**Assessment guideline for electronic identification services**

Traficom Guideline 211/2023 O EN

Draft 26.5.2023

Contents

[Annex C: Special criteria for mobile identification solutions 3](#_Toc135996126)

[1 Architecture, design and threat modelling 4](#_Toc135996127)

[2 Data storage and privacy 5](#_Toc135996128)

[3 Cryptography requirements 7](#_Toc135996129)

[4 Authentication, characteristics of the authentication method; session management 8](#_Toc135996130)

[5 Data communication 13](#_Toc135996131)

[6 Platform interaction 14](#_Toc135996132)

[7 Code security, quality and development environment 16](#_Toc135996133)

[8 Security controls and resilience 17](#_Toc135996134)

[References 18](#_Toc135996135)

# Annex C: Special criteria for mobile identification applications

**General**

The mobile application criteria is intended to **complement the general criteria** in case the identification means or identification scheme includes a mobile app.

The criteria is created **primarily for the level of assurance substantial**. References to LoA (Level of Assurance regulation, (EU) 2015/1502) are to the level of assurance substantial, unless otherwise stated. The criteria may be updated in the future to provide more detail on the high level of assurance when experience of its application in Finland is available and when standardised interpretation practices concerning the eIDAS Regulation have been established in Europe.

This document is a guideline. The assessment body must evaluate how well the app corresponds to the criteria provided in this guideline. Risks related to irregularities are assessed as a whole. Operating system and identification app versioning must be monitored and the overall impact of changes to conformity must be assessed. Identification service providers must ensure that the application suppliers provide them adequate and up-to-date information on any changes in hardware and software.

In this context, sensitive data (as referred to in the OWASP criteria) means, for example, personal data, cryptographic materials or confidential/secret information related to identification or registration events.

The guideline is targeted for security evaluation of mobile authentication applications. These applications typically have a strong link to the issuer back-end services. Wallet type of applications with a minimized connections to the back-end can also be evaluated using this guideline.

The criteria is based on the English-language OWASP Mobile AppSec Verification document  ([OWASP Mobile Application Security Verification Standard, MASVS version 1.4.2)](https://github.com/OWASP/owasp-masvs/releases/download/1.1.4/OWASP_Mobile_AppSec_Verification_Standard_1.1.4_Document.pdf), which has been extended and modified for identification purposes.

The testing guide for the original OWASP criteria is available on the OWASP website. The guide contains specific and exhaustive instructions for testing the original OWASP criteria.

Alternative criteria:

* FIDO 3 & 3+ (<https://fidoalliance.org/certification/authenticator-certification-levels/>) ???
* Others?

# Architecture, design and threat modelling

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. All app/wallet components are identified, classified and known to be needed. | LoA, section 2.4.6, point 1  ITSA, section 8.1.4 |  |
| 1. Security controls are never enforced only on the client side, but on the respective remote endpoints. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. A high-level architecture for the mobile app/wallet and all connected remote services has been defined and security has been addressed in that architecture. | LoA, section 2.4.6, point 1  ITSA, section 8.1.4 |  |
| 1. Data considered sensitive in the context of the mobile app/wallet is clearly identified, classified and protection measures documented. | LoA, section 2.4.4, point 1  LoA, section 2.4.6, points 1 and 3 |  |
| 1. All app/wallet components are defined in terms of the business and/or security functions they provide | LoA, section 2.4.6, point 1  ITSA, section 8.1.4 |  |
| 1. A threat model for the mobile app/wallet and the associated remote services has been produced that identifies potential threats and countermeasures. | LoA, section 2.3.1, substantial, point 2  LoA, section 2.3.1, high | Attack potentials are assessed as substantial or high. |
| 1. All security controls have a centralized implementation or | LoA, section 2.4.6, point 1 |  |
| 1. Local security controls are implemented following industry best practises and validated against this criteria. | LoA, section 2.4.6, point 1  M72B subsection 6.1.1 |  |
| 1. There is an explicit policy for how cryptographic keys are managed, and it is based on an internationally approved, up-to-date standard. | LoA, section 2.4.6, point 3  LoA, section 2.4.6, substantial |  |
| 1. The mobile app/wallet reports the operating system, hardware capabilities and application version number to the (application/wallet issuer) server. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. The solution includes a mechanism that ensures that the app is genuine and has not been tampered when presenting authentication/attribute information to a relying party. | LoA 2.3.1, substantial | NOTE: added 19.5.2023 |
| 1. The mobile app/wallet does not support/run on mobile operating system versions that are no longer supported/receiving security updates from the operating system vendor. | ITSA section 8.1.4  M72B, subsection 5.4.d  LoA, section 2.4.6, point 4 | NOTE: added 23.2.2023 |
| 1. A mechanism for enforcing update of the mobile app/wallet exists. | ITSA section 8.1.4  M72B, subsection 5.4.d |  |
| 1. An outdated mobile app/wallet prompts the user to update the operating system and/or mobile app/wallet to complete the transaction or when launcing the app/wallet instance. | (LoA 2.1.1, point 2) | Best practice (BP). LoA 2.1.1 is not incorporated in the Identification Act. |
| 1. Security is addressed within all parts of the software development lifecycle. | LoA 2.4.6, sections 1 and 4  ITSA, section 8.1.4 |  |

