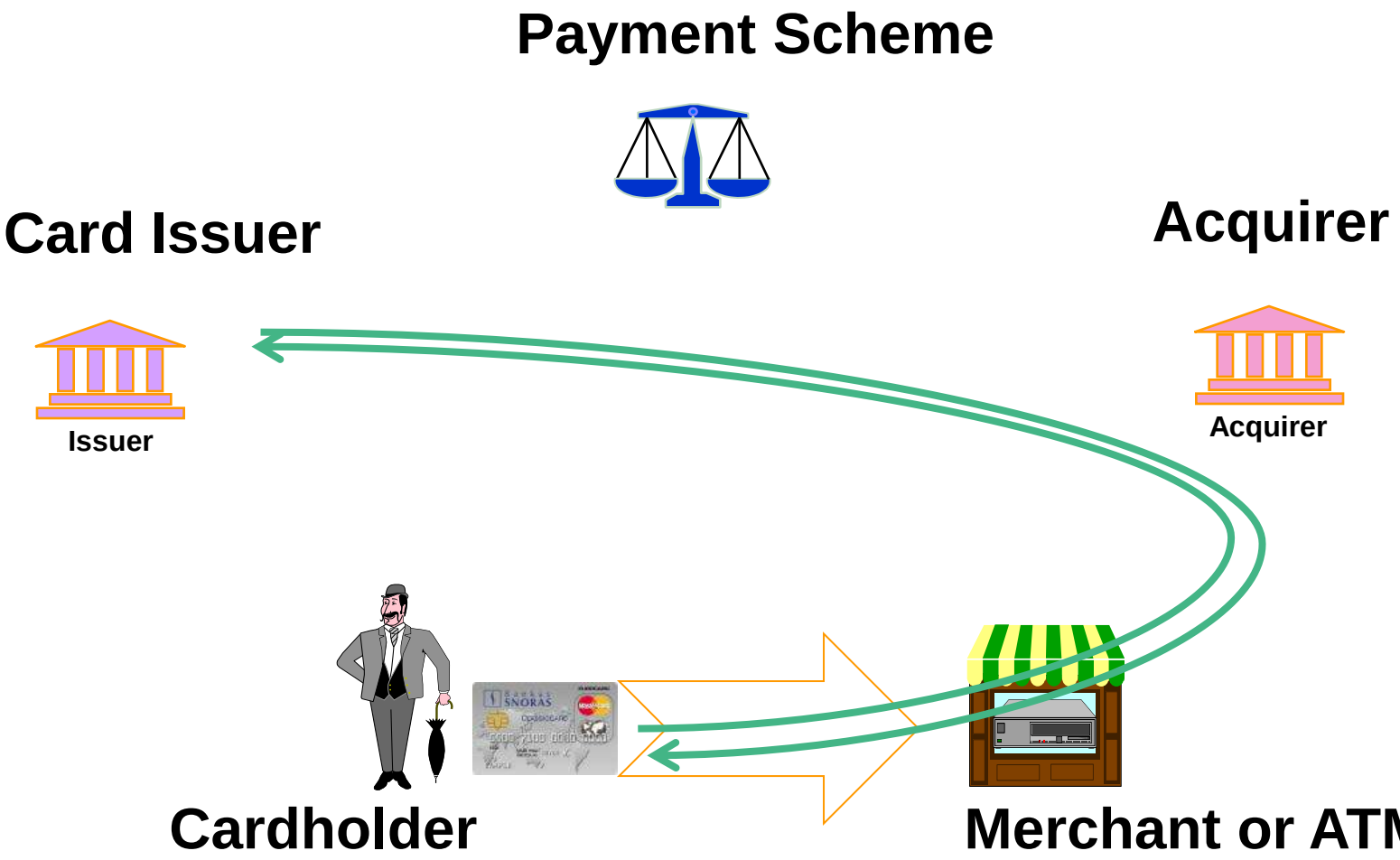
Merchant

- Funds received for release of goods/services
  - Integrity of an authorised transaction
  - Source authentication of authorisation
  - Non repudiation of a properly constructed authorisation
  - Audit and enquiry trail

Financial institution

- Source authentication of the merchant/cardholder
- Non-repudiation by acceptor /cardholder
- Data integrity for both originated and received
- Identification and rejection of counterfeit cards

Card Payments - The Players



Symmetric Cryptography

Cryptograms from card

- ARQC, TC, AAC
- 8 byte MACs on critical transaction data

Response from Issuer

- Issuer authentication by card (4-8 byte cryptograms)
- Secure Messaging: Card block/unblock, PIN Change

