european cards stakeholders group

Card Payments Cryptography

Strategy for ECSG going forward in the advent of Quantum Computing

DISCLAIMER: The information, data and other materials contained therein are provided to you "as is" without warranty of any kind, and are not intended to provide, and do not constitute regulatory or legal advice to any individual or entity. The ECSG does not accept any liability for any error, omission or non-conformance, and your use of the information, data and other materials contained therein is at your own risk.

Brussels - 22/04/2020

European
Cards
Stakeholders
Group

ADDRESS

Rue Abbé Cuypers 3,
1040 Brussels, Belgium
secretariat@e-csg.eu

Introduction

This presentation describes an analysis made by the ECSG and is currently in an early stage, e.g. regarding the analysis on AES256 or versions with shorter key lenght.

ECSG will continue to investigate the progress made in Quantum Computing and Cryptography and will adjust accordingly the possible strategies identified.

The work is based on the following issue to solve:

- The length of RSA keys supported by the current (1st Gen) EMV specifications is limited. Therefore EMVCO developed specifications supporting ECC for asymmetric cryptography (2nd Gen). Migration aspects to ECC were however not specified, such as POI updates.

- In the meantime EMVCo decided to not publish the 2nd Gen specification, but to enhance 1st Gen specifications with ECC (1st Gen+). In addition discussions about a new EMVCo Contactless Kernel started including considerations for common recommendations on how to use ECC in existing kernels.

Background: Quantum Computing (QC)

- QC developments are attracting a growing amount of investments from both National Governments and Industry. The question about QC is no longer “if” but “when”.
- QC is not about increasing the computing power of traditional computers. It is a paradigm shift based on quantum physics and carries with it stringent operation requirements (e.g. temperature) and new logical gates, amongst many other changes.
- QC new computational “logic” will have many useful applications to solve some old and new problems at incredible speed when compared to even the highest spec Super Computer of today
- Unfortunately it has been proven that QC – when it becomes practically available– will be able to break most of the current cryptographic algorithms used in card payments

Impact of QC

According to expert agencies, QC will be able to break

- Symmetric (a.k.a. “Private Key”) Cryptography (used for cryptograms and for online PIN Encryption)
  - Triple DES
  - AES with 128 Bit key

- Asymmetric (a.k.a. “Public Key”) Cryptography (used for offline Card Authentication and for offline PIN Encryption)
  - RSA
  - ECC (Elliptic Curve Cryptography)
    - *Important Note:* ECC is proposed by EMVCo as a more efficient alternative to RSA, given the increased length of RSA keys needed to stay abreast of super-computer attacks.

Cryptographic algorithms resistant to QC attacks

Symmetric Cryptography

- AES with 256 Bit key: This is the only Quantum-Resistant Algorithm endorsed by the financial industry

Asymmetric Cryptography

- These algorithms are not yet available.
- NIST has in place a formal, open process to define such algorithms.
- According to ASC X9 the timeline looks as follows:

  - Selection of candidates (in different phases)
  - Standardization
  - Development
  - Deployment
  - Expect QC-Resistant algorithms deployed in 20 years from now

This will impact

- All current EMV based cards that do not currently support AES256
- All POI PTS terminals that currently do not support AES256.

Several Industry Bodies are working on this topic

- The INNO ET group has taken into account and used as reference reports from these expert organizations:
  - ➢ ASC X9, NIST, German BSI
- As well as from these ECSG members: EPC and EMVCo
  - ➢ EPC Highlights:
    - From EPC342-08v9.0 report, which covers PSP needs at large and not only card payments
      - citing BSI report, a stable QC could be "decades away";
      - ECC is a valid option for systems with performance constraints and use AES-256 if long term confidentiality (that is, for several decades) is needed.
  - ➢ EMVCo Highlights:
    - Will shortly publish specific ECC algorithms options for contact transactions in line with NIST security recommendations.
    - Is considering the possibility to develop a new single contactless Kernel which would support the ECC algorithms.

Strategic options considered

For Symmetric Cryptography:

- Move from Triple DES and AES128 towards AES256

For Asymmetric Cryptography:

- While the expert community gathers around the NIST process to find the best possible Quantum-Resistant algorithm the present alternatives for the cards payments industry are as follows:

1. "ECC" : Migrate from RSA to ECC and then at a later stage to QC-Resistant algorithms when available.
   - ➢ Even if ECC is also vulnerable to QC attacks, ECC solves the current RSA key-length inflation issue.

