EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL

Ensuring High Assurance of EUDI Wallets
& the NL National eID Scheme

NL-P-03

NL EUDI Wallet Certification System

Secure Software Development and Vulnerability Management Practices for Wallet and PID Providers

RC1.0

2026.11.01

Document reference	NL-P-03
Version	RC1.0
Status	Release Candidate Draft
Date	01/11/2026
Document type	Secure Software Development and Vulnerability Management Practices
Parent framework	NL-SYS-01 NL-P-P/W
Scheme Owner	Kingdom of the Netherlands Minister of Economic Affairs
Certification target	Wallet Providers and PID Providers under the NL EUDI Wallet Certification System
Primary audience	Wallet Providers, PID Providers, CABs and Scheme Owners
Secondary audience	Supervisory bodies, accreditation bodies and EUDI Wallet ecosystem stakeholders
Assurance level <identity proofing CIR 2015/1502> and <evaluation, EU Regulation 2019/881>	High/High
Related Documents	NL-P-02 NL-P-03 NL-P-P/W04*

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Version	**RC1.0**	State	Date
RC1.0	Transmission of working doc into Certification System Template	Release Candidate	2026-10-31

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

1 Introduction

1.1 Foreword

European Digital Identity Wallets form part of a cross-border trust infrastructure in which software defects, compromised dependencies and unremediated vulnerabilities can affect not only an individual wallet unit, but also Wallet Providers, PID Providers, relying parties and confidence in the national electronic identification scheme.

Secure software development, secure maintenance and effective vulnerability management are therefore continuing assurance conditions throughout the lifecycle of the wallet solution and the services on which it depends.

This document translates that lifecycle perspective into requirements and guidance for Wallet Providers and PID Providers operating under the NL EUDI Wallet Certification System. It complements the certification and governance framework established by NL-SYS-01 by defining practices for product cybersecurity risk management, secure development and maintenance, third-party component governance, verification and validation, monitoring, coordinated vulnerability disclosure, remediation, security updates and secure decommissioning.

The document is informed by Regulation (EU) No 910/2014 as amended by Regulation (EU) 2024/1183, Directive (EU) 2022/2555 (NIS2), Regulation (EU) 2024/2847 (Cyber Resilience Act), the applicable EUDI Wallet implementing acts and relevant standards. References to the Cyber Resilience Act express alignment with its lifecycle and vulnerability-handling principles. They do not, by themselves, determine whether a specific wallet component, provider or service falls within the legal scope of that Regulation.

The requirements are intended to support consistent implementation and assessable evidence while avoiding duplication with applicable product, organisational or service certification. They shall be read together with NL-SYS-01 and the applicable Wallet Provider and PID Provider certification schemes.

1.2 Scope

This document specifies lifecycle requirements and supporting guidance for secure software development, secure maintenance and vulnerability management by Wallet Providers and PID Providers within the NL EUDI Wallet Certification System.

It applies to the software and related processes used to develop, build, test, release, operate, maintain and decommission EUDI Wallet mobile applications and the Remote Data Processing Solutions (RDPS), interfaces, build and distribution services, and third-party components on which those applications depend.

The requirements cover product cybersecurity risk management; cybersecurity planning and requirements; architecture and design; secure implementation; technical documentation and software bills of materials; verification and validation; secure production and distribution; monitoring and issue management; third-party component management; coordinated vulnerability disclosure; remediation; security updates; and secure decommissioning. They

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

apply throughout the support period and shall be revisited when the product, its dependencies, its operational environment, the threat landscape or applicable legal and technical requirements change.

For the purposes of this document, secure maintenance includes the controlled modification of software and dependencies, continued verification of security controls, monitoring for newly disclosed vulnerabilities, risk-based remediation, release of security updates and communication of residual risks. Vulnerability management includes intake, triage, risk evaluation, coordination, disclosure, remediation, testing, release and post-release monitoring.

This document does not replace the functional, organisational or product-security requirements contained in the applicable EUDI Wallet legislation, implementing acts, EU cybersecurity certification schemes or NL certification schemes. Nor does it establish whether Regulation (EU) 2024/2847 or national NIS2 legislation applies to a particular provider or product. Where such legislation applies, its mandatory provisions prevail.

This document also does not prescribe all security properties of the wallet solution itself; those properties remain governed by the applicable certification requirements, architecture, risk assessment and technical specifications.

2 Legal Basis & References

2.1 Legal Basis

The legal basis for these requirements is formed by the Union and applicable national legislation governing European Digital Identity Wallets, electronic identification, cybersecurity risk management and incident reporting.

The following instruments are particularly relevant:

- Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, establishing the European Digital Identity Framework.
- Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act (CRA), including essential cybersecurity and vulnerability-handling requirements throughout the product lifecycle.
- Commission Implementing Regulation (EU) 2024/2690, where the provider or certified service falls within its scope or where its technical and methodological requirements are adopted by the applicable national framework.
- Commission Implementing Regulation (EU) 2015/1502 concerning assurance levels for electronic identification means, including assurance level High.

Where national transposition or sector-specific rules impose more specific or stricter requirements, those requirements prevail. The applicant shall identify the competent authority, applicable reporting obligations and any sector-specific cybersecurity requirements relevant to its certified services.

2.2 Normative references

The following documents contain provisions which, through reference in this document, constitute requirements or criteria for its application. The latest applicable version adopted by the NL EUDI Wallet Certification System shall be used unless a specific version is stated:

- ISO/IEC 17065, Conformity assessment — Requirements for bodies certifying products, processes and services.
- ISO/IEC 17067, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes.
- ISO/IEC 27001, Information security management systems — Requirements.
- ISO/IEC 27002, Information security controls.
- ISO/IEC 27005, Guidance on managing information security risks.

1.1 Parent & Related Documents

This document is a subsidiary requirements specification within the NL EUDI Wallet Certification System and shall be applied in conjunction with:

- NL-SYS-01, NL EUDI Wallet Certification System framework.

- NL-SYS-02 and the other applicable NL-SYS system documents governing terminology, governance, scheme ownership, accreditation, authorisation and system operation.

- NL-P-P/ W, PID Provider & Wallet Provider Certification Schemes.
- NL-P-01, Organisational and security requirements for Wallet Providers and PID Providers.
- NL-P-02, Resilience Requirements for Wallet and PID Providers

2.3 Informative references

The following documents provide supporting context and guidance. Informative references do not create additional certification requirements unless a normative requirement expressly incorporates them:

- European Digital Identity Wallet Architecture and Reference Framework.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

3 Relationships with NIS2, CRA

3.1 Relationship with NIS2

Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, establishes the legal and trust framework for European Digital Identity Wallets and requires wallet solutions to satisfy applicable functional, security and certification requirements. Within the NL EUDI Wallet Certification System, NL-SYS-01 organises how the wallet and the electronic identification scheme under which it is provided are brought together through interrelated conformity assessments and continuing certification controls.

Directive (EU) 2022/2555 (NIS2) addresses cybersecurity at entity and service level. Where a Wallet Provider, PID Provider or a supporting service falls within its scope as transposed into national law, the entity is required to implement proportionate cybersecurity risk-management measures and comply with the applicable incident-reporting obligations. Article 21 of NIS2 expressly includes supply-chain security, security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure, policies and procedures to assess the effectiveness of cybersecurity risk-management measures, and the use of cryptography and encryption.

The eIDAS and NIS2 frameworks are therefore complementary rather than interchangeable. eIDAS and its implementing acts establish wallet-specific trust, functionality, security and certification outcomes. NIS2 establishes entity-level governance, risk management, supply-chain, business-continuity and incident-reporting duties where applicable. Secure software development, secure maintenance and vulnerability management provide the operational link between those layers by ensuring that certified wallet-related services continue to manage software and dependency risks after initial development and certification.

The requirements in this document support that link by requiring traceable cybersecurity planning, secure design and implementation, controlled development environments, component inventories and SBOMs, recurring verification and validation, monitoring of vulnerabilities and incidents, coordinated disclosure, risk-based remediation, security updates and post-release review. Evidence generated through these activities may support both continued certification under the NL system and demonstration of relevant NIS2 controls, but conformity with this document does not by itself establish full compliance with NIS2 or national implementing legislation.

3.2 Relationship with CRA

Regulation (EU) 2024/2847, the Cyber Resilience Act (CRA), establishes horizontal cybersecurity requirements for products with digital elements. Its subject matter includes essential cybersecurity requirements for the design, development and production of such products and essential requirements for the vulnerability-handling processes maintained during the period in which the product is expected to be in use. The CRA therefore expresses a lifecycle model in which security is designed into the product, maintained after release and supported by effective vulnerability handling and security updates.

An EUDI Wallet solution comprises software with security-critical functions and may depend on mobile applications, wallet secure cryptographic applications or devices, backend RDPS,

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

interfaces, build and signing infrastructure, software libraries and distribution platforms. A weakness in any of these elements can affect wallet integrity, confidentiality, availability, authenticity, sole control by the user, protection of person identification data or trust in the electronic identification scheme. For that reason, CRA-aligned secure-development and vulnerability-handling practices are directly relevant to the EUDI Wallet assurance context, even where the legal applicability or classification of a particular component under the CRA must be determined separately.

This document adopts the CRA's lifecycle logic as a state-of-the-art baseline for the NL EUDI Wallet Certification System. It requires product-context and risk documentation; security requirements and architecture; secure implementation and development environments; component and dependency inventories, including SBOMs; verification and validation; protection of build, signing and distribution processes; monitoring throughout the support period; coordinated vulnerability disclosure; risk-based remediation; testing and release of security updates; and secure decommissioning.

In the EUDI Wallet context, these practices also support continued conformity after initial certification. Changes to wallet software, RDPS, third-party components, cryptographic mechanisms, supported mobile platforms or the threat landscape can invalidate assumptions on which certification evidence was based. The resulting change, vulnerability and remediation records shall therefore feed the applicable surveillance, change-notification, incident-management and certificate-maintenance processes defined by NL-SYS-01 and the relevant Wallet Provider, PID Provider and product certification schemes.

Alignment with the CRA is not intended to create a parallel certification route or to treat CRA conformity as a substitute for EUDI Wallet certification. The applicable eIDAS requirements, implementing acts, EU cybersecurity certification requirements and NL scheme rules remain authoritative for the certification target. Conversely, certification under the NL EUDI Wallet Certification System does not automatically demonstrate CRA conformity where the CRA applies; the responsible economic operator must separately establish the applicable CRA obligations, conformity-assessment route, technical documentation, reporting duties and market-surveillance requirements.

The technical content of this document draws on the standardisation work supporting the CRA, in particular the draft CEN/CENELEC JTC 13/WG 9 work on product cybersecurity risk management, the product lifecycle and vulnerability handling. It also considers the draft CEN/CENELEC TC 224/WG 17 work relevant to identity-management and access-control products.

Mandatory requirements and non-mandatory guidance are distinguished throughout this document. Requirements apply to the relevant provider or manufacturer within the scope assigned by the applicable certification scheme. Guidance explains recognised implementation approaches but does not create an additional obligation unless incorporated by a normative requirement or by another applicable legal or scheme provision.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

4 Product Cybersecurity Risk Management

4.1 Introduction

Risk management is a continuous activity that spans the entire product lifecycle -from design and development through production, maintenance, and decommissioning - ensuring cybersecurity remains appropriate for the product's intended purpose and foreseeable use. Changes in circumstances, such as significant design modifications or shifts in the threat landscape, may necessitate revisiting risk management activities, particularly risk assessments, to keep residual risk within accepted bounds.

The risk management process consists of six interconnected activities: establishing the product context, defining risk acceptance criteria, risk assessment (encompassing asset identification, risk analysis, risk evaluation and acceptance), treating identified risks, communicating residual risks, and ongoing monitoring and review. These activities will be laid out in the following sub clauses.

See OpenCRE 307-242 at opencre.org/cre/307-242 for related resources and topics for guidance.

4.2 Product Context Documentation

Introduction

Establishing the product context is the foundational step for identifying and treating cybersecurity risks associated with a product. It is an iterative activity that needs to be revisited whenever the product or its environment changes throughout the product lifecycle.

The product context encompasses several interrelated elements: the intended purpose and reasonably foreseeable use, the product's functions, its operational environment, an architectural overview of its components and interfaces, any Remote Data Processing Solutions (RDPS), a description of its users, and an overview of how cybersecurity functions are distributed across the product and its environment. Together, these elements define the scope within which risks are identified, assessed, and treated.

Output: documentation containing the product context.

Requirements

Requirement CR-ID: 5.2-CR-01

The product context shall be identified and documented, covering the product's intended purpose and reasonably foreseeable use (IPRFU), its functions, its operational environment, an architectural overview, a description of its users including their experience level and security-relevant objectives, and where relevant and useful: general product insights from the market segments involved, including market expectations.

Source: RMA-01-RQ-01, Input clause (40000-1-2 6.2)

Guidance

- **IPRFU**: Document the conditions of use for which the product is designed, including scenarios that are not intended but can reasonably be foreseen. Consider accessibility, including the use of Assistive Technology, as part of this scope.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- **Product functions**: Include both functional features and cybersecurity-specific features (e.g., functions that protect the product or safeguard user health and safety), as well as any configuration capabilities.
- **Operational environment**: Describe the networks, systems, and physical setting in which the product will be used or could reasonably be expected to be used. Characterize the applicable physical and logical access levels (for example public, restricted, or controlled). External systems and people capable of influencing the product's functions should also be treated as part of this operational environment.
- **Architecture overview**: Provide a high-level overview of the product's key components, interfaces, and dependencies. Highlight how integrated components introduce cybersecurity risks and what cybersecurity features they provide or require. Where RDPS is present, describe its role in delivering product functions.
- **User description**: Classify users according to their expected level of experience and capability - for example, as vulnerable, ordinary, instructed, or skilled users - and identify their security-relevant objectives (e.g., data confidentiality, protection against fraud, health and safety). Note that a single product may serve multiple user groups in different contexts.
- **Distribution of cybersecurity functions**: Record which security functions the product supplies for its own use, which ones it instead relies on the environment to provide, and which ones it offers for other products to use. This is not a one-time exercise - since adding a control to the product can itself alter the product context, it may need to be revisited.

Requirement CR-ID: 5.2-CR-02

Where the product includes remote data processing solutions (RDPS), the RDPS shall be considered to be included in the product context.