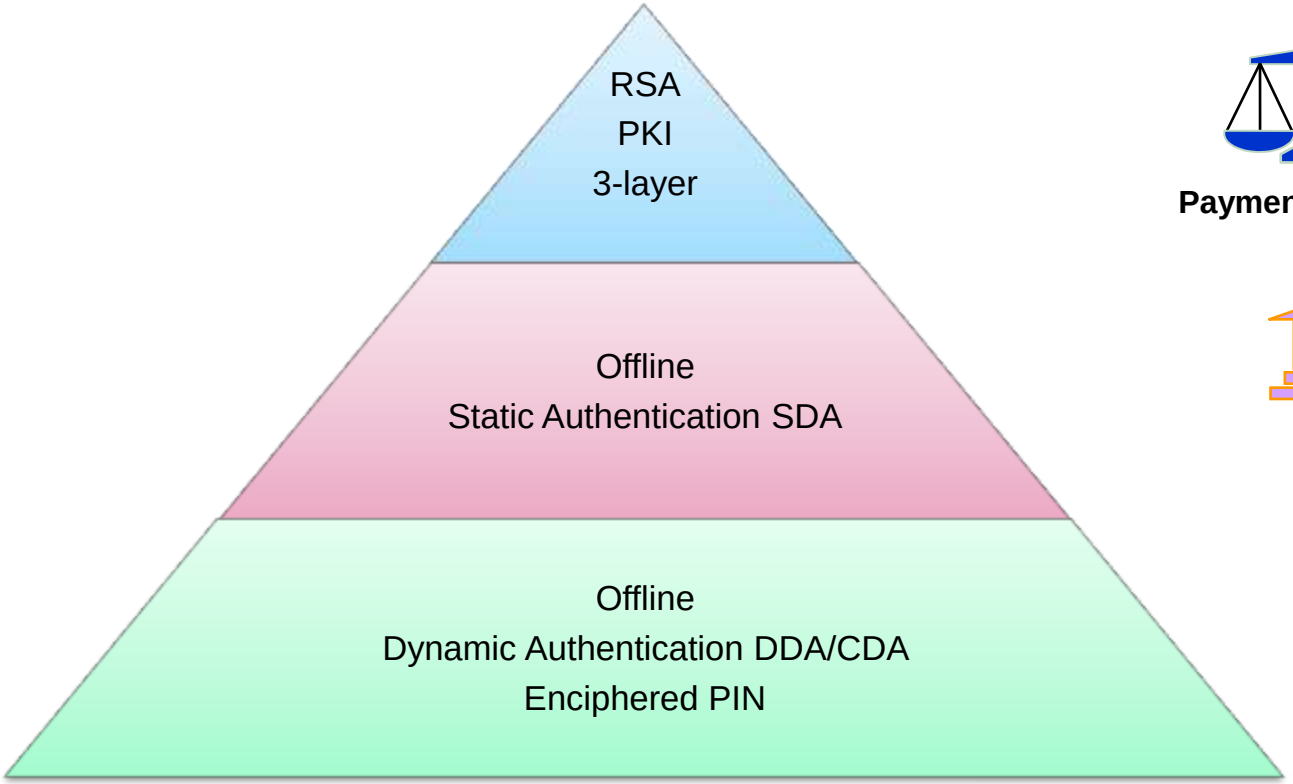
EMV recommended key derivation

- Card keys derived from Issuer keys using Card Number
- Session keys derived using Transaction Ctr and/or UN

MACs: EMV recommends ISO/IEC 9797-1

- Algorithm 3 (ANSI Retail MAC with 2-key TDES)
- Algorithm 5 (CMAC with AES-128/192/256)

Asymmetric Cryptography



Payment Scheme

Key Pair

Issuer

Key Pair

Card

Key Pair

- ISO/IEC 9796-2: Digital Signature Scheme giving message recovery – Part 2: Integer Factorization based methods (method 1) with SHA-1
- Signature formats and PIN encipherment are EMV proprietary