2. Not move to ECC and wait until QC-Resistant algorithms are available.
   - ➢ In the meantime, wherever possible, migrate to a full online-only environment.

3. RSA:
   - ➢ Two RSA options have been considered. One is to stay with RSA "as is" (current key lengths). The other is to continue with RSA but using longer keys, even if this would not be supported by EMVCo.

High-level impact analysis of all Asymmetric options is included in an annex to this presentation.

- ➢ One Annex includes options 1 and 2
- ➢ Another Annex include the two RSA options

Strategic options proposed

For Symmetric Cryptography:

- Move from Triple DES and AES128 towards AES256
- The need to move from triple DES towards AES256 should be clearly communicated by the ECSG and this migration made effective by all stakeholders in the shortest timeframe possible. (*)

For Asymmetric Cryptography, two options are retained for further consideration:

1. ECC: Migrate from RSA to ECC and then at a later stage to QC-Resistant algorithms when available. (*)
2. Not move to ECC and wait until QC-Resistant algorithms are available. In the meantime, wherever possible, migrate to a full online-only environment.
   - Some environments such as Mass Transit may still require the use of Asymmetric Cryptography – In those cases RSA would continue to be used.

(*) Note: There may be synergies (e.g. cost, testing, time-to-market) to be achieved by combining the AES migration with the ECC migration.

Annex 1

High Level Analysis of RSA Options

Key impacts of keeping RSA Cryptography (I)

	RSA as it is	RSA with longer certificates
Interaction Payer/Payee	No Impact	No Impact
Reputational Risk in case of attack	Yes (for not having migrated to ECC, not followed NIST or EMVCo recommendations)	Limited (not unless EMVCo keeps the annual key lengths assessment) Successful attacks on a single card possible (ICC key max 1640 bit), but very limited impact
Security Function Relay Resistance Protocol	Only some schemes specify RRP	Only some schemes specify RRP
Security Function Secure Channel	Secure Channel can be done through RSA (instead of ECC as proposed by EMVCo) but poor performances and requires update of EMV specifications	Secure Channel can be done through RSA (instead of ECC as proposed by EMVCo) but poor performances and requires update of EMV specifications

Key impacts of keeping RSA Cryptography (II)

	RSA	RSA with longer certificates
Replacement of Terminals (Hardware)	No impact	? (support of RSA 4096)
Terminal Software (Kernel)	No	Yes – update of EMVCo specs to support « split certificates » over several records with new tags, and kernels to recover them properly.
Card Replacement and personalization	No	Yes – perso to support « split certificates » over several records with new tags, introduction of new mechanism similar to EMVCo ECC proposal (AIP bit, normal card lifecycle)

Annex 2

High Level Analysis of ECC and Online only Options

Key impacts of current alternatives for Asymmetric Cryptography (1/2)

	ECC	Online Only
Interaction Payer/Payee	No Impact	May disrupt some offline use cases like mass transit as well as remove fall-back possibilities if online is not available
Security Function Relay Resistance Protocol	RRP was designed offline for the EMVCo Next Gen Draft	Viability of RRP done online to be assessed
Security Function Secure Channel	- Easy to implement - Secure Channel is established automatically through Diffie-Hellmann Key Exchange and includes card authentication	Lack of Offline PIN encryption method (Offline PIN is still a viable solution also for online-only cards)

Key impacts of current alternatives for Asymmetric Cryptography (2/2)

	ECC	Online Only
Replacement of Terminals (Hardware)*	- A vast majority of equipment can be updated to handle ECC, only old legacy terminals can not be updated to support ECC - New terminals supporting PCI-PTS v6 will include support of ECC as per PCI mandate	No replacement needed
Terminal Software (Kernel)	Yes – As a upgrade or as an addition of new Kernel Kernel can manage both ECC and RSA cards An additional Kernel or major upgrades may imply replacement of terminals	Configuration update should be sufficient (e.g. by setting Terminal Action Codes to online only, Zero Floor Limits etc.)
Card Replacement and personalization	Yes – Can follow normal expiry cycle	No Most cards can be configured for online only via issuer scripting

*Migration to AES 256 may require replacement of terminals