Source: RMA-01-RQ-02 (40000-1-2)

Guidance

- The operational environment description should include connectivity characteristics, expected availability, data handled, and expected uptime constraints relevant to the RDPS.
- Where relevant, RDPS should be reflected consistently across all product context elements, including IPRFU, functions, architecture, and user description.

Requirement CR-ID: 5.2-CR-03

A documented procedure shall be maintained for establishing and updating the product context, including defined triggers for re-evaluation when the application, its RDPS, or its operational environment changes.

Source: SOTA

Guidance

Triggers for re-evaluation may include: release of a new application version, changes to backend RDPS infrastructure, changes to third-party SDK or library dependencies, changes to target platform (iOS/Android OS version), changes to data processing scope, or changes to the intended user population. The procedure should define roles responsible for initiating and approving product context updates and should reference the output artefacts (e.g., product context document, architecture overview) that need to be revised.

4.3 Risk Acceptance Criteria

Introduction

Risk acceptance criteria establish the threshold at which identified risks are considered tolerable, either without further treatment or after mitigation measures have been applied. These criteria reflect the product context and are typically defined at the beginning of the risk assessment process, although they may need to be reviewed and updated as the threat landscape, state of the art, or product lifecycle changes.

Output: Documented risk acceptance criteria for the product's cybersecurity.

Requirements

Requirement CR-ID: 5.3-CR-01

The cybersecurity risk acceptance criteria shall be established. At minimum, the criteria shall account for the product context, regulatory factors, supply chain aspects, the nature of risks, the current state of the art, and user needs.

Source: RMA-02-RQ-01 (40000-1-2) and corresponding assessment criteria (user needs)

Guidance

Several factors commonly inform these criteria:

- the product's intended purpose and reasonably foreseeable use;
- applicable regulatory requirements;
- supply chain considerations including contractual agreements, downstream integrators, and reasonable user expectations;
- operational environment characteristics;
- the scale of deployment - a risk acceptable for a single product instance may become unacceptable when aggregated across a large installed base;
- how severe the impact would be and how likely the risk and any consequences it brings are to occur;
- nature of the risks, such as the health and safety of individuals affected;
- user needs;
- and the user population's capacity to further mitigate residual risk.

In some circumstances, deviation from established criteria may be justified - for instance, when a user explicitly accepts certain risks through contractual agreement. Where residual risk is transferred, clear communication to relevant parties is essential.

Risk acceptance criteria are not static - they should be reviewed and updated when relevant circumstances change, such as shifts in the threat landscape, changes in applicable legislation, or transitions in the product or component lifecycle (e.g., obsolescence or deprecation). When defining criteria, consider that some risks may be inherently necessary for the product to function; such risks may be acceptable under the criteria provided the product context and relevant communication are accounted for.

Aggregated risk from large mobile install bases can transform individually low-severity risks into systemic threats, particularly for vulnerabilities exploitable at scale (e.g., credential harvesting, silent data exfiltration, botnet enrollment). The process should define explicit thresholds or scaling factors at which individual-instance risk acceptance decisions are re-examined. This is particularly relevant for widely distributed consumer mobile applications.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

The OWASP Mobile Top 10 typically provides example attack scenarios that illustrate the potential impact of prevalent mobile application security weaknesses, including, in some cases, impact across large user populations

NOTE: Some product categories are covered by a vertical (sector-specific) standard that already defines its own risk acceptance criteria and metrics; where such a standard exists, applying its criteria is considered justified and consistent with the state of the art for that category.

Mobile-specific factors that may inform risk acceptance thresholds include: the heterogeneity of end-user devices and OS versions in the installed base; the inability to enforce timely patch adoption across user populations; the exposure of the application to shared-device or rooted/jailbroken environments; and the dependency on platform-enforced security controls (e.g., iOS App Transport Security, Android Keystore). OWASP MASVS provides a structured baseline of security controls for mobile applications that can serve as a reference point when calibrating what constitutes an acceptable residual risk level for a given mobile product category.

4.4 Product Cybersecurity Asset Identification

Introduction

Product cybersecurity asset identification establishes what needs to be protected for the product. Assets are closely tied to the product's context and span a broad range: data stored, processed, or transmitted (such as cryptographic keys, personal data, and logs); functions the product performs; software and hardware components and their interfaces; update and patch processes; and the wider system environment including adjacent networks and devices. Beyond the product itself, assets may relate to the user's high-level objectives-such as health, safety, privacy, user data, and availability of functions-as well as to the broader environment, including other persons, domestic animals, and public interest.

Output: an inventory of the product's cybersecurity assets together with the cybersecurity properties associated with each.

Requirements

Requirement CR-ID: 5.4-CR-01

When conducting a product cybersecurity risk assessment, all cybersecurity assets relevant to the product shall be identified, and it shall be determined which cybersecurity properties (confidentiality, integrity, availability, authenticity, and others as applicable) need to be ensured for each. This identification shall be grounded in the product context established under section 5.2, and the resulting asset list with associated cybersecurity properties shall be included in the product's technical documentation. The asset scope is broad and shall consider data assets (e.g. credentials, keys, personal data, configuration data, safety signals, firmware images, logs), functional assets, hardware and software components and interfaces, user-objective assets (health, safety, privacy, availability), and environmental assets (adjacent networks, third parties, public interest, and assets involved in RDPS).

Source:

- RMA-03-RQ-01 (40000-1-2)
- REQ-KEV-001 (40000-10)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- Related output obligation (40000-1-2 6.4.2.4)
- SOTA: Gap analysis findings on: documentation obligation, authenticity as a named property, safety signals as a discrete asset type

Guidance

Asset identification should be conducted in a manner that is representative of the product within its specified product context. The following guidance supports practitioners in scoping the exercise:

- Assets may be grouped into categories: product-level data assets, functional assets, supporting/operational assets (components, interfaces, update processes), user-objective assets, and environmental assets.
- Examples of data assets worth considering include credentials, cryptographic keys and authentication tokens, personal and financial data, safety signals, configuration data, firmware images, logs, and access rights.
- For each identified asset, the cybersecurity properties to be ensured should be explicitly indicated. Relevant properties include confidentiality, integrity, availability, and authenticity. Other properties may be applicable depending on the product context.

NOTE 1: Enumerating critical assets focuses security controls and testing on what needs to be protected, supporting a risk-proportionate approach to cybersecurity.

NOTE 2: Mobile applications frequently act as entry points to backend systems. Impact assessment should therefore consider: the sensitivity and volume of data accessible via the RDPS if the mobile application is compromised; the potential for lateral movement from a compromised mobile client to backend infrastructure; and the number of users whose data or services could be affected through a single exploited vulnerability in the mobile application.

Requirement CR-ID: 5.4-CR-02

In case the application employs AI models, AI-specific assets shall be included in the considerations to identify cybersecurity assets.

Source: SOTA

Guidance

Potentially relevant AI-specific assets include training data, test data, input data, model storage, augmentation data, agentic working memory, system prompts.

Further guidance is provided in ISO/IEC 27090, prEN 18282, and the OWASP AI Exchange which is designed to present the consensus of these standards.

4.5 Product Cybersecurity Risk Identification

Introduction

Product cybersecurity risk identification builds on the previously identified assets to determine which threats could realistically affect those assets within the product's context. Not every threat automatically constitutes a risk; the process evaluates whether a threat could cause an incident that compromises an asset and thereby gives rise to a cybersecurity risk.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Threat modelling provides a structured method for this identification, taking into account factors such as the product lifecycle, its functional behaviour, and the capabilities and motives of potential threat actors. Publicly available threat catalogues and sector-specific resources can support this process. Beyond threats, vulnerabilities - weaknesses in the product that threat actors could exploit - represent a distinct category of risk. Awareness of known vulnerabilities, discoverable through publicly available databases, is essential to addressing them appropriately. The applicability of identified threats and vulnerabilities is assessed by estimating exploitability within the defined product context, after which applicable items are documented as product cybersecurity risks.

Output: a list containing the product cybersecurity risks.

Requirements

Requirement CR-ID: 5.5-CR-01

Drawing on the established product context, product cybersecurity risks shall be identified. Each identified risk shall specify which asset(s) are targeted, which cybersecurity objective(s) of those assets may be compromised, and the cause of that potential compromise.

Source: RMA-04-RQ-01 (40000-1-2)

Guidance

Threat modelling is a recommended method for systematically identifying cybersecurity risks in mobile applications. Common approaches include STRIDE, attack trees, and PASTA; sector-specific risk analysis methods may also be used where applicable.

Useful inputs include mobile threat catalogues and knowledge bases such as MITRE ATT&CK, CAPEC, the OWASP Mobile Application Security Verification Standard (MASVS), and the OWASP Mobile Top 10, as well as platform-specific guidance from Android and iOS.

Not every identified threat constitutes a cybersecurity risk. The assessment should determine whether, in the specific mobile application context, the threat could realistically lead to an incident affecting assets such as user data, credentials, cryptographic keys, backend access, or app integrity.

Requirement CR-ID: 5.5-CR-02

Where publicly known vulnerabilities exist that are relevant to the product's assets and their associated cybersecurity properties, those publicly known vulnerabilities shall be identified. This obligation is conditional on the availability of such information.

Source: RMA-04-RQ-02 (40000-1-2)

Guidance

Known vulnerabilities can be identified through publicly available vulnerability databases. Awareness of these vulnerabilities is a prerequisite for addressing the associated risks. Even where exploitation may not be immediately apparent, the presence of a known vulnerability in the product warrants documentation as a potential product cybersecurity risk.

Vulnerabilities represent a specific category of risk arising from weaknesses in the product that threat actors could exploit. The applicability of a known vulnerability to the product should be assessed in the context of the product's exploitability within the defined product context.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 5.5-CR-03

A documented threat modelling procedure specific to mobile applications shall be established and maintained, defining the methodology to be applied (e.g., STRIDE, PASTA, attack trees), the threat catalogues to use, the roles responsible for conducting threat modelling, and the trigger conditions under which threat modelling shall be performed or repeated (e.g., new feature introduction, platform OS update, third-party SDK integration).

Source: SOTA

Guidance

The procedure should specify how mobile-specific threat surfaces are addressed, including: client-side attack vectors (e.g., reverse engineering, tampering, repackaging), inter-process communication mechanisms, and interactions with Remote Data Processing Solutions.

Threat catalogues should incorporate mobile-relevant threat taxonomies, including MITRE ATT&CK for Mobile (https://attack.mitre.org/matrices/mobile/), which covers tactics and techniques specific to Android and iOS platforms, and OWASP Mobile Top 10. Entries should be mapped to the asset categories and annotated with relevance to RDPS interactions (e.g., insecure API endpoints, token interception). The review interval should be risk-proportionate but no less frequent than annually, or following a significant change to the mobile platform ecosystem (e.g., a major Android or iOS release introducing new attack surfaces).

In case the application employs AI models, relevant threat taxonomies can be found in ISO/IEC 27090, prEN 18282, and the OWASP AI Exchange, which is designed to present the consensus of these standards.

4.6 Product Cybersecurity Risk Analysis

Introduction

This document does not require one specific risk analysis method. Different methods may be used, provided that the risk estimate considers both the likelihood of a successful attack and the impact if that attack succeeds. Possible approaches include fishbone diagrams, event tree analysis, fault tree analysis, attack feasibility ratings, or attack potential assessments.

Product cybersecurity risk analysis aims to estimate both the likelihood of occurrence and the potential impact of cybersecurity incidents arising from identified product risks. These estimates may be expressed qualitatively (e.g., using risk matrices) or quantitatively (e.g., using numerical scoring systems), and should be applied consistently to enable informed decisions on risk treatment or acceptance. Both likelihood and impact are assessed from the perspective of the users potentially affected. Likelihood factors may include how easily a risk can be discovered and how quickly it can materialize, while impact factors may include exposure of sensitive data, account takeover, fraud enablement, data loss, economic harm, and loss of accessibility.

Output: documented likelihood, impact severity, and incident scenario for each identified risk, including a rationale.

Requirements

Requirement CR-ID: 5.6-CR-01

For each product cybersecurity risk identified in accordance with 5.5, the likelihood of the associated cybersecurity incident occurring shall be estimated.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Source: RMA-05-RQ-01 (40000-1-2)

Guidance

When estimating likelihood, consider factors such as the discoverability of the risk and the speed at which it could materialize. Some risks may be easily detected by users, while others may be exploited without the user's awareness or so rapidly that intervention is not possible.

Likelihood estimates should be informed by current threat intelligence rather than solely by theoretical analysis. Relevant sources include: Apple Platform Security documentation and iOS Security Advisories, Android Security Bulletins published by Google, CVE databases filtered for mobile platform components, and OWASP Mobile Top 10 for prevalent mobile attack categories. The organization should establish a process for reviewing these sources at defined intervals (e.g., quarterly) and reassessing likelihood estimates when significant new threat information is published.

When estimating likelihood, the analysis should consider how exploitability is for relevant threat actors, taking into account their capabilities, access, and motivation. Threat actors may include external attackers, malicious apps on the same device, insiders, or unauthorized users with physical or logical access to the device or application.

Requirement CR-ID: 5.6-CR-02

For each product cybersecurity risk identified in accordance with 5.5, the severity of impact of the associated cybersecurity incident shall be estimated.

Source: RMA-05-RQ-02 (40000-1-2)

Guidance

When estimating impact, consider dimensions such as health and safety consequences, data loss, economic losses to the user, and effects on accessibility. As with likelihood, impact may be expressed qualitatively or quantitatively and should reflect the perspective of the users potentially affected by the risk.

Requirement CR-ID: 5.6-CR-03

For each product cybersecurity risk identified in accordance with 5.5, the cybersecurity incident scenario in which that risk could materialize shall be documented.

Source: RMA-05-RQ-03 (40000-1-2)

Guidance

Risk scenarios describe the context in which a risk could materialize into a cybersecurity incident. Documenting scenarios supports consistent analysis and enables informed risk treatment decisions.

The organization should structure risk scenarios using a defined template that captures the threat actor or source, the attack vector applicable to the mobile application or its RDPS, the vulnerability or weakness exploited, the attack path, and the resulting harm to the user.

