EMVCo™

EMV®

Mobile Payment

Consumer Device Cardholder Verification Method—Best Practices

Version 1.0

15 March 2019

Legal Notice

This document summarizes EMVCo's present plans for evaluation services and related policies and 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.

Contents

Tables

1 Introduction

This document provides best practice guidelines for the implementation and use of CDCVM Solutions. These best practices are intended to balance user experience, security and relating to enabling one or more CDCVMs on a Consumer Device and the usage of CDCVMs when initiating a payment or during payment processing. The best practices are focused on aspects of a CDCVM Solution that are not covered in a security evaluation of the solution or, if for example, a biometric is used as the verification method by the solution, are not covered in the biometric evaluation of the solution.

1.1 Target Audience

This document is intended for use by architects and developers of CDCVM Solutions, Consumer Device architects, payment service and Token Service Providers, Payment Systems, security laboratories, and Mobile Application providers.

1.2 Supporting Documentation

Table 1.1: Related Documentation

Reference	Document
BIO_REQ	FIDO Biometrics Requirements, working Draft August 30, 2018
CDCVM_REQ	Consumer Device Cardholder Verification Method Security Requirements

1.3 Definitions

Table 1.2: Definitions

Term	Definition
Authentication Policy	Configuration or default settings within a relying entity related to when consumer authentication is required. For example, instant, prolonged, persistent. And in the case of the latter two, the period of time within which a previously performed consumer authentication will be accepted.
CDCVM	Consumer Device Cardholder Verification Method is a form of CVM where the comparison of the method captured is compared with reference data on a Consumer Device itself. CDCVM examples are a passcode, password, pattern (e.g. used for Android device unlock) or a biometric (e.g. fingerprint, iris, facial).
FAAR (False Artefact Accept Rate)	The percentage of artefacts that are incorrectly accepted by the system. An artefact is an artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns. (See ISO/IEC 30107-1)
FAR (False Accept Rate)	The proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed. See Section 4.6.6 in (ISO/IEC 19795-1).
FRR (False Reject Rate)	The proportion of verification transactions with truthful claims of identity that are incorrectly denied. See Section 4.6.5 in (ISO/IEC 19795-1).
Instant (authentication/ verification)	Prompt for CDCVM for every transaction.
Not Verified	An indication from the CDCVM solution that CDCVM has not occurred. This verification result could be in response to a request from a relying application inquiring whether successful verification of a CDCVM has occurred within a specified timeframe.
Persistent (authentication/ verification)	Prompting for CDCVM is not necessary as long as certain conditions remain satisfied (for example consistent monitoring of the consumer presence).
Platform	The underlying device on which an application is deployed. This is a combination of the hardware, firmware, operating system and built in functionality of the device.
Prolonged (authentication/ verification)	Prompt for CDCVM only if a CDCVM has not occurred within a pre-defined time period
Reference Data	A stored value against which the captured verification data is compared.
Relying Party	An entity that relies on a CDCVM Solution to provide consumer authentication functionality.

Term	Definition
Verification Attempt Failed	An indication from the CDCVM solution that CDCVM capture has been attempted in response to a request and that verification has failed. This verification result could be in response to a request from a relying application to prompt for, capture and verify a CDCVM. For example, a biometric or password match was not successful.
Verification Data	A consumer biometric, or a value known to the consumer, captured when prompting for a CDCVM.
Verified	An indication from the CDCVM solution that CDCVM has been successfully performed. This verification result could be in response to a request from a relying application to prompt for, capture and verify a CDCVM or in response to a request from a relying application inquiring whether verification of a CDCVM has occurred at some point in the past. Each CDCVM solution could have a different setting for how long this state remains active or what events cause this state to transition to Not Verified.

2 CDCVM Solution Best Practices

The following are a set of best practices that should be considered as integral to a CDCVM Solution and that should be considered when implementing or using a CDCVM Solution to prevent unauthorised access to a device and the usage of CDCVMs by Mobile Applications. While it is understood that these best practices are not relevant to every CDCVM Solution, usage thereof, or to every Mobile Application it is expected that where applicable, the implementation and usage of a solution should make every effort to meet or exceed the best practice listed hereunder.

