EMV® General Bulletin No. 55
First Edition August 2022

Guideline for ECC Issuer Self-signed Public Key Certificates

This General Bulletin defines a recommended format for ECC Issuer self-signed public key certificates.

Payment systems may decide individually whether to adopt the recommendation in this General Bulletin when processing Issuer certificate requests in the context of:

- *EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 – Security and Key Management, Version 4.3, November 2011*

as updated by Specification Bulletin 243.

Field Name	Length (bytes)	Description	Format
Certificate Format	1	Hex '28'	b
Certificate Encoding	1	Hex '00'	b
Issuer Identifier	5	Leftmost three to ten digits from the Primary Account Number (PAN), padded on the right with hex 'F's.	cn 10
Issuer Public Key Algorithm Suite Indicator	1	Indicates the algorithms to be used with the Issuer Public Key that is used to verify ICC Public Key Certificates and this Issuer Self-Signed Public Key Certificate.	b
Certificate Expiration Date	4	Year, month, day (YYYYMMDD) after which this certificate is invalid. This field is also used to define the requested expiration date of the Issuer Public Key Certificate generated by the Payment System Certification Authority.	n 8
RID	5	Identifies the Payment System which is requested to sign the Issuer Public Key.	b
Certification Authority Public Key Index	1	When combined with the RID, uniquely identifies the Payment System key to be used to sign the Issuer Public Key and the associated algorithm suite.	b
Payment System Proprietary Identifier	4	Proprietary Identifier whose usage is determined by the Payment System and whose value is assigned by Payment System or Issuer (e.g. for identifying a service).	b
Tracking Number	4	Proprietary Tracking Number whose value is assigned by Payment System or Issuer.	n 8
Issuer Public Key	N_{FIELD}	Representation of Issuer Public Key (x-coordinate of Issuer public key point) on the curve identified by the Issuer Public Key Algorithm Suite Indicator.	b
Issuer Public Key Certificate Signature	N_{SIG}	Output of digital signature ECC algorithm on concatenated first ten data objects using the Issuer private key on the elliptic curve identified by the Issuer Public Key Algorithm Suite Indicator.	b

Legal Notice

This document is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement this document is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with this document.