For mobile applications, the attack vector field should reflect mobile-specific vectors such as: malicious applications on the same device, network-based attacks exploiting insecure communication, physical access to an unlocked or unencrypted device, and supply chain compromise of third-party SDKs or libraries integrated into the application. OWASP MASTG threat modelling guidance and OWASP Mobile Top 10 (2016/2024) provide reference scenario structures applicable to mobile contexts. STRIDE or PASTA methodologies can be

adapted for mobile scenario structuring. EN 18037 also provides guidance on risk scenario structuring.

Requirement CR-ID: 5.6-CR-04

A repeatable risk analysis methodology for cybersecurity risks shall be defined and documented, specifying the rating scale, criteria, and scoring rationale to be applied consistently across all risk assessments.

Source: SOTA

Guidance

The methodology should define discrete likelihood levels (e.g., rare, unlikely, possible, likely, almost certain) with explicit criteria for each level. For mobile-specific contexts, criteria may reference factors such as: public availability of exploit code targeting the mobile platform (iOS/Android), ease of exploitation given typical mobile threat actor capabilities, and whether the attack requires physical device access, network proximity, or can be conducted remotely. The methodology should be documented in a risk assessment procedure and applied uniformly by all analysts performing assessments. OWASP MASTG and OWASP Mobile Top 10(2016/2024) provide reference threat scenarios that can inform likelihood criteria calibration.

The impact methodology should extend general impact categories (health and safety, data loss, economic harm, accessibility) with mobile-specific sub-categories, such as: exposure of data processed or stored by the mobile application (including data accessible via platform APIs such as contacts, location, camera, and biometric data); loss of control over device functions that could affect the user or third parties; and cascading impact on backend Remote Data Processing Solutions (RDPS) accessed by the application. OWASP MASVS v2 (particularly the MASVS-STORAGE, MASVS-PRIVACY, and MASVS-RESILIENCE categories) provides a structured taxonomy of mobile-specific impact areas that can inform impact criteria definition. NIST SP 800-30 Rev. 1 Table H-2 provides a general impact taxonomy that can be adapted for mobile contexts.

Requirement CR-ID: 5.6-CR-05

The rationale and evidence supporting each likelihood and severity result shall be documented, enabling independent review and auditability of the risk analysis.

Source: SOTA

Guidance

For each risk, the risk record should capture: the likelihood rating assigned, the criteria applied from the defined methodology, the evidence or assumptions supporting the rating (e.g., known exploitation in the wild, CVSS exploitability sub-score, availability of attack tooling for the relevant mobile platform), and the identity and date of the analyst performing the assessment. This supports both internal quality assurance and external assessment.

Impact records should capture: the impact dimensions assessed (e.g., data confidentiality, user safety, economic harm, accessibility), the magnitude rating assigned per dimension, the aggregation method used where multiple dimensions are affected, and any assumptions made regarding the user population or deployment context. Where CVSS v3.1 or v4.0 impact sub-scores are used as inputs, this should be noted. Documentation should be sufficient to allow a third party to reproduce or challenge the estimate. NIST SSDF RV.1.3 supports this documentation requirement.

4.7 Product Cybersecurity Risk Evaluation and Risk Acceptance

Introduction

Product cybersecurity risk evaluation involves comparing identified risks against pre-established risk acceptance criteria to determine whether each risk is acceptable or requires treatment. Accepting a risk is a conscious decision to acknowledge it without taking further action to reduce it, provided it meets the predetermined criteria.

Accepted residual risks do not disappear - they are effectively shared with the product's user. This sharing is conditional: it requires that the conditions of use clearly communicate any controls or operational environment requirements needed to use the product securely. Risk sharing does not relieve a manufacturer of legal obligations, and is particularly relevant for products used as components, where certain risks cannot be addressed at the component level and instead need to be managed by the integrating party.

Output: evaluation of determined risks and justification for risk acceptance.

Requirements

Requirement CR-ID: 5.7-CR-01

Every identified risk shall be systematically assessed against the pre-established risk acceptance criteria to determine whether it can be accepted as-is or shall be subjected to treatment measures.

Source: RMA-06-RQ-01 (40000-1-2)

Requirement CR-ID: 5.7-CR-02

A risk may be deemed acceptable only when it demonstrably aligns with the predetermined risk acceptance criteria defined in 5.3. Risks that do not meet these criteria shall not be accepted, regardless of other considerations such as cost or feasibility.

Source: RMA-06-RQ-02 (40000-1-2)

Requirement CR-ID: 5.7-CR-03

When residual risks are shared with users - because the product relies on the operational environment or user action to provide necessary controls - it shall be verified that the required user mitigations are realistic and achievable for the intended user base, given their expected knowledge and capability. Risk acceptance under these conditions is contingent on this verification.

Source: RMA-06-RQ-03 (40000-1-2)

Guidance

When residual risks are shared with users - for example, because the product is intended to be deployed within a specific operational environment that provides additional controls - the manufacturer should verify that the required mitigations are realistic for the intended user base. For instance, a component lacking built-in access controls may be acceptable if the intended operational environment provides those controls externally, but this assumption needs to be clearly communicated and needs to be achievable by the expected users. Similarly, a memory chip that does not support data confidentiality or integrity may transfer

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

that responsibility to an integrator, but only if the integrator can reasonably be expected to implement the necessary protections.

NOTE 1: Sharing risk with users does not exempt a manufacturer from its legal responsibilities.

NOTE 2: This applies particularly to products that function as components: certain risks affecting a component simply cannot be resolved at that level and are therefore passed on to whoever integrates or uses the product.

NOTE 3: In some cases it may be appropriate for the manufacturer to organize a recall of a product subject to a severe risk discovered after the product is placed on the market, where that risk cannot be addressed by action of the user.

Requirement CR-ID: 5.7-CR-04

For each accepted or residual risk, a documented acceptance justification shall be produced and retained explaining why the risk is considered acceptable. This justification shall reference the risk acceptance criteria from 5.3 and shall describe any conditions of use or operational environment assumptions on which the acceptance is predicated.

Source:

- RMA-06-RQ-04
- 6.4.5.4 output requirement and 6.4.5.5 assessment criteria (40000-1-2)

4.8 Product Cybersecurity Risk Treatment

Introduction

Risk treatment aims to reduce risks to an acceptable residual level. The primary approaches are risk avoidance - eliminating the source of a risk entirely - and risk mitigation - implementing controls that reduce likelihood or impact. Where neither is feasible within the product itself, adjusting the product context (e.g., restricting intended use or operating environment) can bring risks within acceptable bounds.

When risks cannot be fully addressed through product changes, user-side action may be necessary. In such cases, users need to be clearly informed of the remaining risks and what actions they should take. The appropriate level of information shared with users depends on their expected capabilities and context. For instance, insecure features may be disabled by default and only enabled through explicit user configuration, accompanied by clear warnings.

Output: risk treatment decisions with rationale.

Requirements

Requirement CR-ID: 5.8-CR-01

For every risk that does not satisfy the established risk acceptance criteria, a treatment option that is appropriate to the product context shall be applied.

Source: RMA-07-RQ-01 (40000-1-2)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

Risk treatment options include:

- **Risk avoidance**: eliminating the source of the risk altogether - for instance by removing interfaces that serve no purpose, steering clear of libraries that are not yet mature, dropping insecure legacy communication protocols, or dropping support for external plugins or scripting where it is not genuinely needed.
- **Risk mitigation**: implementing controls that reduce the likelihood or impact of a risk. Note that adding controls may itself introduce new risks or alter existing ones, requiring a repeat of the risk assessment.
- **Context adjustment**: altering the intended purpose or conditions of use to modify the risk acceptance criteria, thereby rendering a previously unacceptable risk acceptable.
- **User-side treatment**: where risks cannot be avoided or mitigated within the product itself, informing users of the remaining risks and the actions required of them. This is particularly relevant when insecure features need to remain available but are disabled by default, with users explicitly enabling them via configuration accompanied by clear warnings.

Requirement CR-ID: 5.8-CR-02

For each risk subject to treatment, documentation shall be made of the treatment option selected and the justification for why that option is appropriate given the product context together with the applicable risk acceptance criteria.

Source: RMA-07-RQ-02 (40000-1-2)

Guidance

Documentation of the risk treatment decision should capture which treatment option was selected for each unacceptable risk and why that option is appropriate given the product context and risk acceptance criteria. Documentation should be sufficient to support traceability and auditability of risk management decisions. The output should include a risk treatment decision with justification per risk, and assessors will verify that the justification is aligned with the risk acceptance criteria established in 5.3.

Requirement CR-ID: 5.8-CR-03

Following the application of any risk treatment measure, the affected risks shall be re-evaluated to determine whether residual risks indeed meet the established acceptance criteria.

Source: RMA-07-RQ-03 (40000-1-2)

Guidance

Re-evaluation should account for the fact that risk treatment measures - particularly mitigation controls - can change the profile of existing risks and may introduce new risks. The re-evaluation feeds back into the risk assessment process (see 5.5 - 5.7), ensuring that residual risks are measured against the established acceptance criteria. This iterative cycle continues until all risks are either acceptable or have been addressed through an appropriate treatment option.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

4.9 Product Cybersecurity Risk Communication

Introduction

Risk communication ensures that users receive clear, actionable information about cybersecurity risks associated with a product. This includes both the risks transferred to the user and the measures users are expected to take to mitigate them. Communication should be tailored to the needs of the intended audience: while technical language may suffice when addressing other manufacturers, end users - including those with impairments - may require simpler language or alternative formats to meaningfully access and act on this information.

Output: documentation containing the circumstances and misuse that can lead to significant cybersecurity risks, conditions of use, and mitigation instructions to users.

Requirements

Requirement CR-ID: 5.9-CR-01

Risk communication directed at users shall employ language and methods appropriate to the audience; where the audience consists of consumers, the language used shall be clear and free of technical jargon to the extent practicable.

Source: RMA-08-RQ-01 (40000-1-2)

Guidance:

When communicating risks to end users, avoid jargon and technical terminology. Consider the audience's background and adjust the language accordingly. For instance, a consumer product manual should describe risks and mitigations in plain language, whereas documentation directed at professional integrators or other manufacturers may use more technical terms where mutually understood.

Requirement CR-ID: 5.9-CR-02

Where a product is subject to applicable accessibility obligations or where the intended user base includes individuals with impairments, risk communication shall consider formats and using language to ensure each user can meaningfully access the information.

Source: RMA-08-RQ-02 (40000-1-2)

Guidance

Where a product is subject to accessibility legislation (e.g. the European Accessibility Act), or where the user base is known to include individuals with impairments, risk communication should be made available in multiple formats. Examples include audio descriptions, screen-reader-compatible digital documents, or printed materials with simplified language. Relying solely on a website for risk disclosure may be insufficient for users without reliable internet access or those with visual impairments.

NOTE: What counts as adequate communication depends on who the audience is. Some end users may be unable to access written information at all or may be excluded if that information exists only on a website. Where the recipient is another manufacturer, however, simply providing the information in a language they understand may be enough.

Requirement CR-ID: 5.9-CR-03

Risk communication documentation shall address a minimum set of elements: the circumstances and foreseeable misuse scenarios that could give rise to significant

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

cybersecurity risks; the mitigation measures users are expected to implement; and the operational conditions under which the product may be used securely.

Source: RMA-08-RQ-03 (40000-1-2)

Guidance

Risk communication documentation should cover:

1. Scenarios in which the product could be misused or exposed to elevated risk, including foreseeable misuse cases identified during risk assessment;
2. Concrete steps users can take to reduce those risks, such as network segmentation, configuration hardening, or restricted physical access; and
3. The operational conditions under which the product can be considered secure, for example supported software versions, required network configurations, or maintenance obligations.

4.10 Product Cybersecurity Risk Review

Introduction

Maintaining appropriate cybersecurity over a product's lifetime requires periodic review and, where necessary, updating of risk management activities to account for changes in the threat landscape and the evolving state of the art. Reviews may be conducted at regular intervals, with the frequency determined by the nature of the risks and the specific product context.

Output: record of the review and any updates to risk management documentation.

Requirements

Requirement CR-ID: 5.10-CR-01

Reviews of product cybersecurity risk management activities shall be conducted at planned intervals, where the frequency of those intervals is determined by the risk assessment and the context in which the product operates, and at least once a year - despite design staying the same.

Source: RMA-09-RQ-01 (40000-1-2)

Guidance

The appropriate interval between reviews is not fixed; it should be calibrated to the risk level and the context in which the product operates. Higher-risk products or those deployed in rapidly changing environments may warrant more frequent reviews.

Requirement CR-ID: 5.10-CR-02

In addition to planned-interval reviews, a review of risk management activities shall be initiated when trigger conditions are met, including product modification, context changes, changes to risk acceptance criteria, changes in cybersecurity risk exposure (including threat landscape changes), identification of a known exploitable vulnerability, occurrence of a severe incident, or obsolescence of a component with cybersecurity impact.

Source: RMA-09-RQ-02 (40000-1-2)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

Beyond planned interval reviews, organizations should establish monitoring mechanisms capable of detecting these trigger conditions in a timely manner. This may include subscribing to threat and vulnerability intelligence feeds and tracking cybersecurity testing outcomes so that event-driven reviews can be initiated promptly when a trigger is identified.

Requirement CR-ID: 5.10-CR-03

Where a review conducted under 5.10-CR-01 or 5.10-CR-02 reveals that existing risk assessment documentation is affected, the relevant documentation produced under Clause 5 shall be updated accordingly.

Source: RMA-09-RQ-03 (40000-1-2)

Guidance

Updating documentation may include adding or modifying product controls where the review reveals that existing controls are insufficient to address newly identified or changed risks.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

5 Product Cybersecurity Lifecycle Activities

5.1 Introduction

Cybersecurity lifecycle activities for mobile applications and their backend services are intended to integrate with modern software development practices, including agile and DevSecOps approaches, rather than depend on a single linear process. Although some activities require prerequisite inputs, many can be performed concurrently or in varying sequences. Additionally, activities may be revisited at appropriate points or at regular intervals, as a change in one activity can have implications for several others.

5.2 Product Cybersecurity Planning

Introduction

Product cybersecurity planning defines the cybersecurity activities applicable to a product throughout its lifecycle. The extent and frequency of these activities are informed by the risks identified through risk assessment, for example when determining the type or cadence of testing to be performed. Although the activities are generally consistent across development approaches, the way they are carried out may differ. Planning typically produces a living document that is updated as further information becomes available and may refer to organization-wide policies where activities are implemented consistently across multiple products.

