



## **EMV® Contact Chip Specification Elliptic Curve Cryptography**

### **Frequently Asked Questions (FAQ)**

#### **1. What has EMVCo published?**

Specification Bulletin 243<sup>1</sup> to enable the use of Elliptic Curve Cryptography (ECC) for EMV® contact chip payment transactions has been published following approval of its release by EMVCo's Board of Advisors.

#### **2. What is ECC and why is EMVCo incorporating it into its specifications?**

In an EMV contact payment, the merchant POS terminal can cryptographically authenticate a card and its data by verifying digital signatures generated by the card, its issuer and the payment system.

Since its inception, the EMV Contact Chip Specification has used RSA (Rivest-Shamir-Adleman) public key cryptography whose security depends on the so-called factorisation problem. This has proven to be robust and provides strong security.

ECC is another form of public key cryptography based on the algebraic structure of elliptic curves over finite fields.

While ECC and RSA can each be used to secure transactions, ECC can be used with much smaller key sizes due to its greater security efficiency when compared to RSA.

The size of a cryptographic key is important. As a general rule, the longer the key the more storage and processing power required.

EMVCo recognises that RSA could continue to be used with longer and therefore 'stronger' keys over time; however, the increase in key length increases computing time making transaction times slower. In contrast, ECC is compact and efficient, which makes it an appealing option for use in devices with limited storage and processing capabilities, and where transaction speed is important.

#### **3. What benefit does ECC bring to the wider payment community?**

ECC enables the payment community to achieve security without impacting technical performance, constraining payment innovations or restricting existing and new

---

<sup>1</sup> EMVCo publishes Specification Bulletins as and when required to detail and confirm changes to the EMV Specifications. Over time, once a number of updates have been made, an editorial update is undertaken to include the bulletins into the larger specification document. SB 243 is to be incorporated in the Contact Card Specification v4.4.

---



transaction scenarios. It is a particularly appealing option for use in devices with limited storage and processing power.

ECC achieves this efficiency and scalability over the more conventional RSA public key cryptography, while minimising changes to the overarching key management infrastructure.

It also provides the EMV community with a state-of-the-art security standard that will evolve in line with new technologies and has the ability to support the long-term needs of EMV Specifications.

#### **4. Will this make contact payments more secure?**

No. ECC doesn't necessarily make payments more secure than today. It does, however, enable robust security to be maintained as payment technology advances and innovates, due to the possibilities presented by the small key lengths and digital signatures.

It is also important to note that the payment community approaches security in 'layers', using many different techniques to combat fraud. Cryptography is just one of these layers of protection.

#### **5. Why is EMVCo introducing ECC now?**

EMVCo continually evaluates its security offering and monitors developments within the industry. In 2010, the U.S. National Institute of Standards and Technology (NIST) announced that it would not support the use of EMV's longest RSA 1984-bit key length after 2030. EMVCo works to align with other bodies and identified that it was important to provide a security roadmap that supports the long-term security needs of the wider industry. It has taken EMVCo time to not only include the technical details of the ECC standard, but also identify how best to incorporate it into the future of EMV chip technology offering.

#### **6. Will EMVCo continue to support RSA and undertake an RSA key length review?**

Yes. EMVCo looks at RSA lengths annually and recommends updates. This ongoing review will continue while there is demand within the payments sector.

EMVCo offers a suite of technical solutions and options to the payment community. In the context of cryptography, this now includes RSA and ECC. It also includes the cryptographic hash functions and block cipher-based methods supported by EMV.

Going forward, however, emphasis is to be placed on the long-term role of ECC within the EMV payment ecosystem due to its smaller key size and the possibilities that this presents.

---



**7. Will there be a testing infrastructure to confirm payment products are using ECC as specified by EMVCo?**

Yes. EMVCo has begun work to update its testing and certification programme to validate cards and payment acceptance terminals to confirm that they align to this new specification. EMVCo is already working with its network of test tool vendors and test laboratories globally to ensure products and services are available worldwide. Updates will be provided via the EMVCo website.

**8. How will the industry migrate to ECC?**

Updates to the EMV contact chip technology infrastructure to incorporate ECC will be part of the natural product lifecycle over a period of time for both cards and point of sale terminals.

During EMVCo's engagement process with payment acceptance terminal manufacturers, it was highlighted that many terminals already have the capability and capacity to support ECC today.

*As a technical body, EMVCo does not mandate the use of its specifications or set the business rules related to how the technology is implemented. Industry stakeholders are free to choose from any or all of the related EMV Specifications to address their customer and marketplace needs. To learn more about the role EMVCo plays within the payments ecosystem, read its [Operating Principles](#).*

**9. What role has the payment community had in deciding to use ECC?**

EMVCo has been working with the EMV Associate and Subscriber community for some time on how to enhance the EMV Chip Specifications. Security has consistently been a key element of this discussion.

Additionally, EMVCo's security experts have extensive engagement with leading academics at the forefront of advancements in cryptography.

**10. What about EMV contactless chip payments? Is EMVCo also going to incorporate ECC?**

EMVCo does not manage an EMV Contactless Chip Specification but makes recommendations to payment systems to ensure consistency and support innovation. Within this context, the use of ECC in EMV contactless chip payment cards is being considered.

**11. What about Quantum Computing, how does this impact ECC and EMV cryptography?**

---



EMVCo is monitoring the role of Quantum Computing and its impact. It is engaged in efforts led by the NIST on quantum-resistant cryptography.

It is important to note, however, that EMV Chip exclusively uses cryptography for real-time payment authorisation and terminal PIN protection. This contrasts with other use cases that need information that is protected now to remain confidential for many years and survive the arrival of cryptographically significant quantum computers.

*EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo, LLC.*

---