Best practices included in this document are grouped into the following categories:

- **Functional**—Applies to the User Experience and other aspects such as:
    - Indication of password/passcode/pattern strength
    - Time taken to verify a biometric
    - Behaviour when an invalid password/passcode/pattern is entered or the verification of a biometric was not successful
- **Relying Party/Mobile Application**—Applies to the Mobile Application using a CDCVM Solution
- **Wearables**—Applies to wearables using a CDCVM Solution
- **Security-related**—Applies to security considerations for the platform and for the CDCVM Solutions incorporated into the platform

2.1 Functional

Table 2.1: Functional Best Practices

ID	Best Practice	Description
1.1	Provide clear indication to the consumer related to the CDCVM being used at the point that the consumer is required to authenticate themselves.	Clearly prompt the consumer to use their preferred CDCVM If a preferred CDCVM is unavailable, provide such an indication and either • Indicate that consumer authentication has been disabled (access is not possible), or, • Prompt the consumer to use an alternative or fall-back CDCVM.

ID	Best Practice	Description
1.2	Provide clear indication to the consumer related to the verification result of a CDCVM at the point that the consumer is attempting to authenticate themselves.	This is intended to inform the consumer that: • If verification of the CDCVM was successful, then it should be clearly evident to the consumer • If CDCVM was not successful, provide such an indication and then, ○ Prompt the consumer to retry (potentially indicate how many opportunities remain), or, ○ Prompt the consumer to use an alternative or fall-back CDCVM.
1.3	When a consumer is choosing a passcode, password or pattern, dissuade the consumer from using “weak” values or patterns. At a minimum the consumer must be informed if they have chosen a weak value.	This is intended to make the consumer aware that the value or pattern chosen is easily guessed by an attacker. Examples of “weak” values are 0000, 1234, password, or, 12345678, and an example of a weak pattern is
1.4	CDCVM solutions may implement a delay between authentication attempts if multiple incorrect attempts have been made.	To balance a brute force attack with convenience in the event that a consumer has temporarily forgotten a password or is unable to present a biometric successfully, the solution can disable the CDCVM for a period of time.
1.5	The sensor should be able to capture an accurate sample in adverse environments	Examples include: • The camera should be able to successfully capture the consumer’s facial image in various lighting conditions • A microphone should be able to successfully capture the consumer’s voice with a reasonable amount of background noise • A fingerprint sensor should be able to capture a fingerprint from both a dry and a wet finger.

ID	Best Practice	Description
1.6	Assuming a relatively proper presentment, the sensor should be able to capture an accurate sample of Verification Data.	This is a broad best practice that is dependent on the capture mechanism and applies largely to verification and to a lesser extent to enrolment that may require multiple presentments. The following are some examples: • A fingerprint sensor should be able to capture a sample with a single presentation. • A camera should have the ability to capture a facial sample at reasonable angles and distances. • A keyboard on a wearable should not be susceptible to incorrect entry of digits/characters—that is, it should not be so small as to make it unusable.
1.7	The solution should be able to verify the consumer in a timely manner.	This is a broad best practice as some authentication mechanisms are by their very nature more time intensive and not always controllable by the solution. For example, the solution cannot control how long it takes the consumer to enter a PIN, password or pattern or to successfully align the device to capture a face or scan an iris. Generally, once the sample has been captured, the verification result should be returned in less than 300ms.

2.2 Relying Party/Mobile Application

Table 2.2: Relying Party/Mobile Application Best Practices

ID	Best Practice	Description
2.1	Mobile Applications should use CDCVM Solutions that adhere to the CDCVM Security Requirements.	Solutions adhering to the requirements provide a level of confidence that CDCVM Solutions used by a Mobile Application are securely implemented and can undergo a Security Evaluation.
2.2	Mobile Applications should be able to indicate which CDCVM Solution(s) are being used based on the EMVCo assigned solution Identifier.	The payment solution should be able to determine the CDCVM Solution used for a specific transaction.

ID	Best Practice	Description
2.3	The Mobile Application should query the verification result of a consumer authentication whenever it determines that a payment is occurring (or is about to occur) and should not maintain the Verified state beyond a defined timeframe.	For example, if possible the verification result should be queried during a payment, or when the user explicitly enables the Mobile Application for payment, rather than when a Mobile Application is opened. Additionally, the Mobile Application should not maintain the Verified state beyond a defined period of time (such as 90s) after which time the verification result should be queried again before a new payment occurs.
2.4	Discontinue the use of a specific CDCVM Solution if that CDCVM Solution, or the underlying platform, indicates that a compromise to that solution has been identified.	In the case that a CDCVM solution, or the underlying platform, surfaces APIs that allow the Mobile Application to be informed of an issue with a CDCVM Solution, the Mobile Application should react appropriately and not allow payment to proceed with that CDCVM.
2.5	The Mobile Application should have the ability to determine when Consumer Authentication occurred so that the verification result is not based solely on the device being unlocked.	This is the caching mechanism for a CDCVM Solution. In the case that a Mobile Application is checking whether Consumer Authentication has occurred, the Mobile Application must make sure that the authentication was not performed too far in the past.
2.6	If there is no CDCVM Solution linked to the Mobile Application, then disable the relevant payment functionality and if necessary delete credentials	For example, the consumer has set the unlocked mechanism to swipe or none, or the consumer has deleted the fingerprint templates.
2.7	Prolonged authentication should only be valid for a limited number of transactions.	A consumer must re-authenticate after a defined number of transactions even if within the defined timeframe for prolonged authentication.