Output: Documented product cybersecurity planning.

See OpenCRE 635-851 at opencre.org/cre/635-851 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 6.2-CR-01

The product cybersecurity plan shall take the product context from 5.2 into account, when available, and define, at minimum, every applicable cybersecurity activity defined in Clauses 6 and 7.

Source:

- CLA-01-RQ-01 (40000-1-2)
- SOTA

Guidance

Certain activities may be organization-wide instead of just for the product, in which case the plan can reference an organization-wide policy.

Mobile application development introduces platform-specific lifecycle phases and artefacts (e.g., app store submission, OS version compatibility cycles, SDK dependency updates) that differ from generic software development. The planning procedure should identify which activities apply per platform and per lifecycle phase.

Mobile application development teams frequently include platform-specific engineers, backend engineers responsible for RDPS, and release managers handling app store submissions, each with distinct security responsibilities. The plan can assign named roles or

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

role types to planned cybersecurity activities and consider proper training for the people involved.

Requirement CR-ID: 6.2-CR-02

Throughout the entire product lifecycle, the product cybersecurity plan shall be kept current through regular maintenance and review, and the execution of all planned activities shall be actively tracked. Review shall take place not only on a regular schedule but also upon occurrence of defined triggers.

Source:

- CLA-01-RQ-02 (40000-1-2)
- SOTA (triggers)

Guidance

The product cybersecurity plan should be treated as a document that develops over time. It may start with limited detail and be expanded as further information becomes available. Reviews should take into account changes in the risk landscape, such as newly discovered threats after release that may require adjustments to planned testing. Monitoring progress against the plan helps confirm that agreed activities are performed and that missing or delayed actions are detected early. The plan may also address roles, responsibilities, and training needs, so that cybersecurity activities can be maintained throughout the product lifecycle.

5.3 Product Cybersecurity Requirements

Introduction

Product cybersecurity requirements specify what shall be implemented in the product. They are grounded in the product context, informed by risk assessment, and shaped first by applicable legal and regulatory obligations, then by stakeholder needs. In defining these requirements, qualities such as traceability, validity, understandability, and verifiability are typically considered, together with the cybersecurity characteristics of the product's operating environment across its lifecycle, including development, deployment, production, maintenance, and decommissioning. These requirements provide a foundation for subsequent engineering activities and should be actively managed throughout the product lifecycle.

Output: Documented cybersecurity requirements.

See OpenCRE 004-517 at opencre.org/cre/004-517 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 6.3-CR-01

Product cybersecurity requirements shall be derived from and grounded in the product context, the decisions made regarding treatment of product cybersecurity risks, and all applicable regulatory requirements.

Source: CLA-02-RQ-01 (40000-1-2)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

When specifying product cybersecurity requirements, consider ensuring they are traceable back to their source inputs (product context, risk treatment decisions, regulatory requirements, stakeholder needs), understandable to relevant stakeholders, and verifiable through assessment or testing. Requirements should reflect the cybersecurity properties needed across the product's environment during development, deployment, production, maintenance, and decommissioning.

For mobile applications, requirements should account for platform-specific threat surfaces (iOS, Android, cross-platform frameworks) and the cybersecurity properties of any Remote Data Processing Solutions (RDPS) the application depends upon.

NIST SSDF practice PO.1 ("Define Security Requirements for Software Development") and OWASP MASVS provide relevant reference points for structuring mobile-specific security requirement sets.

Requirement CR-ID: 6.3-CR-02

Whenever any of the defined inputs - product context, risk assessment outcomes, risk treatment decisions, or applicable regulatory requirements - undergo change, the product cybersecurity requirements shall be reviewed and updated as necessary to remain current and accurate.

Source:

- CLA-02-RQ-02;
- input list from section 7.3.2 (40000-1-2)

Guidance

Organizations may consider establishing a change management process or trigger-based review mechanism to ensure that updates to any of these inputs are systematically evaluated for their impact on the product cybersecurity requirements.

Requirement CR-ID: 6.3-CR-03

Changes to product cybersecurity requirements shall be communicated to all affected development, testing, and operations teams in a timely and documented manner, with impact assessment by each affected party.

Source: SOTA

Guidance

Communication may be formalized through a requirements change notification process integrated into the project's change control board or sprint planning cycle. For mobile applications developed using agile or DevSecOps methods, requirement changes should be reflected in the product backlog with security impact labels, and downstream artefacts (threat models, test plans, security test cases) should be flagged for update.

5.4 Cybersecurity Architecture and Design

Introduction

Cybersecurity architecture and design translate the cybersecurity requirements (defined in 6.3) and product context (defined in 5.2) into concrete design decisions and control

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

selections. Design decisions are based on those requirements and may, where necessary, result in refinement of the cybersecurity requirements. Key design considerations include defining trust boundaries between components and subsystems, designing secure interfaces with attention to authentication, input validation, and attack surface minimization, and ensuring secure-by-default configurations. Typical design artefacts include design documents, interface definitions, and data-flow or trust-boundary diagrams. Catalogues such as draft prEN 40000-1-4 or vertical standards under standardization request M/606 may serve as reference sources for control selection, though manufacturers are free to use other technically appropriate sources.

Output: Documented cybersecurity architecture and design.

See OpenCRE 326-704 at opencre.org/cre/326-704 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 6.4-CR-01

A specification of the product's cybersecurity architecture and design shall be produced. This specification shall include the selection of cybersecurity controls chosen to satisfy the cybersecurity requirements established in 6.3.

Source: CLA-03-RQ-01 (40000-1-2)

Guidance

The cybersecurity architecture and design documentation can, where relevant, describe how the product is structured and protected. This may cover default security configurations for components, the product's internal and external interfaces and the protections applied to them, and diagrams that show data flows, trust boundaries, components, and subsystems.

The choice of controls can be based on suitable control catalogues, such as EN 40000-1-4, relevant sector-specific standards developed under standardization request M/606, or other sources that are technically appropriate for the product and its risks.

5.5 Secure Implementation

Introduction

Secure implementation ensures that a product is built in accordance with its cybersecurity requirements and architecture.

Output:

- documentation on securing the development environment;
- the product with implemented cybersecurity according to security requirements, secure coding standard, architecture and design, and approved cryptography, including secure hardware modules;
- secure coding standard;
- documented process regarding memory-unsafe programming;
- documented process for managing keys and certificates;
- documented protocol inventory review;
- documented compensating security for vulnerable protocols;

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- documented changes to risk management and lifecycle, if any, caused by implementation deviations.

Requirements

Requirement CR-ID: 6.5-CR-01

The product shall be developed and maintained securely by using a secure development environment to prevent unauthorized access, to an extent appropriate given the product's risk profile, design, and scope. This shall be demonstrated by including the development environment in the scope of the provider's Information Security Management System certified against ISO/IEC 27001 by an accredited certification body.

Source: CLA-04-RQ-01(40000-1-2), SOTA (27001 for this security level)

Guidance

A secure development environment may include measures such as:

- access control and monitoring of access to engineer workstations, source code repositories, build systems, components, signing infrastructure, provisioning profiles, and CI/CD pipelines;
- branch protection rules;
- separation of development, build, test, and production environments;
- patching and hardening of development systems;
- protection of secrets, keys, and credentials used in development;
- development environments monitoring for suspicious activity;
- controls over who may trigger production builds or submit applications to app stores (Google Play, Apple App Store).

See OpenCRE 148-853 at opencre.org/cre/148-853 for related resources and topics for guidance.

Requirement CR-ID: 6.5-CR-02

The product shall implement all cybersecurity requirements established in 6.3, in conformance with the cybersecurity architecture and design defined in 6.4.

Source: CLA-04-RQ-02 (40000-1-2)

Guidance

Implementation should include the cybersecurity controls defined during design.

Requirement CR-ID: 6.5-CR-03

A documented secure coding standard shall be adopted and enforced, applicable to the programming languages and frameworks used in the mobile application, covering at minimum: prohibited functions, memory safety practices, input validation, output encoding, error handling, preventing common security weaknesses, and prohibition of hard-coded credentials.

Source: SOTA and guidance

Guidance

Coding standards support code quality, consistency, and avoiding weaknesses.

Applicable sources may include the CERT Secure Coding Standards (SEI CERT C, C++, Java), OWASP Mobile Top 10, and platform-specific guidance from Google (Android Developers Security) and Apple. For cross-platform frameworks (React Native, Flutter), the standard should address framework-specific risks. The standard should be enforced through automated static analysis and linting integrated into the CI/CD, and be the input for code review.

See OpenCRE 036-275 at opencre.org/cre/036-275 for related resources and topics for guidance, and for an overview of all technical application security controls: opencre.org/cre/636-660

Requirement CR-ID: 6.5-CR-04

A process shall be established for identifying, reviewing, and approving the use of memory-unsafe programming languages or constructs in the mobile application, and shall document the rationale and compensating controls where their use cannot be avoided.

Source: SOTA

Guidance

Where native code (C/C++) is used in Android NDK modules or iOS frameworks, memory-safe practices should be applied including bounds checking, use of safe string and memory functions, and static analysis for buffer overflows and use-after-free vulnerabilities. Consider migration to memory-safe languages (Rust, Swift, Kotlin) where feasible.

The guidance "The Case for Memory Safe Roadmaps" (2023) by CISA, NSA et al provides a roadmap approach.

Requirement CR-ID: 6.5-CR-05

Where secure implementation activities produce deviations from the cybersecurity architecture and design, reviews shall be triggered of the cybersecurity risk management activities, as defined in 5.10 and all affected cybersecurity product lifecycle activities.

Source: CLA-04-RQ-06 (40000-1-2)

Guidance

Deviations can occur when practical implementation limits, selected tools, or the behaviour of components do not match the assumptions made during design. When this happens, the architecture and design documentation should be reviewed and updated where needed. The product cybersecurity requirements and related risk management activities should also be reconsidered, so that the product's security position remains aligned with the intended design.

Requirement CR-ID: 6.5-CR-06

The product shall use cryptographic mechanisms that reflect the state of the art and that conform to the cryptographic requirements applicable to the product and agreed within its certification, regulatory, or sectoral context - covering the selection of algorithms, parameters, key sizes, operational modes, random number generation, key lifecycle management, and the deprecation policy.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Where the applicable requirements do not designate a specific cryptographic reference, the agreed cryptographic mechanisms defined in the ECCG "Agreed Cryptographic Mechanisms" (ACM) shall be used as the recognised baseline. Where the product is subject to a European Digital Identity Wallet certification scheme or to the EUCC, the applicable ACM version is the one required by that scheme (via the EUCC "Guidelines on Cryptography") at the time of the conformity assessment or surveillance evaluation; versions issued as drafts or for public review are excluded until adopted.

Where the applicable requirements or the ACM do not address a specific mechanism, equivalent state-of-the-art cryptographic guidance shall be applied. Continued conformity as the applicable requirements or the applicable ACM version evolve shall be maintained in accordance with 6.5-CR-09.

Source:

- REQ-CON-002 (40000-10)
- SOTA (fallback obligation; alignment of the applicable requirements and version with the product's certification/regulatory context)

Guidance:

The requirement is deliberately layered. The primary obligation is to meet the cryptographic requirements that are applicable to the product and agreed within its context, while reflecting the state of the art; the ECCG "Agreed Cryptographic Mechanisms" (ACM) is then named as the concrete reference. This keeps the requirement usable both for products inside a formal certification scheme and for high-attack-potential mobile applications addressed under other regimes.

Determining what is applicable and agreed depends on the product's context. For a product certified under, or being prepared for, a European Digital Identity Wallet certification scheme (built on the EUCC), the applicable agreed reference is the ECCG/ENISA ACM in the version the scheme mandates at the time of assessment. This mirrors how the EU framework itself handles the reference: the ACM version is carried in a maintained companion document (the EUCC "Guidelines on Cryptography").

For other mobile applications exposed to adversaries with a high attack potential, the applicable requirements may come from a sectoral scheme, a regulatory regime, or a customer or contractual security baseline. Where one of these designates a cryptographic reference, that reference governs; where none does, the ACM serves as the recognized default baseline, because it expresses mechanisms agreed as state of the art across the EU national cybersecurity certification authorities.

At the time of writing, the current ACM version is v2 (May 2025). A version 3, realigned for the post-quantum era, was in public review until the end of July 2026; once adopted and taken up by the applicable scheme or baseline, it becomes the applicable version and the migration provisions of 6.5-CR-09 apply. Manufacturers should confirm the version and any cryptographic reference mandated by their specific context, since these can be updated independently of this document. Drafts and public-review versions are not applicable until adopted; the intent is a deferred-dated reference in which the applicable context fixes a single version at any point in time, giving a determinate target while allowing the baseline to advance without amending this document.

Because high-attack-potential contexts (and, for wallets, Level of Assurance High) demand a current cryptographic baseline and a credible post-quantum path, the product should be designed for cryptographic agility, so that algorithms and parameters can be replaced — including migration to post-quantum or hybrid mechanisms — during the product's lifecycle

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

and support period without redesign. Note that the ACM sets validity periods and deprecation deadlines for legacy mechanisms; migration timing may be dictated by those deadlines rather than by a fixed interval.

See OpenCRE 170-772 at opencre.org/cre/170-772 for related resources and topics for guidance.

Requirement CR-ID: 6.5-CR-07

The product shall protect cryptographic keys through secure hardware modules. If hardware-based protection is not feasible, the product shall use secure software modules to protect cryptographic keys.

Source: REQ-CON-003 (40000-10)

Guidance

Cryptographic keys play a central role in protecting the product, its communications, and its data. They should therefore be stored using strong protection measures. Where suitable for the product, hardware-based protection such as hardware security modules, or comparable trusted execution environments, should be used.

If hardware-based protection is not suitable because of the product's design or practical constraints, software-based measures, such as encrypted key stores or secure enclaves, may be used as an alternative.

See OpenCRE 032-213 at opencre.org/cre/032-213 for related resources and topics for guidance.

Requirement CR-ID: 6.5-CR-08

A process shall be established for inventorying and verifying all locations in the mobile application and its RDPS where cryptographic keys are generated, stored, used, and destroyed. Verification shall ensure that each location meets the cryptographic requirements in this document.