Experience and Research I

MasterCard Worldwide

Requirements
Recommendations
Best Practice

Session Key Derivation
Secure Messaging

Issuer Auths
Crypto Failures

Random Numbers
MACs

2-key Triple DES

References

Experience and Research II

MasterCard Worldwide

Payment System RSA key lengths

768, 896, 1024,1152, 1408,1984

Low-exponent

~~e=2 Rabin~~

e = 3 or 65537

References

References

RSA Signatures ISO/IEC 9796

$\sigma = (6A||m_1||h(m)||BC)^d \bmod n$

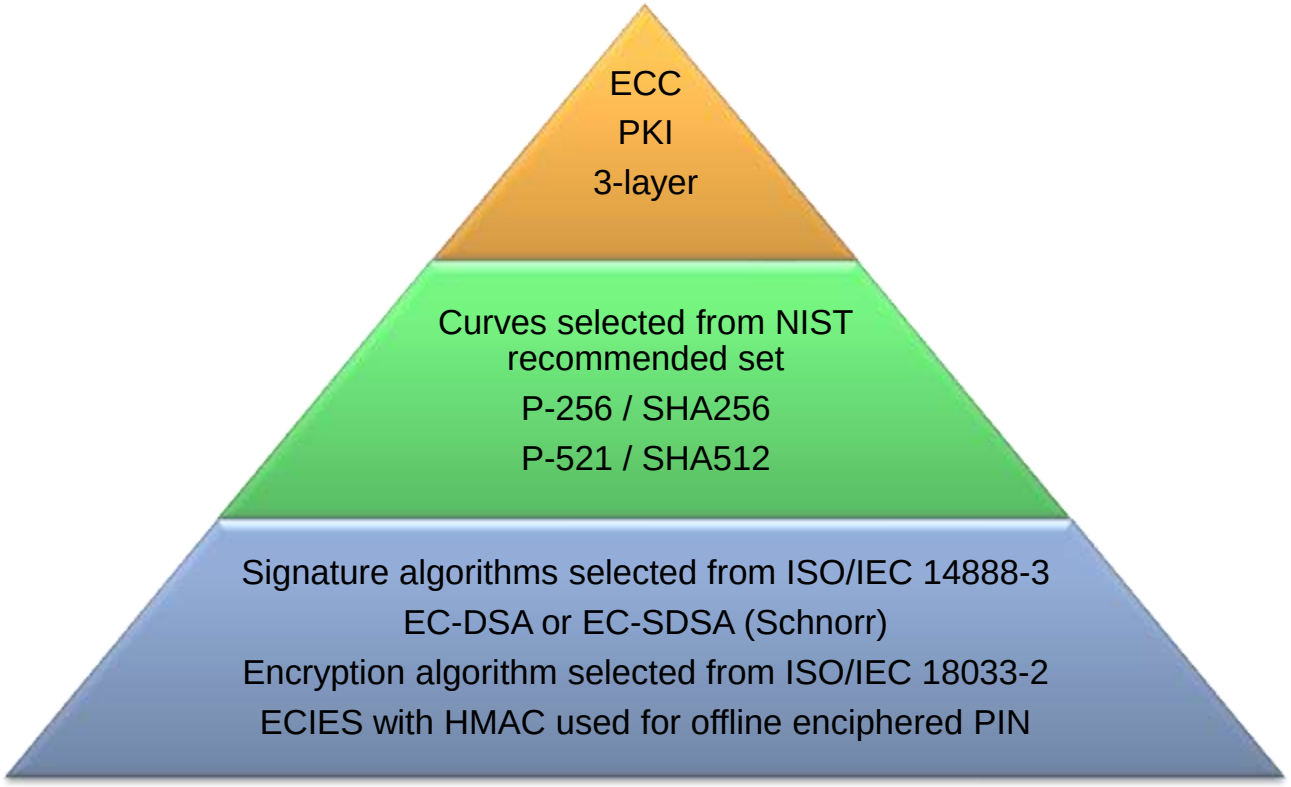
CRT RSA Key Gen

RSA Encryption Key Separation

$Enc(pin) = (7F||pin||UNcard||RANDterminal)^e \bmod n$

References

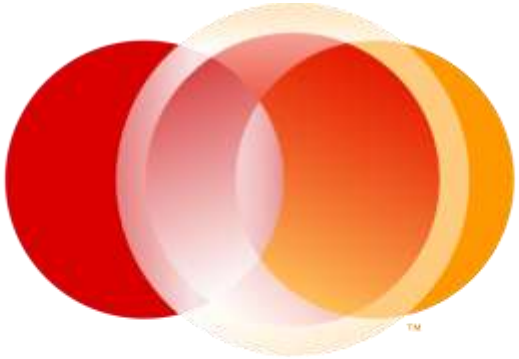
Future Asymmetric Cryptography (work in progress)



Hash algorithm selected from ISO/IEC 10118

- Defaults are SHA256 (for P-256) and SHA512 (for P-521)
- Considering also SHA3 (due 2012) or AES-based hash

References



MasterCard
Worldwide

The Heart of Commerce™

Symmetric Cryptography references

- A note on EMV secure messaging in the IBM 4758 CCA, Adida, Anderson, Bond, Clulow, Lin, Rivest, 2005
- The frequency injection attack on ring-oscillator-based true RNGs, Markettos and Moore, 2009
- The security of the cipher block chaining message authentication code, Bellare, Kilian, Rogaway, 1994.
- A key recovery attack on the ANSI X9.19 retail MAC, Preneel, van Oorschot, 1996.
- A new key recovery attack on the ANSI retail MAC, Mitchell, 2002.