# Data storage and privacy

In this context, sensitive data (as referred to in the OWASP criteria) means, for example, personal data, cryptographic materials or confidential/secret information related to identification or registration event.

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. Security services and features offered by the platform are used appropriately to store sensitive data. | LoA 2.4.6, section 1, point 3 |  |
| 1. The level of authentication currently performed is communicated clearly to the user. | LoA, section 2.1.1, point 2 | Recommended practice. |
| 1. No sensitive data should be stored outside of the app /wallet container or system credential storage facilities. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. No sensitive data is written to application logs. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. No sensitive data is shared with third parties unless it is a necessary part of the architecture. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. The keyboard cache is disabled on text inputs that process sensitive data. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. No sensitive or secret data, such as passwords or pins is exposed through the user interface. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. The clipboard is deactivated on text fields that may contain sensitive data. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. No sensitive data is exposed via IPC mechanisms. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. No authentication secrets are stored or transferred outside of the app storage facilities. | LoA 2.4.6, low, section 3  LoA, section 2.4.6, substantial  M72B, subsection 5.4.b |  |
| 1. The app/wallet removes sensitive data from views when moved to the background. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. The app/wallet does not hold sensitive data in memory longer than necessary, and memory is cleared explicitly after use. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. The app/wallet recommends enabling a minimum device-access-security policy (PIN code or biometric unlocking mechanism of mobile device and similar features) to the end user. | LoA, section 2.1.1, point 2 | Recommended practice. |
| 1. The app educates the user about best practices the user should follow in processing personally identifiable information. | LoA, section 2.1.1, point 2 | Recommended practice. |
| 1. No sensitive data should be stored locally on the mobile device. Instead, data should be retrieved from a remote end point when needed and only be kept in memory. | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b |  |
| 1. If sensitive data is still required to be stored locally, it must be encrypted using a key derived from hardware backed storage which requires the use of an identification factor(s). | LoA, section 2.4.6, point 1  M72B, subsection 5.4.b | Principle of minimizing the need to store sensitive data. A wallet -type of application stores sensitive data, so this criteria should be used for wallet -type of applications. |
| 1. The app/wallet must be deacivated after five failed authentication attempts (of the identification factor). | M72B, subsection 6.1.2 | To re-enable the app, normal issuance/activation process must be followed |
| 1. If the retry count cannot be communicated to the server side, the app/wallet must have adequate protection in place for the local retry counter. | LoA, section 2.3.1, substantial point 2  M72B subsection 5.3.e-f |  |