Source: SOTA

Guidance

The inventory should cover: keys stored in the Android Keystore system or iOS Secure Enclave/Keychain; keys used in RDPS backend services; keys embedded in configuration files or transmitted over the network; and keys used by third-party SDKs. For each key, document: the key type and purpose, the protection mechanism applied, the hardware backing status (e.g., StrongBox on Android, Secure Enclave on iOS), and the key lifecycle.

OWASP MASVS-CRYPTO-1/-2 and OWASP MASTG provide test cases for verifying key protection. Align with NIST SSDF PW.5.

Requirement CR-ID: 6.5-CR-09

A process shall be established for periodically reviewing the protocol inventory (see technical documentation in 6.6) against current state-of-the-art guidance and for identifying protocols that have been deprecated, are vulnerable, or require compensating measures in accordance with 6.5-CR-10.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Source: SOTA

Guidance

The review should be triggered by: publication of new vulnerability disclosures affecting protocols or mechanisms in the inventory; a change to the applicable cryptographic requirements or the adoption of a new applicable ACM version (or other state-of-the-art guidance) that deprecates algorithms, parameters, protocol versions, or cipher suites; and at defined periodic intervals (at least annually). For mobile applications, particular attention should be paid to TLS version support across the range of OS versions the application supports, as older OS versions may not support current TLS configurations.

Where the product is certified, aligning the transition period with the scheme's own maintenance mechanisms - such as mandatory surveillance evaluations under a wallet certification regime, and the assurance-continuity handling of updated state-of-the-art documents under EUCC - keeps the certified status consistent as the cryptographic baseline evolves and avoids the product silently falling out of conformity between assessments. Where the product is not certified, the same review-and-migrate discipline should be applied against the applicable baseline. The review outcome should feed into the vulnerability management process and, where protocol or mechanism changes are required, into the deviation handling process under 6.5-CR-05.

Align with OWASP MASVS-NETWORK and NIST SSDF RV.1.

Requirement CR-ID: 6.5-CR-10

When the product relies on legacy or vulnerable protocols, the product shall implement security measures mitigating protocol issues - such as, but not limited to, multi-factor authentication - sufficient to maintain a security level commensurate with the risks introduced by those protocols.

Source: REQ-EMM-002 (40000-10)

Guidance

Use the protocol inventory maintained under 6.6-CR-04 to determine whether any outdated or vulnerable protocols are still used by the product.

Where such protocols cannot be avoided, additional protections should be applied. These may include measures such as multi-factor authentication, network segmentation, access control lists, stronger monitoring, or encryption layers around the communication.

Some weaker protocols may be needed to remain compatible with older systems or products. However, their use should not lower the product’s overall cybersecurity level. The added protections should be appropriate to the risk created by the specific protocol.

5.6 Technical Product Documentation

Introduction

Technical product documentation extends product context documentation with technical details.

Output:

- a list of integrated components;

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- documentation on complying with components' intended purpose and instructions;
- technical documentation and user information and instructions;

Requirements

Requirement CR-ID: 6.6-CR-01

The product shall maintain an identified list of all integrated components including at least the top-level dependencies and the transitive dependencies when technically feasible, in a commonly used machine-readable format. This is referred to as an SBOM (Software Bill Of Materials). A list entry shall include the type of dependency, software producer, unique component identifier (e.g. producer, component name, and component version). The SBOM shall contain the identity of the SBOM author, a version indicator, and a timestamp. When integrating third-party components, the intended purpose and user instructions to address cybersecurity risks of those components are the conditions that shall be adhered to.

Source:

- (40000-1-2) CLA-04-RQ-03; CLA-04-RQ-04
- (40000-1-3) PRE-7-RQ-01 (SBOM); PRE-7-RQ-02 (SBOM content); PRE-7-RQ-03(top level); PRE-7-RQ-04(format); PRE-7-RQ-06 (metadata); PRE-7-RQ-03-RE (transitive); PRE-7-RQ-07 (required information); PRE-1-RQ-04 (SBOM for vulnerability handling)

Guidance:

When a vulnerability is disclosed in third-party or open-source software, organizations need to quickly determine whether the affected component is present in their products. That requires an accurate record of the software components included in each product, along with their origins, dependencies, and supporting documentation.

The identification process should make use of all available relevant inputs - including source code, binary artefacts, configuration files, and cybersecurity architecture documentation - to achieve a complete picture. The intended outcome is a thorough, traceable inventory of components that can underpin vulnerability assessments across the full product lifecycle.

Top-level dependencies are components that are directly incorporated into or required by the product. Further clarification on how to define and scope top-level dependencies can be found in BSI TR-03183-2 v2.1.0, section 8.3.1.

Capturing transitive dependencies - those that are indirectly required through other components - in the SBOM supports quicker and more effective identification of vulnerabilities that may be inherited from upstream components. It is recognized that complete enumeration of transitive dependencies may not always be achievable, as suppliers do not always provide the information needed. For further guidance on scoping the depth and breadth of SBOM content, ISO/IEC 27036-3:2023, Annex B, section B.3.1.3 is a relevant reference.

Among the machine-readable formats widely used in the software industry, SPDX (standardized as ISO/IEC 5962:2021) and CycloneDX are commonly adopted options.

Where an open-source component is maintained under the oversight of an open-source steward, the stewarding organization's name should be entered in the software producer field.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Unique component identifiers function as reference keys that allow components to be looked up in vulnerability databases. Recognized identifier types include Common Platform Enumeration (CPE), Package URL (PURL), and SoftWare Hash IDentifier (SWHID); where multiple identifiers exist for a component, all may be recorded. Licence information is an optional supplementary field that may also be captured for each component.

When third-party libraries are selected and integrated, preference should be given to libraries that are secure, actively maintained, and kept current. Integrated components should also be configured carefully, because configuration choices and implementation options can influence the cybersecurity of the product as a whole.

See OpenCRE 863-521 at opencre.org/cre/863-521 for related resources and topics for guidance.

Requirement CR-ID: 6.6-CR-02

A mapping of upstream dependencies and interdependencies, apart from components, shall be available to support coordination and notification when a vulnerability is discovered, so that related issues can be resolved without undue delay.

In case the application employs AI models, any externally supplied element for this employment shall be part of this mapping, including third-party models, training data, augmentation data, MCP servers and agentic skills.

Source:

- PRE-1-RQ-04 (40000-1-3)
- SOTA (AI)

Guidance

When a vulnerability is identified, this inventory, next to an SBOM, supports the rapid identification of affected elements and facilitates timely engagement with the relevant upstream stakeholders.

More guidance regarding AI-dependencies and AIBOM (AI Bill Of Materials) can be found in ISO/IEC 27090, prEN18282, and the OWASP AI Exchange as it is designed to represent the consensus of these standards.

Requirement CR-ID: 6.6-CR-03

If a new software build or release is created, or if an inaccuracy is found in the current SBOM, a revised SBOM shall be issued.

Source:

- PRE-7-RQ-05 (40000-1-3)
- PRE-7-RC-01 (40000-1-3)

Guidance:

The obligation to produce a new SBOM extends beyond major or feature releases and applies to any build that incorporates an updated component or dependency, regardless of whether other aspects of the product have changed. This includes dependency changes introduced through automated dependency management tools such as Dependabot or Renovate. To ensure SBOM currency is maintained independently of feature release cycles, organizations should establish procedures that trigger SBOM regeneration as part of the pull request or merge workflow whenever such updates occur.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 6.6-CR-04

Technical documentation and user instructions shall be written in language easily understood by the user and shall include at least:

a) documentation of all logical and physical interfaces and transport protocols with their security properties;
b) cybersecurity prerequisites for the deployment environment;
c) a description of implemented security functions;
d) usage instructions covering installation and hardening;
e) data deletion and decommissioning procedures; and
f) detailed configuration and maintenance instructions.

These topics shall at least cover when applicable: configuration baselines, safe defaults, backup and restore, patching and updating, key rotation, log management including synchronization of time, incident response hooks, and interactions with platform security services (iOS Keychain, Android Keystore, biometric APIs, app sandboxing).

Source:

- CLA-04-RQ-05 (40000-1-2)
- REQ-TGSA-003 [sub-item (a)] (40000-10)
- REQ-KEV-003 [sub-item (b)] (40000-10)
- REQ-SBD-001 [sub-item (c)] (40000-10)
- REQ-DRT-002 [content specification for sub-item (d)] (40000-10)
- REQ-DRT-003 [sub-item (e)] (40000-10)
- REQ-DRT-004 [content specification for sub-item (f)] (40000-10)
- SOTA (interactions with platform security services)

Guidance

Technical documentation and user instructions may be prepared and updated at various phases of the product lifecycle. Regardless of when they are drafted, they should be reviewed for consistency and appropriateness, typically during verification and validation activities.

a) For sub-item (a): Enumerate every physical and logical interface and protocol the product uses. For each one, capture relevant security properties (e.g. authentication, confidentiality, integrity), any trust boundaries involved, and whether it is enabled by default or optional, together with the protocol version, cipher policy, and any relevant state-of-the-art conformity or certification. Because interfaces and protocols are frequently targeted by attackers, documenting them thoroughly helps ensure they are configured and tested correctly.
b) For sub-item (b): Specify OS and hypervisor versions, database hardening requirements, PKI requirements, network segmentation and ACLs, and SIEM integration requirements. This enables avoidance of deploying a securely designed product on an information system that does not meet the necessary requirements.
c) For sub-item (c): Document the product's security functions, which may include (among others) authentication, authorization, logging, secure update, secure boot, rate limiting, secure storage at both the physical and logical level, physical protection, safeguards against sensitive-data exposure via the user interface (e.g. clipboard, screenshots, app-switcher snapshots, keyboard caching), and any accepted residual risk. Setting these functions out explicitly turns the product's

protection goals into something that can be checked and tested. Cryptographic functions should be documented as described under 6.6-CR-05.

d) For sub-item (d): Set out the instructions end users need to operate the product, covering secure installation, initial hardening, account management, backup and restore, safe default settings, and warning banners. Together these give the end user everything they need to use the product correctly.
e) For sub-item (e): Explain the procedures available to the user for a factory reset, for purging selected data, and, where supported, for cryptographic erasure, including how to verify each of these completed successfully. Clear data-deletion instructions are needed both to meet privacy obligations and to support proper decommissioning of the product.
f) For sub-item (f): Supply configuration baselines together with the procedures for patching, updating, rotating keys, managing logs, taking backups, hooking into incident response, and synchronizing time. Taken together, this equips administrators with everything they need to keep the product running securely.

Documentation should describe how the mobile application uses platform-provided security primitives, the trust model between the application and its RDPS, and the security assumptions made about the underlying mobile operating system version. This documentation supports both internal security review and external assessment. OWASP MASVS-STORAGE and OWASP MASVS-CRYPTO provide a framework for what platform security service usage should be documented. OWASP MASTG provides test cases that can be cross-referenced against this documentation.

The protocol inventory should cover: application-layer protocols (HTTP/S, WebSocket, MQTT, gRPC, custom binary protocols); transport-layer protocols and versions (TLS 1.2, TLS 1.3); authentication protocols (OAuth 2.0, OpenID Connect, SAML); and any legacy or proprietary protocols. For each protocol, document: the version in use, the security properties applied (authentication, confidentiality, integrity), the cipher suites or algorithm parameters, and whether the protocol is enabled by default or optionally. Third-party SDKs often introduce undocumented protocol usage; static and dynamic analysis tools (OWASP MASTG network testing techniques) should be used to detect these. Align with OWASP MASVS-NETWORK.

Where TLS is used for sensitive communications, the inventory should also record whether certificate or public-key pinning is applied and, if so, the pinning and key-rotation strategy, given the operational trade-off between resistance to interception and the risk of denial of service if pinned keys are rotated without a corresponding application update.

See OpenCRE 820-877 at opencre.org/cre/820-877 for related resources and topics for guidance.

Requirement CR-ID: 6.6-CR-05

The product's technical documentation shall provide a detailed specification of all cryptographic mechanisms employed, including the algorithms used, their parameters, key sizes, operational modes, random generation methods, key lifecycle management, and policy of deprecation.

Source: REQ-CON-001(40000-10)

Guidance

The cryptographic specification should describe the cryptographic mechanisms used in the product in enough detail to support conformity checks and evaluation of the product's security position.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

The specification should also link to the security functions documented under 6.6-CR-04(c), where those functions rely on cryptography.

Requirement CR-ID: 6.6-CR-06

The product's technical documentation shall include an artefact - such as a coverage matrix - that explicitly links each identified risk to the security function or functions that address it.

Source: REQ-SBD-002 (40000-10)

Guidance

A matrix or equivalent structured artefact should be provided within the technical documentation, linking identified threats to the security functions implemented in the product, and indicating the degree of coverage for each threat. Maintaining such a coverage mapping prevents gaps in threat coverage.

NOTE: This requirement addresses the forward-looking demonstration of threat coverage within the product's technical documentation. It is distinct from the justification of accepted residual risks required by 5.7-CR-04, which concerns post-evaluation documentation of acceptance decisions. Both obligations apply and are complementary.

5.7 Cybersecurity Verification and Validation

Introduction

Cybersecurity Verification and Validation (V&V) confirms that a product's concept, design, and implementation meet every applicable cybersecurity requirement and that the controls put in place actually work. Rather than being a one-off check at the end of development, it recurs across the whole product lifecycle and is generally carried out again whenever the product is modified - for instance during maintenance work or once a newly found vulnerability has been resolved.

A range of testing techniques may be applied depending on the product's risk and design: functional, unit, integration, system, fuzz, stress, and penetration testing each address distinct aspects of security.

Output: Documentation of selected verification and validation approaches and their outcome.

See OpenCRE 433-442 at opencre.org/cre/433-442 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 6.7-CR-01

Verification and validation shall take key elements as input:

- the product implementation including relevant hardware, software, and remote data processing solutions;
- the technical documentation, together with user information and instructions;
- the cybersecurity requirements;
- the product cybersecurity context including relevant information about use from for example customer input and support cases;

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- the cybersecurity state-of-the art as described in publications, standards, and guidelines;
- the evolving threat landscape applicable to the product, including information on vulnerabilities found in similar products including components.

Source:

- Input clause 7.6 (40000-1-2)
- PRE-9-RQ-03 (40000-1-3)

Requirement CR-ID: 6.7-CR-02

The cybersecurity verification and validation process shall confirm that the product is sufficiently secure, meaning it satisfies the cybersecurity requirements established in 6.3 and the levels of the identified risks (see 5.5) meet the acceptance criteria (see 5.3).