- A known-plaintext attack on two-key triple encryption, van Oorschot and Wiener, 1990
- Attacking triple encryption, Luchs, 1998.
- NIST FIPS 197 The Advanced Encryption Standard, 2001
- ISO/IEC 18033-3 IT Security Techniques – Encryption Algorithms – Part 3: Block Ciphers
- NIST Special Publication 800-57 Recommendation for key management – Part 1: General, 2011
- ECRYPT Yearly report on algorithms and key sizes.
- ISO TR 14742 Financial services — Recommendations on cryptographic algorithms and their use
- ISO/IEC JTC1 SC27 SD12 On the assessment of cryptographic algorithms and key lengths

- A provable-security treatment of the key-wrap problem, Rogaway and Shrimpton, 2006
- Format-preserving encryption, Bellare, Ristenpart, Rogaway, and Stegers, 2009

Brøk

Low Exponent RSA

- Low-exponent RSA with related messages, Coppersmith, Franklin, Patarin and Reiter, 1996.
- Small solutions to polynomial equations and low exponent RSA vulnerabilities, Coppersmith, 1997
- New Attacks on PKCS#1 v1.5 Encryption, Coron, Joye, Naccache, Paillier, 2000

- Twenty years of attacks on the RSA cryptosystem, Boneh, 1999
- Breaking RSA May Be As Difficult As Factoring, Brown, 2005
- Using LLL-Reduction for Solving RSA and Factorization Problems: A Survey, May, 2010

Back

RSA Signature references

- On the security of RSA padding, Coron, Naccache, Stern, 1999
- On Rabin type signatures, Joye and Quisquater, 1999
- A Chosen Messages Attack on the ISO/IEC 9796-1 Signature Scheme, Grieu, 2000
- Cryptanalysis of ISO/IEC 9796-1, Coppersmith, Coron, Grieu, Halevi, Jutla, Naccache, Stern, JoC 2008

- Practical Cryptanalysis of ISO/IEC 9796-2 and EMV Signatures, Coron, Nacccache, Tibouchi and Weinmann, 2009

- Fault Attacks on RSA Signatures with Partially Unknown Messages, Coron, Joux, Kizhvatov, Naccache, Paillier, 2009
- Fault Attacks Against EMV Signatures, Coron, Naccache, Tibouchi, 2010

- Modulus Fault Attacks Against RSA-CRT Signatures , Brier, Naccache, Nguyen, Tibouchi, 2011

Back

RSA Encryption references

- Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1, Bleichenbacher, 1998
- A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1 v2.0, Manger, 2000
- OAEP reconsidered, Schoup, 2001

- Breaking RSA-based PIN encryption with thirty ciphertext validity queries, Smart, 2009

- Universal padding schemes for RSA, Coron, Joye, Naccache, Paillier, 2002
- On the joint security of encryption and signature in EMV, Degabriele, Lehmann, Paterson, Smart, Strefler, 2011

Back

Original and Next Step references

Original EMV

- Contemporary Cryptology: the science of information integrity, Simmons, 1992
- Final report of the RACE Integrity Primitives Evaluation, 1995
- Precautions taken against various potential attacks in ISO/IEC DIS 9796, Digital signature scheme giving message recovery, Guillou, Quisquater, Walker, Landrock, Shaer, 1990
- A method for obtaining digital signatures and public key cryptosystems, Rivest, Shamir, and Adleman, 1978
- Digitized signatures and public-key functions as intractable as factorization, Rabin, 1979

Next ECC

- Efficient signature generation for smart cards, Schnorr, 1991
- The exact security of digital signatures, Bellare and Rogaway, 1996
- Flaws in applying proof methodologies to signature schemes, Stern, Pointcheval, Malone-Lee, Smart, 2002
- Another look at “Provable Security” II, Koblitz and Menezes, 2006
- Security arguments for digital signatures and blind signatures, Pointcheval and Stern, 2000.
- Deterministic polynomial time equivalence of computing the RSA secret key and factoring, Coron and May, 2005
- Hash function requirements for Schnorr signatures, Neven, Smart, Warinschi, 2009
- Intractable problems in cryptography, Koblitz and Menezes, 2010

Back