

EMV® Chip Specifications To Support Elliptic Curve Cryptography

Cryptography standard enables robust EMV® contact chip security long-term as payment technology evolves

28 October 2021 – The EMV® Contact Chip Specification, managed by global technical body [EMVCo](#), now supports Elliptic Curve Cryptography (ECC). Use of this cryptography standard by the payment community can enable enhanced security without impacting technical performance of a payment device or slowing transaction processing time. The inclusion of ECC is required to support new, future payment scenarios.

In an EMV contact chip payment, the merchant point-of-sale terminal can cryptographically authenticate a card and its data. For this purpose, EMVCo has based its EMV Contact Chip Specifications on RSA (Rivest-Shamir-Adleman) public key cryptography since its inception and intends to continue to support this standard. The addition of ECC into EMV Specifications helps achieve superior cryptographic strength with much smaller key sizes, enabling more efficient transactions in the future.

Robin Trickel, EMVCo Executive Committee Chair, explains: “The longer the cryptographic key used to secure a transaction, the more storage and processing power required. The size of a cryptographic key is therefore important. EMVCo recognises that RSA could continue to offer ‘stronger’ keys, however, these would increase in length resulting in slower computing and transaction times. In contrast, ECC is compact and efficient, making it an appealing option for use in devices with limited storage and processing capabilities.”

EMVCo has been working with the payment community for several years through its [Associate Programme](#) to identify how it can facilitate scalable security as payment practices and technology evolve.

“ECC provides strong security efficiency when compared to RSA, which is essential to ensure a smooth migration,” adds Trickel. “So while it doesn’t make current payments more secure today, it ensures robust security can be maintained in new payment innovations, setting the foundation to support the long-term security needs of the payment community.”

The EMV Contact Chip Specification for ECC ([Specification Bulletin 243](#)) has been published following approval of its release by EMVCo’s Board of Advisors and is available for royalty-free download from

www.emvco.com. Updates to the EMV chip technology infrastructure will be part of the natural product lifecycle over a period of time for both cards and point-of-sale terminals.

EMVCo aims to provide EMV technology users with a suite of options to meet regional and local requirements. Both ECC and RSA will be supported by EMVCo while there is demand within the payment community. EMVCo does not mandate the use of encryption standards.

[Read the FAQ to learn more.](#)

– ENDS –

For further EMVCo media information please contact David Amos / Chloe Smith – Tel: +44 113 3501922 or email: david@iseepr.co.uk / chloe@iseepr.co.uk

To unsubscribe from future EMVCo news, reply 'unsubscribe' to this email.
Click [here](#) to read our privacy policy.

Notes to Editors:

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.

About EMVCo:

EMVCo creates and manages EMV Specifications and programmes that enable seamless and secure card-based payments for businesses and consumers worldwide.

EMV Specifications support technologies including EMV Chip [Contact](#), EMV Chip [Contactless](#), [Mobile](#), [QR Code](#), [Secure Remote Commerce](#) (SRC), [3-D Secure](#) (3DS) and [Payment Tokenisation](#) and are widely used by the payments industry to develop products and services that deliver trusted and convenient in-store, online and remote card-based payments.

As a global technical body, EMVCo is collectively owned by American Express, Discover, JCB, Mastercard, UnionPay and Visa. Hundreds of payments stakeholders, including merchants, banks and technology providers, participate as EMVCo [Associates](#) and [Subscribers](#) to develop, evolve and enhance flexible EMV Specifications that support innovation and address marketplace needs. All EMV Specifications are available royalty free on the EMVCo website.

www.emvco.com | [EMV® Insights](#) | [LinkedIn](#) | [Twitter](#) | [Podcast](#) | [An Introduction to EMVCo](#) | [YouTube](#)