Source:

- CLA-05-RQ-01 (40000-1-2) - but the subject is scoped from the security controls to the product
- CLA-05-RQ-02 (40000-1-2) – further specifying the role of risk assessment

Guidance

Cybersecurity analysis methods can be used to review implementation artefacts and check whether the intended cybersecurity controls have been implemented correctly and fully. These methods may include static and dynamic analysis, inspections, and peer reviews.

Functional testing can also be used to verify that the implemented product behaviour matches the defined cybersecurity requirements.

Traceability between cybersecurity requirements, implemented controls, and corresponding test cases can be maintained in a requirements traceability matrix (RTM) or equivalent artefact.

Requirement CR-ID: 6.7-CR-03

Threat scenarios and attack profiles shall be defined, documented, and used as the basis for validation testing, derived from the applicable attack potential level (e.g., AVA_VAN level), the risk assessment and the product's cybersecurity context . Each validation testing cycle, these shall be reviewed.

The validation testing shall include advanced penetration testing calibrated to the goal, and specialized techniques - including where applicable protocol robustness testing, deep fuzzing, verification of hardened configurations, testing of secure boot/attestation, assessment of hardware key protection, and verifying supply chain integrity.

A process for conducting these penetration tests shall be defined including: the scope of testing (including the mobile client, associated RDPS, and communication channels), the minimum qualifications required of testers, the testing methodology to be followed, and the criteria for determining when re-testing is required following remediation.

Source:

- CLA-05-RQ-02 (40000-1-2)
- REQ-KEV-009 (40000-10)
- SOTA

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

Penetration testing - involving purposeful attacks with varying levels of pre-existing knowledge - can provide evidence that the product can withstand threats identified in the risk assessment.

Threat scenarios used for validation should reflect the operational environment of the mobile application, including threats specific to mobile platforms such as malicious applications on the same device, rooted or jailbroken device environments, network-level adversaries (e.g., on untrusted Wi-Fi), physical device access, and abuse of platform inter-process communication (IPC) mechanisms.

The OWASP MASTG provides mobile-specific test scenarios that can be used to populate or cross-check the threat scenario inventory. For RDPS (remote data processing solutions) used by the mobile application, threat scenarios should additionally address server-side attack surfaces exposed via the mobile client. Scenarios should be reviewed and updated whenever the risk assessment is revised or new attack techniques relevant to the product's context are identified.

The penetration testing methodology should address mobile-specific attack surfaces such as defined in the OWASP MASTG, including but not limited to: local data storage security, inter-process communication (including URL scheme and deep link handling, and verification of Android App Links / iOS Universal Links), WebView security, binary protections, network communication, and authentication mechanisms. For RDPS, the methodology should additionally address API security testing (e.g., authentication, authorization, input validation, rate limiting). Testers should demonstrate familiarity with both iOS and Android platform security models, as applicable. Re-testing criteria should specify that all findings rated high or critical need to be re-tested after remediation before release. The organization should retain penetration test reports as evidence of V&V activities.

Requirement CR-ID: 6.7-CR-04

The V&V process shall validate that all cybersecurity risks associated with integrated components - including third-party software - have been identified and adequately addressed in the product's implemented design.

Source: CLA-05-RQ-05 (40000-1-2)

Guidance

Vulnerability scanning of third-party and integrated software components can help identify known vulnerabilities. Integration testing can further verify that the interaction between components does not introduce cybersecurity gaps that were not addressed during design.

Requirement CR-ID: 6.7-CR-05

A process shall be established for assessing supply chain integrity as part of cybersecurity V&V, including verification that the application binary and its dependencies are built from verified sources, that the build pipeline is protected against tampering, and that the deployed artefact matches the verified build output.

Source: SOTA

Guidance

Supply chain integrity assessment should include: verification that all source code and third-party dependencies are obtained from authenticated and integrity-verified sources (e.g., via

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

cryptographic hash verification or signed package repositories); verification that the build pipeline (CI/CD system) is protected against unauthorized modification (e.g., through access controls, audit logging, and pipeline configuration management); and verification that the application binary delivered to end users (via the app store or enterprise distribution) matches the binary produced by the verified build pipeline (e.g., via reproducible builds or post-build hash comparison). For Android applications, the organization should verify that the application signing key is protected in accordance with Google Play signing requirements or equivalent. For iOS applications, the organization should verify that code signing certificates and provisioning profiles are managed securely.

Requirement CR-ID: 6.7-CR-06

Where appropriate to the product's design, risk assessment, and cybersecurity context, the V&V process shall encompass key elements: artefact analysis including architecture review, error-handling and input validation, external interface and protocol assessment (including deprecation and encryption/integrity checks), additional security testing, documentation review, and risk treatment alignment verification. See guidance for these key elements.

Source:

- CLA-05-RQ-03 (40000-1-2)
- REQ-EMM-001 (40000-10)
- SOTA

Guidance

- **Artefact analysis (a):** Both manual review and automated tools (e.g., static analysis) can be applied in analysis to confirm fulfilment of cybersecurity requirements. Artefacts include code, configuration, and architecture documentation .
- **Error handling and input validation (b):** Fuzz testing - subjecting the product to unexpected, random, or invalid inputs - can reveal crashes, memory leaks, or unexpected behaviour caused by inadequate input handling.
- **External interfaces and protocols (c):** Integration testing can identify cybersecurity gaps arising from component interactions. For protocol assessment, retrieve the protocol inventory identified in accordance with CR-ID: 6.6-CR-04. Check that none of the protocols in use is deprecated or known to be vulnerable. Confirm that each protocol provides secure transmission, including encryption and integrity checks. Vulnerability scanning tools can assist in detecting known protocol weaknesses. For RDPS APIs, the assessment should additionally verify authentication token handling, input validation at API boundaries, and correct implementation of authorization controls
- **Additional security testing (d):** Running dynamic testing tools, penetration testing and stress testing (to surface denial-of-service vulnerabilities or inefficient resource handling) are applicable techniques.
- **Documentation review (e):** A test strategy document covering what, when, and how to test can serve as a basis for assessing accuracy and completeness of cybersecurity documentation.
- **Risk treatment alignment (f):** Traceability between identified risks, their treatments, the implemented cybersecurity requirements, and the verification thereof should be established and verified.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 6.7-CR-07

A process shall be established for selecting, configuring, and maintaining static application security testing (SAST) tools and dynamic application security testing (DAST) tools appropriate for the mobile platform(s) in scope (iOS, Android, or cross-platform), and the rationale for tool selection relative to the product's technology stack and cybersecurity requirements shall be documented.

Source: SOTA

Guidance

For Android applications, SAST tools may need to be capable of analyzing Java/Kotlin bytecode and native code (e.g., via APK analysis). For iOS applications, tools may need to support analysis of Swift and Objective-C source and binaries. For cross-platform frameworks (e.g., React Native, Flutter), the organization should ideally confirm that selected tools cover both the framework layer and the underlying platform code. Tool configurations should be reviewed at least annually and upon significant changes to the technology stack.

The OWASP MASTG identifies specific tool categories and example tools relevant to mobile SAST and DAST. Tool outputs should be reviewed by qualified personnel; automated findings should not be accepted or dismissed without human review.

Requirement CR-ID: 6.7-CR-08

Products shall undergo code review conducted by suitably qualified reviewers who are independent of the code's authors; the review scope shall encompass at least misuse patterns and all critical findings shall be remediated prior to release.

Source: REQ-KEV-010 (40000-10)

Guidance

Conduct the review using qualified personnel independent from the authors (who may belong to the same organization). The review scope may include constant-time evaluation, and unit/integration test coverage.

Define and document the qualifications, independence criteria, and review scope requirements for personnel conducting code reviews. Qualification criteria should specify: relevant security-focused training or certification (e.g., familiarity with CERT Secure Coding Standards for the applicable language - SEI CERT C, CERT C++, or CERT Java/Android as applicable), demonstrated experience with mobile platform security models, and familiarity with the vulnerability classes relevant to the product's technology stack. Independence criteria should specify that the reviewer was not the primary author of the code under review; reviewers from the same organization are permissible provided the independence criterion is met. Review scope documentation should confirm that the review addressed: adherence to secure coding standards, misuse patterns relevant to the product's threat model, constant-time implementation of security-sensitive operations (e.g., cryptographic comparisons, PIN verification), and the adequacy of unit and integration test coverage for security-relevant code paths. Records should be retained as evidence of V&V activities.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 6.7-CR-09

The V&V process shall document and identify all test methods and selected test tools for cybersecurity V&V activities, including the rationale for their selection relative to the product's risk profile and design, and any deviations from the planned test scope together with their justification.

Source:

- CLA-05-RQ-06 (40000-1-2)
- SOTA

Guidance

A test strategy document can be used to record the selected methods (e.g., tools, techniques such as fuzzing, penetration testing, static analysis) alongside the rationale for their selection relative to the product's risk profile and design. This documentation supports traceability, internal and external review, and continuous improvement of V&V activities.

Requirement CR-ID: 6.7-CR-10

Cybersecurity V&V activities shall recur throughout the product lifecycle in alignment with the vulnerability management activities described in 6.9 and shall not be limited to final development stages.

For this purpose, a documented schedule for recurring cybersecurity V&V activities shall be established that specifies, at minimum, the trigger conditions for re-testing (e.g., new release, significant code change, newly disclosed vulnerability affecting a component, change in threat landscape) and the V&V activities required for each trigger type.

Source:

- CLA-05-RQ-04 (40000-1-2)
- SOTA

Guidance

V&V activities should be planned to recur throughout the product lifecycle - not only at final development stages - including after maintenance activities, resolution of newly uncovered vulnerabilities, or substantial product modifications.

Trigger conditions should be defined in a V&V policy or test strategy document and should include: (a) each planned product release; (b) any change to security-relevant components, including third-party libraries or RDPS components; (c) disclosure of a CVE or equivalent vulnerability affecting a component integrated into the product; and (d) a defined maximum interval (e.g., annually) even in the absence of other triggers. For mobile applications, the organization should additionally consider platform-level changes (e.g., new iOS or Android major version releases) as a trigger for re-assessment of platform-dependent security controls.

The OWASP MASTG recommends continuous or release-gated security testing as part of a mobile DevSecOps pipeline.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 6.7-CR-11

A security test and review plan shall be developed that is grounded in the product's context, its cybersecurity architecture and design, the defined cybersecurity requirements for the product, the results of the risk assessment, and the results of tests and reviews. The plan shall define what tests and reviews are to be performed, what methodologies to apply, how often, and at what intervals, calibrated to the risk profile associated with the product's intended use.

Source:

- PRE-9-RQ-01 (40000-1-3)
- PRE-9-RQ-02 (40000-1-3)
- PRE-9-RQ-04 (40000-1-3)

Guidance

The plan may cover a class of products or an entire portfolio where that scope is appropriate. How frequently tests and reviews are conducted should reflect where the product is in its lifecycle, any shifts in the risk environment or threat landscape, and lessons drawn from security incidents.

The inputs to security testing are dynamic and may change over time. Test cases and methodologies should be reviewed and updated as technology advances and as the understanding of relevant vulnerabilities and threats develops, so that the plan continues to reflect the current security landscape.

5.8 Secure Production and Distribution

Introduction

Secure production and distribution activities manage cybersecurity risks from the point of production through to market placement. For digitally distributed software, this means protecting the integrity and authenticity of software artefacts (including information and instructions) both in transit and at rest – protecting against manipulation by external actors.

A secure production control plan is a practical tool to support these activities. It typically captures cybersecurity-relevant production instructions, measures to prevent unauthorized alteration (addressing physical access, cryptography, and access controls), and methods to confirm the product is produced in accordance with its cybersecurity requirements.

Output: software distribution artefacts, documentation of measures used to protect the authenticity and integrity of the artefacts – in transit and at rest, plus documentation how information and instructions to the user are made accessible.

See OpenCRE 473-177 at opencre.org/cre/473-177 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 6.8-CR-01

Software products and software updates that are distributed as software images or other distribution artefacts shall be protected against manipulation throughout the entire distribution lifecycle, covering both network transit and storage at rest. For this purpose, a

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

documented build and release pipeline shall be maintained, including automated integrity controls and verification at defined points in the pipeline, including compilation, packaging, signing (conformant to 6.8-CR-05), and release or upload to the distribution channel.

Source:

- CLA-06-RQ-01 (40000-1-2)
- PRE-10-RQ-01 (40000-1-3)
- RLS-1-RQ-04 (40000-1-3)
- SOTA (requiring a documented standardized pipeline process)

Guidance

Consider using integrity controls for distribution artefacts, such as cryptographic hashes or digital signatures, so that any unauthorized modification can be identified whether it happens in transit across a network or while the artefacts are stored or hosted. Assessing the cybersecurity of the digital distribution channel, for example an app store or a manufacturer's download site, can support a determination of whether the hosting environment is appropriate and can reveal issues to be addressed through the product cybersecurity risk assessment.

Consider implementing a CI/CD pipeline (e.g. using GitHub Actions, GitLab CI, Fastlane, or Bitrise) in which each stage produces a cryptographic hash (e.g. SHA-256) of the artefact and compares it against the hash of the input to that stage. The pipeline should fail and alert on any mismatch. Pipeline configuration files themselves should be version-controlled and protected against unauthorized modification.

Requirement CR-ID: 6.8-CR-02

Where justified by the product's risk assessment and cybersecurity context, the production and distribution activities for digital software products shall incorporate access authentication.

Source: CLA-06-RQ-02 without the authenticity overlap already covered in CLA-06-RQ-01 (40000-1-2)

Guidance

Which measures are suitable should be decided based on the product's cybersecurity risk assessment. Multi-factor authentication is also a typical control used to limit access to protected areas of a hosting platform. If the risk assessment indicates that the risk is lower, it may be adequate to implement only some of these measures.

Requirement CR-ID: 6.8-CR-03

Where applicable, user-facing information and instructions distributed digitally shall be protected against manipulation or unauthorized disclosure during distribution, including protection of the communication channels through which they are delivered.