# Cryptography requirements

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. The app/wallet does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption. | M72B subsection 5.3.g M72B, section 7 |  |
| 1. The app/wallet uses proven cryptographic primitives that are appropriate for the particular use-case and compliant with regulation.. | M72B subsection 5.3.g) |  |
| 1. The app/wallet does not use cryptographic protocols or algorithms that have expired or are widely considered depreciated for security purposes. | M72B subsection 5.3.g)  M72B, section 7 |  |
| 1. The cryptographic primitives are configured according to best practises or based on regulatory requirements (if they exist). | LoA, section 2.4.6, point 2  M72B, subsection 7.1 |  |
| 1. The app/wallet doesn't re-use the same cryptographic key for multiple purposes. | LoA, section 2.4.6, point 1  ITSA, section 8.1.4 |  |
| 1. All random values are generated using a sufficiently secure and high-quality random number generator. | LoA, section 2.4.6, point 1  ITSA, section 8.1.4 |  |
| 1. The app/wallet uses a signature counter to enable the server-side detection of app cloning attempts. | LoA, section 2.3.1, substantial, point 2  LoA, section 2.3.1, high |  |
| 1. The app/wallet does not include or use any hardcoded usernames or passwords. | LoA, section 2.4.6, point 1  LoA, section 2.3.1, point 2  M72B section 6 | Development time credentials (if any) must be cleaned from production version. No hard coded credentials/secrets to allow vendor access.  Possible activation and PUK-codes are valid for only one-time use, and only for a predetermined period of time. |
| 1. Weaker cryptographic protocols, identifications or certificates used during development (if any) are removed from the production version. | LoA, section 2.4.6, points 1 and 3  LoA, section 2.4.6, high  M72B, subsection 5.3.g  M72B, section 7 |  |

# Authentication, characteristics of the authentication method; session management

This chapter employs the OWASP standard and chapter 4 where applicable. Additional criteria relating to the characteristics of the authentication method are also provided.