2.3 Wearables

Table 2.3: Wearables Best Practices

ID	Best Practice	Description
3.1	When using a wearable to enable persistent authentication, the loss of presence should be detected within an acceptable period.	The sensor being used to ensure user presence (a switch, infrared (IR) sensor, heart rate (HR) sensor) should be able to recognise loss of presence within three seconds after which the verification state should be reset.
3.2	For a wearable to enable persistent authentication, the consumer must authenticate (either on the wearable or on the companion device) after the user presence has been detected.	The conditions for persistence must be established before consumer authentication is performed.

2.4 Security-related

Table 2.4: Security-related Best Practices

ID	Best Practice	Description
4.1	Do not set a dormant value (factory-set default Reference Data) for a CDCVM Solution	Factory set Reference Data could potentially be determined by malicious parties and then used to gain access to the device and as such provide unauthorised access to a Mobile Application.
4.2	Warn the user when prompting for consumer authentication if the device is not in the appropriate secure state.	At the appropriate points there should be a check that OS counter measures and protections are enabled at run time. Some examples are if the device has been rooted or if USB debugging is enabled.
4.3	Prolonged authentication should not extend beyond a reasonable period of time.	The period should provide confidence that the consumer is still in possession of the device, and it should not exceed 10 minutes.
4.4	If the conditions for persistence are broken, then re-authentication must be performed.	For example, if a wearable device detects that it has been removed, then it should require that the consumer re-authenticate before performing sensitive operations.

ID	Best Practice	Description
4.5	The number of incorrect CDCVM attempts should be limited.	For example: • The number of incorrect attempts allowed prior to disabling a biometric should be between 4 and 11. • The number of incorrect attempts allowed prior to disabling a passcode, password or pattern or introducing a delay should be 3, 4 or 5.
4.6	Do not allow weak CDCVMs	For example: • A passcode should be more than 5 digits. • A password should be more than 5 digits/characters. • A pattern should have more than 5 unique points making up the pattern. The order of points should be taken into account
4.7	Manage the lifecycle of a CDCVM appropriately	It should not be possible to register a new biometric without first authenticating the user. For example, by using a previously registered biometric or a previously set up passcode, password or pattern.
4.8	Biometric modalities should not allow the registration of too many of those same modalities.	One example relates to fingerprints and as such a fingerprint solution should not allow the registration of more than 5 different fingerprint slots. Registering multiple reference data for a single biometric modality increases the likelihood of false acceptance and may result in an effective FAR worse than the FAR of the biometric which is based on a single instance of reference data.
4.9	The platform should provide a means for a Mobile Application to determine whether a suitable level of consumer authentication is active for the device.	A Mobile Application should be able to determine if the device unlock has been rolled back to a non-secure mechanism (e.g. a swipe).

ID	Best Practice	Description
4.10	The fall-back/primary CDCVM should be sufficiently strong.	The passcode/password (and to a certain extent, pattern) used to unlock the consumer device is most likely considered as the primary consumer authentication method. The valid entry of a passcode or password allows the consumer to add/delete/modify reference data for biometric and other consumer authentication methods. In addition, passcode/password is often used as a fallback consumer authentication mechanism when another authentication mechanism fails or is disabled. As a result, the overall strength of the CDCVM mechanisms on a device are dependent on the underlying password/passcode. Use of a weak passcode, password or pattern undermines the FRR, FAR and FAAR rates of a biometric authentication mechanisms.
4.11	For a biometric, there should be a balance between allowing the verification of the incorrect biometric and not verifying the correct biometric.	A biometric should not have a false reject rate (FRR) above 5% at a false accept rate (FAR) of 1 in 10 000.
4.12	There should be a mechanism for liveness detection and the ability to spoof the solution should be minimised.	Some (non-exhaustive) examples are: • When using facial or iris recognition, the solution should be able to differentiate between a photograph and an actual person. • When using fingerprint, the sensor should be able to differentiate between a live finger and a silicone replica.