Source: CLA-06-RQ-03 (40000-1-2)

Guidance

Digitally distributed user documentation-such as manuals, safety information, and configuration instructions-should be treated as part of production and distribution processes. Organizations should consider protecting this material with the same authenticity and integrity safeguards applied to software artefacts and should ensure that the delivery path used to provide it (for example, a manufacturer website or an in-product update channel) is evaluated for cybersecurity risk.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 6.8-CR-04

Where applicable, information and instructions intended for the user shall be delivered and presented in a manner that is accessible to the intended user population.

Source: CLA-06-RQ-04 (40000-1-2)

Guidance

Accessibility covers both:

- technical access - the distribution channel should remain available to users and should not be limited in a way that blocks them from receiving the information; and
- usability - the information should be presented in a format and language suitable for the intended audience.

Requirement CR-ID: 6.8-CR-05

A code-signing process shall be established and maintained for mobile application distribution artefacts that defines:

- the lifecycle management of signing credentials, including Android signing keys/keystores and iOS distribution certificates and provisioning profiles, as applicable;
- the roles authorized to approve and perform signing operations; and
- the conditions under which signing is permitted.

Signing keys used for Android (keystore) or iOS (provisioning profiles and certificates) shall be stored in a secrets management system (e.g. HashiCorp Vault, AWS Secrets Manager) and not in the repository.

Source: SOTA

Guidance

The signing process should specify approved key generation parameters in accordance with the ENISA "Agreed Cryptographic Mechanism" guidance, storage requirements (e.g. HSM or equivalent managed key service), rotation schedules, expiry monitoring, backup and recovery arrangements where permitted, and revocation procedures.

For Android, the organization should consider enrolling in Google Play App Signing so that Google manages the app signing key while the organization retains control of the upload key.

For iOS, the organization should document the management of Apple Developer Program accounts, certificate and profile expiry monitoring, and the process for renewal or revocation.

Production signing and release should be subject to multi-person approval, and access to signing credentials should be restricted to authorized personnel and systems.

Mobile application signing keys, including Android app signing keys/keystores and iOS distribution certificates and provisioning profiles, are high-value cryptographic assets. If compromised, an attacker may be able to distribute malicious applications that appear to originate from the organization, subject to platform-specific controls. These assets should be protected using HSMs, secure enclaves, or other hardware-backed key management systems where feasible, with strict access control, auditing, and separation of duties. organization

Requirement CR-ID: 6.8-CR-06

Multi-factor authentication (MFA) and role-based access controls shall be enforced for all accounts with the ability to publish, update, or manage mobile application releases on

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

distribution platforms (e.g. Google Play Console, Apple App Store Connect), and an access review process shall be maintained for these accounts.

Source: SOTA

Guidance

Access reviews should be conducted at least annually or upon personnel changes. Accounts should follow the principle of least privilege; for example, testers may require access to internal testing tracks but should not have production release rights. Service accounts used by automated pipelines should use short-lived credentials or API keys with restricted scopes rather than full administrative access. Orphaned accounts (e.g. for former employees or contractors) should be revoked promptly. Audit logs from the distribution platform should be retained and reviewed periodically for anomalous activity.

Requirement CR-ID: 6.8-CR-07

The product shall be made identifiable by recording, at minimum, the manufacturer's name, the product name, and a version for recognizability and traceability to support for example vulnerability handling, down-stream software bill of materials (SBOM) generation and verification, and vulnerability information sharing and reporting.

Source: PRE-6-RQ-01 (40000-1-3) – with version made mandatory

Guidance

The mandatory identification fields listed in the requirement can be supplemented with additional identifiers. Appropriate identifiers include release version, build number, Software Hash Identifier (SWHID), and release date. One or more of these may be used as needed.

Requirement CR-ID: 6.8-CR-08

A communication mechanism shall be provided through which security-related information - including advisories, release notes, installation guidance, and notifications - is made available for the product.

Source: PRE-10-RQ-02 (40000-1-3)

Guidance

Appropriate mechanisms for distributing security information may include a dedicated product security page, mailing lists, RSS feeds, or a vendor portal. Through whichever channel is chosen, advisories, release notes, installation guidance, and security notifications should be made accessible to affected users in a timely manner.

Requirement CR-ID: 6.8-CR-09

Where the product type, connectivity, and operational context make it feasible, a mechanism enabling security updates to be distributed automatically or semi-automatically shall be provided.

Source: PRE-10-RQ-03 (40000-1-3)

Guidance

Where the product's architecture and its intended deployment environment permit, an automatic or semi-automatic update mechanism should be considered. Such a mechanism would allow security updates to be delivered to, or retrieved by, the product without the need for manual action. Whether this is applicable will be determined by factors including product type, network connectivity, and the operational context in which the product is used.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

5.9 Product Cybersecurity Monitoring and Issue Management

Introduction

Cybersecurity issues encompass vulnerabilities and incidents affecting a product and its related dependent products and services (RDPS) throughout the product lifecycle. Monitoring the threat landscape is essential to detect new vulnerabilities and respond to changes before they result in incidents. This monitoring typically involves identifying, receiving, and processing cybersecurity-related information from both internal and external sources - including vulnerability databases, lifecycle status of third-party components, end-of-support notices, cybersecurity laboratories, and market surveillance authorities - whether through manual or automated means. Issue management complements monitoring by ensuring that identified issues are handled and resolved, forming a key pillar of ongoing product maintenance.

Output: documentation of the activities undertaken including time aspects, and results of any assessments.

See OpenCRE 888-770 at opencre.org/cre/888-770 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 6.9-CR-01

Periodic procedures, automated where possible, shall be performed for monitoring of internal and external information that may affect the product's risk assessment as defined in 5.4 to 5.7, covering at least cybersecurity incidents and vulnerabilities, at intervals that are justifiable given the product context. Documentation shall include activities, frequency, sources, and the roles responsible for execution and review.

Source:

- CLA-08-RQ-01 (40000-1-2)
- RCP-2-RQ-01 (40000-1-3) (internal and external, where possible automate)
- RCP-3-RQ-01 (40000-1-3)
- SOTA (Documented procedure and automated where possible)

Guidance

Monitoring can involve reviewing vulnerability databases, notices that integrated components have reached end of support, and other sources of vulnerability reporting. Relevant information may also be obtained from cybersecurity laboratories, comparable products available on the market, and market surveillance authorities.

Automation is important for minimizing the likelihood of missed vulnerabilities and to ensure timely identification of new threats.

The sources may include NVD, vendor advisories, OS platform security bulletins for iOS and Android, OWASP dependency vulnerability feeds, Google Android Security Bulletins, Apple Platform Security updates, and advisories from cross-platform framework vendors (e.g., React Native, Flutter). Automated tooling (e.g., software composition analysis tools integrated into CI/CD pipelines) may be used to supplement manual monitoring. The

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

procedure should be reviewed annually, or more frequent, or upon significant changes to the product's technology stack.

Requirement CR-ID: 6.9-CR-02

The risks of verified cybersecurity incidents, changes in the threat landscape, and discovered vulnerabilities shall be assessed aligned with the risk assessment methodology established under 5.4 to 5.7.

Source:

- CLA-08-RQ-02 (40000-1-2)
- CLA-08-RQ-03 (40000-1-2)
- SOTA (guidance on automation)

Guidance

Aligning the assessment with the risk assessment approach employed during product development ensures that the severity and impact of newly identified issues are evaluated consistently within the product's established risk context.

Where possible analysis steps should be automated as much as possible, to allow for timely action. Ideally, procedures are established that use defined exceptions where manual steps are required.

Requirement CR-ID: 6.9-CR-03

Upon discovery of a new vulnerability, documentation of that vulnerability shall be produced and communicated to relevant parties where the risk assessment and cybersecurity context make such communication appropriate.

Source: CLA-08-RQ-04 (40000-1-2)

Requirement CR-ID: 6.9-CR-04

Verified cybersecurity incidents and discovered vulnerabilities shall be treated in a timely manner, with the urgency and nature of treatment proportionate to the risk assessment outcome and the specific cybersecurity context of the product.

Source: CLA-08-RQ-05 (40000-1-2)

Guidance

Treatment decisions should align with the results of the risk assessment. The required response, including how quickly action is needed and what form it should take, may differ according to the seriousness of the vulnerability or incident and the product's particular cybersecurity context. As reflected in relevant standards, regular testing and review can help enable timely treatment.

Requirement CR-ID: 6.9-CR-05

Where cybersecurity incident or vulnerability have residual risk, that risk shall be communicated to stakeholders using the communication processes and channels established under Clause 5.9, where relevant.

Source: CLA-08-RQ-06 (40000-1-2)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 6.9-CR-06

At a minimum, the following designated internal and external sources shall be drawn upon when monitoring for vulnerabilities: the EU Vulnerability Database, externally reported vulnerabilities, outputs from regular testing, and regular review activities.

Source: RCP-2-RQ-02 (40000-1-3)

Guidance

The items listed here should be treated as the minimum starting point. Organizations are encouraged to draw on other information sources where these are relevant to the systems they use or the threats they face, for example supplier-issued security notices or threat intelligence tailored to their sector.

5.10 Secure Decommissioning

Introduction

Secure decommissioning planning ensures that when a product - including its Remote Data Processing Solutions (RDPS) - changes ownership or reaches end of life, user assets are not compromised. This encompasses the secure deletion of user data, settings, and cryptographic keys, as well as restoring the product to a secure default state.

When a product and its associated RDPS reach the end of their support period, manufacturers may have obligations to inform users about this transition and its implications for continued use. Such communications need to be clear, simple, and accessible. Planning for decommissioning therefore extends beyond the product's active life, covering manufacturer responsibilities at and after end-of-support.

It is worth noting that an RDPS may be integrated into multiple products; decommissioning focuses on appropriate removal of user data in context. Additionally, only authorized users - as determined by product context - may perform decommissioning or factory reset operations.

Output: documented communication method of decommissioning, documented rationale, documented activities for decommissioning permissions, user instructions for decommissioning – if any.

See OpenCRE 424-242 at opencre.org/cre/424-242 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 6.10-CR-01

Secure decommissioning shall be prepared by identifying cybersecurity aspects of decommissioning, all confidential assets requiring deletion and their location, establishing appropriate actions for any third-party-operated components, defining the method of user communication and what that communication needs to include, and documenting all manufacturer-side activities required to achieve secure decommissioning.

Source: CLA-09-RQ-01 (40000-1-2)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

When planning for secure decommissioning, manufacturers should identify the logical locations of all confidential assets within the product and any related RDPS, including user data, configuration settings, and cryptographic keys. Because an RDPS may support more than one product, the decommissioning process should address removal of user data only where that is appropriate in the context of the product. In some cases, decommissioning the product should include deletion of user data stored on the RDPS; in others, it should not. In all cases, it is considered best practice to tell users how to remove their data securely.

If third parties operate any part of the product, suitable contractual or technical measures should be in place so that those elements can also be securely decommissioned.

The method used to notify users about decommissioning - for example, through the product, by email, or in documentation - should be appropriate to the product context and intended users. Where a product is approaching the end of its support period, it is considered best practice to explain, in clear, simple, and accessible language, the consequences of continuing to use it.

Decommissioning, or restoring the product to a secure default state, should be performed only by authorized users. Which users are authorized depends on the product context, and not all users will necessarily have that authority.

Manufacturers should have a process that ensures the information for the prepared decommissioning is kept up to date.

Requirement CR-ID: 6.10-CR-02

Where user-facing decommissioning instructions are required, those instructions shall address, as applicable: removal and export of user data, removal of security-relevant configuration data, disconnection from the operational environment, secure disposal of the product, and advance notice of any automated data deletion including its scope and timing.

Source: CLA-09-RQ-02 (40000-1-2)

5.11 Third-Party Component Cybersecurity Management

Introduction

Third-party components - whether commercial, free, or open-source - can introduce cybersecurity risks that compromise the integrity of a product. Managing these risks requires due diligence throughout the component lifecycle: from selection and integration through to end-of-life. Key considerations include evaluating a component's intended purpose, its compliance with legal and cybersecurity requirements, its support status, and the maturity of its vulnerability handling practices. Manufacturers are advised to align responsibilities with their suppliers before bringing a product to market, and to account for the distinct nature of open-source components, where formal support arrangements may not be available but source code transparency offers alternative assessment opportunities. Information sharing about discovered vulnerabilities - including contributing fixes upstream - supports collective cybersecurity improvement and helps prevent fragmentation of the FOSS ecosystem.

Output: evidence that the relevant activities have been performed.

See OpenCRE 613-285 at opencre.org/cre/613-285 for related resources and topics for guidance.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirements

Requirement CR-ID: 6.11-CR-01

Before selecting and integrating any third-party component into a product, due diligence shall be carried out on a number of aspects when applicable. This shall include verifying alignment of the component's intended purpose with its planned use in the product, confirming the absence of known vulnerabilities, and determining whether additional cybersecurity testing is needed. For commercial components, the availability of CE marking and an EU Declaration of Conformity shall be checked. For FOSS components, assessment shall be performed of maintenance activity, availability of a vulnerability disclosure process, stewardship by a recognized organization, evidence of cybersecurity-by-design practices, and availability of security updates. In addition, license obligations shall be identified, documented, and managed prior to integration and throughout the component lifecycle.

Source:

- CLA-10-RQ-01 (40000-1-2)
- SOTA (licenses)

Guidance

To confirm that no known vulnerabilities are present, it may be appropriate to consult public vulnerability databases, including the European vulnerability database created under Article 12(2) of Directive (EU) 2022/2555. Further cybersecurity testing can also involve methods such as binary analysis, source code scanning, rebuilding from source, and code review. In choosing components, take account of the length of their support lifecycle so that risks linked to deprecated components or outdated technologies can be foreseen.

License evaluation should be performed as part of the due diligence process and should cover both direct and transitive dependencies. The procedure should identify license types (e.g., GPL, LGPL, MIT, Apache 2.0) and assess compatibility with the product's distribution model (e.g., proprietary app distributed via app stores). For FOSS components, the procedure should assess whether copyleft obligations could affect the mobile application's source code distribution requirements. SPDX license identifiers may be used to standardize license recording in the SBOM.

Requirement CR-ID: 6.11-CR-02

Both the third-party component itself and the manner in which it is integrated into the product shall be addressed within the risk assessment and risk treatment activities required by Clause 5.

Source: CLA-10-RQ-02 (40000-1-2)

Guidance

The risk assessment should consider how the third-party component is incorporated and used within the product, rather than evaluating the component solely on its own.

Requirement CR-ID: 6.11-CR-03

Third-party components and their integration into the product shall be included in verification and validation specified in clause 6.7.