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. The procedure used for the personalisation of the app/wallet at registration phase ensures that the app is linked to the holder of the identification means. | LoA, section 1 (definitions), point 2  LoA, section 2.2.1, substantial, point 2 |  |
| 1. The secret used for implementing the identification is protected against unauthorised use and can only be accessed using a predefined, secure method. | LoA, section 2.4.6, point 3  LoA, section 2.4.6, substantial  M72B, subsection 6.4.2 | Example: private key. |
| 1. Secrets/identification keys are unique. | M72B, subsection 5.3.g |  |
| 1. Asymmetric secrets that implement the identification are created in the mobile device (key pair, other secret key/secret). | M72B, subsection 5.3.g M72B, subsection 5.4.b | Cf. RTS. |
| 1. If secrets used to implement the identification are created outside the device, they are provisioned to the device using a secure method. | LoA, section 2.4.6, point 2  LoA, section 2.4.6, substantial  M72B, subsection 5.4.b | Cf. RTS. |
| 1. If secrets used to implement the identification are created outside of the device and provisioned to the device using a secure method, the link between the secret and the PID (person/holder) is done on the device and only during the registration phase. | LoA, section 2.3.1, point 2  LoA, section 2.2.1, substantial point 2  M72B, subsection 6.3 |  |
| 1. Identification may not be based on a shared secret alone. | LoA, section 2.2.1, substantial, point 2 |  |
| 1. App initialisation binds the secrets into the mobile device so that the secrets cannot be copied and used in another device or transferred to another device or a backup system so that the secrets could be used in the other device. | LoA, section 2.2.1, substantial, point 2  M72B, subsection 6.4.2 |  |
| 1. The app/wallet implements device binding using a device fingerprint derived from multiple properties unique to the device. | LoA, section 2.3.1, low point 3, substantial point 2  M72B, subsection 6.1 |  |
| 1. The app/wallet does not store identification information/credentials (passwords, pins, usernames, etc) persistently at any point. | LoA, section 2.2.1, substantial, point 2  LoA, section 2.2.1, high, point 2  LoA, section 2.3.1, substantial, point 2  LoA, section 2.3.1, high, point 2  LoA, section 2.4.6, point 3 |  |
| 1. The app/wallet enables pseudonymous authentication | M72B, subsection 12.3  (GDPR art 32) | NOTE: added 30.5. For wallet - type of applications or for privacy preserving scenarios |
| 1. If the app/wallet is able to store attributes provisioned from a third party or generated by the user, the app/wallet stores them securely. | LoA, section 2.4.6, points 1-2  M72B, subsection 6.1 and 9.1.1 | NOTE: added 30.5. For wallet -type of applications |
| 1. If the app/wallet allows for third party attributes to be added, the attributes are provisioned using a secure protocol and a secure presentation format. | LoA, section 2.4.6, points 1-2  M72B, subsection 6.1 and 9.1.1 | NOTE: added 30.5. For wallet -type of applications |
| 1. The app/wallet that stores attributes locally and secures the confidentiality and integrity of the attributes using a secure element | LoA, section 2.4.6, points 1-2 | NOTE: added 30.5. Either in the secure element itself or using a key protected by the/in the secure element. |
| 1. If the app/wallet is used to present attributes directly to the relying party, the app/wallet implements both the transport and presentation using a secure protocol and a privacy preserving presentation and secure format. | LoA, section 2.4.6, points 1-2  M72B, subsection 6.1 and 9.1.1 | NOTE: added 30.5. wallet type of applications. |
| 1. If the app/wallet allows the user to present attributes directly to the relying party, the app/wallet must verify from a trusted source that the relying party is authorized to receive these attributes. | [eIDAS2]  LoA, 2.4.6, low point 3 | NOTE: added 30.5. Wallet -type of applications. |
| 1. If the app/wallet detects that the relying party is asking for information that it is not entitled to, the app clearly warns the end user for sharing of the attributes that are out-of-scope for the relying party. | [eIDAS2]  LoA, 2.4.6, low point 3 | NOTE: 30.5. Wallet -type of application |
| 1. If the app/wallet sends messages that are validated on the server and lead to identification, the messages must be sent securely using up-to-date and approved cryptographic protocols (such as Mutual/2-way TLS 1.2 or later). | LoA, section 2.4.6, point 2  M72B, subsection 5.3.g M72B, subsection 7.1.1, subsections 1-4 |  |
| 1. If personal information is exchanged between the app/wallet and the server, the information is protected using message-level encryption. | LoA, section 2.4.6, point 2  LoA, section 2.4.6, substantial  M72B, subsection 5.3.g |  |
| 1. If the app/wallet is based on or includes a method based on one-time passwords (OTP), the one-time passwords are generated using recommended, standard-based solutions. | M72B, subsection 5.3.g |  |
| 1. The secret used for the identification is stored using services offered by the platform on a hardware based secure environment | M72B, subsection 5.3.c M72B, subsection 5.4.b | Secure element, Trusted execution environment etc. |
| 1. Notice of invalid input is sent to the server separately after each occurrence. The server monitors the number of invalid inputs and locks automatically after X invalid attempts. If no network connection is available and the messages cannot be transmitted to the server securely, the app/wallet must follow the same logic (PSD2, the 5-error rule). | LoA, section 2.4.6, point 1  M72B, subsection 5.3.f | Cf. RTS and SCA. |
| 1. Techniques that prevent replay attacks are used between the app/wallet and the server. In case of a cryptographic nonce: Bounded Probability of a Birthday Collision | LoA, section 2.3.1, substantial, point 2  LoA, section 2.3.1, high |  |
| 1. If session identifiers are used, the session identifiers are generated randomly. | LoA, section 2.3.1, substantial, point 2  LoA, section 2.3.1, high |  |
| 1. (Software/OAuth) If token-based authentication is used, the server provides a token that has been signed using an acceptable and secure algorithm. | LoA, section 2.4.6, point 2  M72B, subsection 7.1.1, paragraph 2 |  |
| 1. Session or token validity is defined on the server side. | LoA, section 2.4.6, points 1 and 4 |  |
| 1. Authorisation policies used to grant access to the target application or service are defined on the (identification) server side. | LoA, section 2.4.6, points 1 and 4 |  |
| 1. If persons registered on the mobile device cannot be distinguished in the implementation of the authentication factor due to the platform properties, a combination that can reliably distinguish between the users is used (such as: mobile device = control, PIN code related to secret = information and fingerprint = property). | LoA, section 2.2.1, substantial, point 1 | Example: Apple iOS, biometry.  Strong identification means does not require all three factors. Two is enough if the independence of the authentication factors can be ensured and they have been bound to the holder of the identification means. |
| 1. If a biometric authentication factor is used and persons registered on a mobile device cannot be distinguished due to the platform properties, the user must be provided with clear instructions on how to remove the biometric identifications/secrets of other persons that belong to other users of the mobile device. | LoA, section 2.2.1, substantial, point 1  LoA, section 2.1.1, point 2  LoA, section 1 (definitions), point 2 | LoA, section 2.1.1 Outside the scope of the Identification Act but recommended practice. |
| 1. If the app/wallet permits adding new, complementary authentication factors or changing the authentication factor, this information is also communicated to the server side. Changing and adding a factor always requires identification on a level at least equal to the level that the new combination would issue identification on. The combinations must be documented and assessed separately. | LoA, section 1 (definitions), point 2  LoA, section 2.2.1, substantial, point 2  LoA, section 2.2.4, substantial | The independence of the authentication factors must be ensured. This means, for example, changing the category of one authentication factor or adding a new category, which would result in authentication factors from three categories becoming available.  The intention is to allow the user to choose authentication factors, but at the same time to ensure that the identification service can guarantee their security at all times. |
| 1. In strong multi-factor authentication, a factor based on information possessed by the user (password, pin) or a physical property of the user (fingerprint, face recognition, iris) is used to unlock the secret that is used to respond to the actual identification request. | LoA, section 1 (definitions), point 3  LoA, section 2.2.1, substantial, point 2  LoA, section 2.3.1, substantial, point 2 |  |
| 1. The implementation of a biometric authentication factor only uses interfaces offered by the platform. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. When a biometric factor is used, the biometric record or the template (fingerprint, facial recognition data, iris scan data, etc.) is not transferred outside the app/wallet during the identification event. | LoA, section 2.2.1, substantial, point 2  LoA, section 2.3.1, substantial, point 2 |  |
| 1. Sensitive information or personally identifiable information used at the registration phase can only be transferred to the server side using secure methods. | LoA, section 2.4.6, point 2 |  |
| 1. The user has the option to temporarily close the secret on a) one device/instance, b) multiple devices/instances and c) all devices/instances at once. | LoA, section 2.2.3, substantial, point 1 |  |
| 1. Opening a secret that is closed temporarily always requires identification on a level equal or higher to the identification that would be required for activating the app. | LoA, section 2.2.3, substantial, point 3 |  |
| 1. The user must have an option to securely deactivate the identification app and secret on a) one device/instance, b) multiple devices/instances and c) all devices/instances. | LoA, section 2.2.3, substantial, points 1 and 2 |  |
| 1. Temporary, device-specific closing and removal of a secret must also be possible on the (issuer) server side. | LoA, section 2.2.3, substantial, points 1 and 2 |  |
| 1. The identification is bound to the desired transaction or browser session; in other words, the identification app must clearly display information about the action that is being done. | LoA, section 2.3.1, substantial, point 2 | E.g. RTS, dynamic linking. EU 2018/389  PSD2 regulation lays down more specific requirements for dynamic linking. These requirements must be met if the identification app is used for both general-purpose identification and identification for payment purposes. |
| 1. The identification app/wallet implements a binding message which enables the user to link the identification in the mobile device to a browser session, for example, in understandable terms. | LoA, section 2.3.1, substantial, point 2, M72B, section 6.2.1 | Use language that can help the user to understand what a session binding message is. |
| 1. The identification app/wallet always displays the name of the service/application the user is authenticating to based on the attribute sp\_name. This information must be visible and easy to understand by the user. | M72B, section 6.2.2 | The language must be clear and not to be confused with the session binding message. |
| 1. If the response of the identification app/wallet is based on an asymmetrical signature, the WYSIWYS principle is followed (the information displayed to the user is the information that is being signed). | LoA, section 2.3.1, substantial, point 2 |  |
| 1. The app/wallet guides the user to select strong PIN codes. | LoA, section 2.1.1, substantial, point 2  M72B, subsection 5.3.g | LoA 2.1.1 is outside the scope of the Identification Act but is recommended practice. |
| 1. The app/wallet does not accept PIN codes or other secrets based on the user's memory that are easily guessed. | LoA, section 2.3.1, substantial, point 2  LoA, section 2.4.6, point 1 | For example, the app does not accept PIN codes that are known to be weak or easily guessed (e.g. 999999, 123456, 999999). |
| 1. User inputs, such as PIN codes, are validated in secure manner. | LoA, section 2.3.1, substantial, point 2  M72B, subsection 5.4.b |  |
| 1. The app/wallet uses hardware-level security features of the mobile device such as TEE/SE and similar, the app indicates the hardware-level component that is used and makes other details available to the (issuer) server in connection with initialisation so that the server can detect and respond to hardware-level vulnerabilities (also in the future). | LoA, section 2.4.6, point 1 and 4  M72B, subsection 5.4.d | CVE-2018-11976 🡪 Providing the server with an opportunity to react to known vulnerabilities in hardware-level components. |
| 1. If the backend or the relying party detects a non-genuine app/wallet, the identification flow must be stopped. I.e. app/wallet attestation must be implemented on the app itself and the attestation validated, when applicable, before proceeding with the identification request. | LoA, section 2.4.6, points 1 and 3  LoA, section 2.3.1, substantial point 1 | NOTE:added 19.05.2023 |
| 1. The app /wallet and/or the back-end ensures that there can not be simultaneous active authentication requests, i.e. previous requests must be invalidated/closed before initiating a new request. | LoA, section 2.3.1, substantial point 2 |  |

# Data communication

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. The network traffic between the app/wallet and the server is protected using internationally or nationally recommended connection procedures. The secure channel is used consistently throughout the app/wallet. | LoA, section 2.4.6, point 2  M72B, subsection 5.3.g | No encryption requirements have been set for the identification scheme's *internal* connections, but the data communication encryption policies defined in M72A, section 7 for use *between the parties* should be taken as the starting point. |
| 1. The app/wallet checks that the TLS (or similar) settings/configuration are in line with current best practices. | LoA, section 2.4.6, point 2  M72B, subsection 5.3.g , subsection 7.1.3, and 7.2 | No encryption requirements have been set for the identification scheme's *internal* connections, but the data communication encryption policies defined in M72A, section 7 for use *between the parties* should be taken as the starting point. |
| 1. The app/wallet pins the endpoint certificate or public key, and subsequently does not establish connections with endpoints that offer a different certificate or key, even if signed by a trusted CA. | LoA, section 2.4.6, point 2 |  |
| 1. The app/wallet does not rely on a single insecure communication channel (email or SMS) for critical operations, such as enrollments and generation of the user secret. | LoA, section 1 (definitions), point 2  LoA, section 2.2.1, substantial, point 2 | In practice, the personalisation of the application must be based on a strong means of electronic identification. |
| 1. The app/wallet only depends on up-to-date connectivity and security libraries. | LoA 2.4.6, sections 1 and 4 |  |

# Platform interaction

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. The app/wallet only requests the minimum set of permissions necessary. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. All inputs form external sources are validated and sanitized. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.c |  |
| 1. The app/wallet does not export data via custom URL schemes or IPC mechanisms | LoA, section 2.4.6, point 2  M72B, subsection 5.3.c |  |
| 1. If the app/wallet needs to display content via a browser (e.g. method selection in the identification server), the operating system's secure features (See OS vendor current best practises) should be used primarily. WebView is used only if more secure alternatives are not available. The components used are configured to allow only the minimum set of protocol handlers required. Other connection policies are blocked/confirmed as being disabled. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. JavaScript is disabled in browser components by default. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. If browser components are used, they are configured to allow only https | LoA, section 2.4.6, point 1  M72B, subsection 7.1-2 and 9.3 |  |
| 1. Native methods are blocked in case the platform's software version has been found vulnerable. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c and 5.4.d) | JavaScript implementations on old versions of the Android operating system, for example, may be insecure. |
| 1. If native methods of the app/wallet are exposed to browser components, verify that the browser component only renders JavaScript contained within the app package. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c ) |  |
| 1. Browser components cannot access / are blocked from local resources. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. Object deserialization, if any, is implemented using safe serialization APIs. | LoA, section 2.4.6, points 1 and 3  LoA, section 2.4.6, substantial  M72B, subsection 5.3.c |  |
| 1. The app/wallet protects itself against screen overlay attacks. | LoA, section 2.4.6, points 1 |  |
| 1. The browser component cache, storage, and loaded resources must be cleared before the browser component is destroyed | LoA, section 2.4.6, points 1 and 3  M72B, subsection 5.4.b |  |
| 1. Verify that the app/wallet prevents usage of third-party keyboards whenever sensitive data is entered. | LoA, section 2.4.6, points 1-2 |  |

# Code security, quality and development environment

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. The app/wallet is signed and provisioned with a valid, trusted certificate and the private key is properly protected | LoA, section 2.4.6, point 1 |  |
| 1. The app/wallet has been built in release mode (e.g. non-debuggable). | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. App/wallet development only uses tested and recommended software development/coding data security policies. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c | All JavaScript components, for example, must be encoded and sanitised to reduce the risk of XSS attacks. |
| 1. Debugging symbols have been removed from native binaries. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. Debugging code and messages has been removed. | LoA, section 2.4.6, point 1  M72B, subsection 5.3 |  |
| 1. Testing or development time settings, verbose logging and configurations have been removed from the release version. | LoA, section 2.4.6, points 1 and 4  M72B, subsection 5.3.c and 5.4.d |  |
| 1. All third party components used by the mobile app/wallet are identified, and checked for known vulnerabilities regularly. | LoA, section 2.4.6, point 4  M72B, subsection 5.4.d |  |
| 1. The app/wallet catches and handles possible exceptions. | LoA, section 2.4.6, point 4  M72B, subsections 5.3.f and 5.4.d) |  |
| 1. The app/wallet or the server minimises the information contained in error messages. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. Error handling logic in security controls denies access by default. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. Memory is allocated, freed and used securely. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. The data security features of the platform / development environment are activated. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |

# Security controls and resilience

| **Criterion** | **Justification** | **Additional information / comment** |
| --- | --- | --- |
| 1. The app/wallet implements multiple defence mechanisms defined in this chapter. | LoA, section 2.4.6, point 1 | The application's capacity to withstand attacks must be assessed as a whole. |
| 1. The app/wallet has more than one feature that attempts to detect the presence of a rooted or jailbroken device. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.f |  |
| 1. The detection mechanisms trigger responses of different types, including delayed and stealthy responses. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.f and 6.1 |  |
| 1. The app/wallet sends a message to the server-side implementation upon detection of a rooted/jailbroken device platform, or the app has the ability to decide what to do upon detection of a rooted/jailbroken platform. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.f |  |
| 1. The app/wallet prevents debugging and detects, and responds to, a debugger being attached. All available debugging protocols must be covered. | LoA, section 2.4.6, point 1  M72B, subsection 5.3.c |  |
| 1. The app/wallet detects, and responds to, tampering with executable files and critical data/files within its own sandbox. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.f |  |
| 1. The app/wallet detects, and responds to, the presence of widely used reverse engineering tools on the device. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.f |  |
| 1. The app/wallet detects, and responds to, being run in an emulator. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.f |  |
| 1. The app/wallet detects, and responds to, tampering the code and data in its own memory space. | LoA, section 2.4.6, point 4  M72B, subsection 5.3.f |  |
| 1. Partitions that are important or critical to the app/wallet are encrypted where applicable on the system level. Analysis cannot be used to identify partitions that are important or critical to the app/wallet. | LoA, section 2.4.6, points 1 and 3  LoA, section 2.4.6, substantial  M72B, subsection 5.4.b M72B, subsection 5.3.c |  |
| 1. Application level payload encryption is applied | LoA, section 2.4.6, points 1-4  M72B, subsection 5.3.g |  |

# References

The criteria used as justification for this guideline:

ITSA - Act on Strong Electronic Identification and Electronic Trust Services 617/2009

LoA - Commission implementing regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

M72B - Regulation on Electronic Identification and Trust Services (M72B/2022) <https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision/electronic-identification>

OWASP - OWASP Mobile Application Security Verification Standard, MASVS version 1.4.2