Source: CLA-10-RQ-04 (40000-1-2)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 6.11-CR-04

Ongoing monitoring of third-party components shall be maintained for the duration of the product's lifecycle, so that vulnerabilities relevant to the product can be identified, in line with the monitoring activities set out in clause 6.9. This is a continuous obligation and does not end once initial integration is complete.

Source: CLA-10-RQ-05 (40000-1-2)

Guidance

Monitoring is to continue throughout the entire product lifecycle, rather than being limited to the initial integration stage.

Requirement CR-ID: 6.11-CR-05

Where a vulnerability is discovered in a commercial third-party component, the vulnerability shall be documented, disclosed to the responsible third-party, and remediated following the applicable vulnerability disclosure and handling procedures. The responsible third-party may be a supplier, service provider, or any party capable of facilitating handling of the vulnerability.

Source: CLA-10-RQ-06 (40000-1-2)

Guidance

Newly identified vulnerabilities should be reported to the appropriate third party responsible for addressing them. This could include a supplier, a service provider, or another party able to support the vulnerability handling process. Relevant parties may put information-sharing arrangements in place through formal agreements, such as a coordinated vulnerability handling process. Section

Requirement CR-ID: 6.11-CR-06

Where the manufacturer discovers a vulnerability in a FOSS component and develops a fix, that fix shall be communicated to the open-source project concerned. Where it is possible to do so, the fix shall also be contributed upstream to the original project, under the terms of the applicable source code license.

Source: CLA-10-RQ-07 (40000-1-2)

Guidance

Contributing fixes back to the original open-source project can be used as a legitimate way to address risk, especially in later versions of the product. Providing the fixes that were developed, or documentation describing those fixes, promotes transparency, contributes to broader cybersecurity improvement, and reduces the risk of fragmentation across the FOSS ecosystem.

Requirement CR-ID: 6.11-CR-07

Third-party component suppliers shall be assessed for maintenance activity (level of support or having reached end-of-support) on an annual basis.

A documented policy shall be established and maintained to define the maximum permissible period between the public disclosure of a vulnerability in a third-party component and the release of a remediated version or the implementation of an accepted compensating control, differentiated by vulnerability severity.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

If a supplier fails to meet the timeframe or support is below the documented threshold, a risk assessment shall be performed on the potential consequences of this support issue, which may lead to eventually deprecating the corresponding component(s).

Source:

- RCP-2-RQ-04 (40000-1-3)
- SOTA (assess supportability and timeframes)

Guidance

Where open-source components lack a declared end-of-support date, organizations should assess ongoing maintenance activity as a practical substitute. Indicators such as latest release version, recent commits, responsiveness to reported issues, and active community participation can serve as evidence that a project remains supported.

Remediation timeframes may be aligned with recognized frameworks such as CISA's Known Exploited Vulnerabilities (KEV) catalogue examples or the organization's own risk acceptance criteria. Example differentiation: critical vulnerabilities (CVSS ≥ 9.0) within 14 days; high vulnerabilities (CVSS 7.0–8.9) within 30 days; medium vulnerabilities within 90 days. For mobile applications, the policy should account for the additional lead time required for app store review processes (e.g., Apple App Store, Google Play Store) when calculating remediation windows. Where a patch is not yet available, the policy should require documented risk acceptance or the application of compensating controls (e.g., feature flag disablement, server-side mitigation). NIST SP 800-218 (SSDF) RV.2.2 reference remediation timeframe policies.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

6 Vulnerability Handling

6.1 Operational Security of Vulnerability Handling

Introduction

Information in vulnerability handling is inherently sensitive, as it can be exploited by malicious actors. Both internal processes and external communications therefore need to incorporate operational security measures throughout the vulnerability handling lifecycle. These controls may be lifted once remediation and advisory information have been made public.

Output: documented operational security measures.

Requirements

Requirement CR-ID: 7.1-CR-01

Operational security measures shall be maintained across all activities involving the receipt and communication of vulnerability information or reports.

Source:

- PRE-3-RC-01 (40000-1-3)
- PRE-5-RC-01(CVD) (40000-1-3)
- PRE-5-RC-02(CVD) (40000-1-3)

Guidance

Implementing operational security controls should not harm accessibility. Organizations should keep submission mechanisms open and usable, and where appropriate, provide the option for anonymous reporting.

Appropriate technical controls for achieving confidentiality and integrity include HTTPS-protected web forms and encrypted or digitally signed email using S/MIME or OpenPGP. Further implementation guidance can be found in EN ISO/IEC 29147:2020, section 5.8.

Where sensitive material is involved - such as exploit code, credentials, or configuration data - the organization should transition the exchange to a secure channel regardless of the medium through which first contact was made.

Further guidance is available in EN ISO/IEC 29147:2020, section 6.7.

Requirement CR-ID: 7.1-CR-02

Access to vulnerability information shall be restricted, when it has not yet been publicly disclosed, where applicable, to only those individuals who require it in order to fulfil their responsibilities within the vulnerability handling process.

Source: PRE-3-RQ-01 (40000-1-3)- but access restriction made mandatory instead of considered

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

Non-public vulnerability information should be made available only to those with a demonstrated need to access it as part of their role in handling the vulnerability. Applying this principle reduces the likelihood of accidental or premature disclosure. Further guidance is provided in EN ISO/IEC 30111:2020, section 7.3.

6.2 Facilities for Vulnerability Handling

Introduction

A vulnerability handling policy is an internal framework that establishes how an organization identifies, assesses, investigates, and remediates security vulnerabilities in its products or systems. It helps ensure that vulnerabilities are managed in a consistent, timely, and coordinated way across teams. A clear policy supports effective security practices, improves response to newly discovered issues, and helps maintain alignment between internal processes and external vulnerability disclosure efforts.

Output: documented vulnerability handling policy and its implementation in the form of facilities.

See OpenCRE 732-148 at opencre.org/cre/732-148 for related resources and topics for guidance.

Requirements

Requirement CR-ID: 7.2-CR-01

A vulnerability handling policy shall be established, implemented, and followed.

Source: PRE-1-RQ-01 (40000-1-3)

Guidance

To help the vulnerability handling process operate effectively, consider establishing an organizational framework that gives clear ownership and accountability for the related activities.

Requirement CR-ID: 7.2-CR-02

The vulnerability handling policy shall describe the organization's overall direction, principles, and responsibilities for handling potential vulnerabilities in products; set out how information about those vulnerabilities will be safeguarded against disclosure before remediation is available; establish a planned timeframe for remediation development; and explain the approach to the regular testing and review activities defined in 6.7.

Source: PRE-1-RQ-02 (40000-1-3)

Guidance

When applying this requirement, the policy should be made more robust by addressing the following:

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

- Describe the end-to-end process in a way that is consistent with broader vulnerability management expectations and clearly assign responsibilities for managing suspected vulnerabilities.
- Ensure that safeguards against early disclosure are consistent with the coordinated disclosure requirements.
- In setting a target remediation timeline, take into account the embargo period, including how it may be affected by coordination complexity with upstream stakeholders, the vulnerability's severity, and the characteristics of the product. This timeline is intended to guide remediation development and should reflect factors such as implementation difficulty and evaluated risk.
- Where feasible and suitable, identify downstream stakeholders that use the in-scope product. Whether this is suitable may depend on privacy or confidentiality obligations.
- Provide a mapping of upstream stakeholders to support the component identification activities.

Requirement CR-ID: 7.2-CR-03

Continuous monitoring shall be in place whether the vulnerability handling process is operating effectively.

Source: PRE-1-RQ-03 (40000-1-3)

Guidance

Consider establishing concrete, measurable indicators or metrics that enable evaluation whether the vulnerability handling process is achieving its intended outcomes. EN ISO/IEC 30111:2020, clause 7.2 offers further direction on how to approach effectiveness monitoring.

Requirement CR-ID: 7.2-CR-04

The vulnerability handling policy shall support all activities defined in the vulnerability disclosure policy described in 7.3

Source: PRE-1-RQ-05 (40000-1-3)

Guidance

During the drafting or periodic review of the vulnerability handling policy, confirm that every activity prescribed by the coordinated vulnerability disclosure policy (5.3.3) is either directly addressed or actively supported by the internal policy. Maintaining this alignment ensures that internal operational processes and external disclosure commitments are coherent and reinforce one another.

Requirement CR-ID: 7.2-CR-05

A documented process shall be established for evaluating, approving, and recording decisions to delay full vulnerability publication under the conditions specified in 7.7-CR-05, including defined criteria for the risk evaluation, designated approval authority, maximum permissible delay duration, and a procedure for communicating the disclosure date to affected users of the mobile application.

Source: SOTA

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

Having this process for this decision, adds the procedural controls necessary to exercise the permission in a trusted, consistent, and auditable manner – even under high time pressure when the necessary decision expertise may not be available.

The evaluation defined in the process should be conducted by a cross-functional group including security, legal, and product management representatives. For mobile applications, the process should account for the time required for app store review and deployment when determining whether a delay is justified and when setting the public disclosure date. The record of the evaluation and approval decision should be retained as evidence. EN ISO/IEC 29147:2020, Clause 7.5, provides guidance on timing of disclosure and conditions under which delay may be appropriate.

6.3 Coordinated Vulnerability Disclosure Facilities

Introduction

Coordinated vulnerability disclosure (CVD) involves a policy that communicates a manufacturer's intentions, responsibilities, and expectations around vulnerability disclosure. It covers both two-party coordination (between reporter and manufacturer) and multi-party scenarios involving multiple stakeholders. The policy is published externally, while supporting internal processes are established to effectively coordinate disclosure activities.

A key principle underpinning CVD is the use of an embargo period: reporters notify manufacturers privately and withhold public disclosure until a fix is available. The stages of receipt, verification, and remediation development take place within this embargo, ensuring vulnerabilities are handled securely and responsibly by all parties involved.

Output: documented CVD policy and its implementation in the form of facilities.

Requirements

Requirement CR-ID: 7.3-CR-01

A coordinated vulnerability disclosure policy shall be established, implemented, followed, and made publicly available in an accessible form

Source: PRE-2-RQ-01 (40000-1-3)

Guidance

When making the CVD policy publicly available, accessibility standards should be taken into account to ensure the policy can be reached and used by the widest possible audience. EN 301 549 v3.2.1 provides applicable requirements and advice on accessibility.

Requirement CR-ID: 7.3-CR-02

The CVD policy shall include contact mechanisms accessible through multiple sensory modalities, ensuring users with diverse impairments are not excluded.

Source: PRE-2-RC-01 (40000-1-3)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

Supporting more than one sensory channel ensures that individuals with particular impairments are not prevented from using the available contact mechanisms. As an illustration, a person with a writing impediment who cannot use a web form or e-mail could instead use a telephone number to both request and supply information. EN 301 549 v3.2.1 provides relevant accessibility requirements and advice.

Requirement CR-ID: 7.3-CR-03

The CVD policy shall explicitly set out what parties can expect with respect to ongoing communication throughout the vulnerability disclosure process.

Source: PRE-2-RQ-03 (40000-1-3)

Guidance

The detail underpinning what ongoing communication expectations should cover is addressed within the vulnerability handling process context. Section 7.5 provides further elaboration on the specific communication expectations that should be reflected in the policy.

Requirement CR-ID: 7.3-CR-04

The CVD policy shall address each of the following areas: the expected contents of a vulnerability report; options for secure communication; the scope of the program; publication arrangements; and recognition of reporters.

Source: PRE-2-RC-02 (40000-1-3)

Guidance

The purpose of a vulnerability report is to help understand, judge, replicate and solve the issue. Typical contents are contact information, product identification, description, replication procedure, any artefacts such as screenshots, description of the effect and how serious it is.

Further elaboration on the recommended elements to include in a vulnerability disclosure policy can be found in EN ISO/IEC 29147:2020, clause 9.3.

Requirement CR-ID: 7.3-CR-05

A disclosure process shall be established so that details about a vulnerability are not made public until the vulnerability has been remediated.

Source: PRE-2-RC-03 (40000-1-3)

Guidance

Disclosure strategies should be applied with flexibility, as no single approach is universally appropriate. The content of reports, agreed timelines, and the nature of responses can all be adapted to the specifics of each case, with agreement reached among all parties involved. Embargo durations are not fixed and may be negotiated individually between the manufacturer and the reporter, or through a coordinator where one is engaged.

Additional guidance on embargo periods is available in EN ISO/IEC 29147:2020, clause 5.6.8, and on disclosure strategy in ISO/IEC TR 5895:2022, clause 7.3.2.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

---

Requirement CR-ID: 7.3-CR-06

Secure communication mechanisms for vulnerability disclosure shall be made known to reporters and stakeholders.

Source: PRE-5-RQ-01-RE (40000-1-3)

Guidance

Reporters and stakeholders should be actively informed of the secure communication channels available to them. Although the provision of such channels is mandatory, their adoption by the reporter cannot be compelled. Secure communication should be maintained throughout the entire vulnerability handling lifecycle, not merely at the point of initial receipt.

Requirement CR-ID: 7.3-CR-07

The vulnerability reporting process shall include an option that allows reporters to submit information without disclosing their identity.

Source: PRE-5-RC-03 (40000-1-3)

Guidance

Providing an anonymous submission route - for example, an unauthenticated web form - reduces the threshold for reporters who may be hesitant to identify themselves. This increases the likelihood that vulnerabilities are reported and thereby strengthens the overall effectiveness of the disclosure program.

Requirement CR-ID: 7.3-CR-08

Security controls applied to communication channels shall not create unreasonable barriers that prevent external parties from contacting the organization.

Source: PRE-5-RC-04 (40000-1-3)

Guidance

The selection of secure communication mechanisms should balance security objectives against usability for external stakeholders. Controls that are disproportionately restrictive risk discouraging legitimate reporters, thereby undermining the purpose of the vulnerability disclosure program.

Requirement CR-ID: 7.3-CR-09

A public reporting channel shall be made available, using the accessible methods specified in 7.3-CR-02, so that vulnerability information or reports can be received.

Source:

- RCP-1-RQ-01 (40000-1-3)
- PRE-2-RQ-02(at least one) (40000-1-3)

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Guidance

Different reporting channel types should be considered to maximize accessibility and reach. These may include web forms, issue tracking systems, dedicated vulnerability reporting services, role-based or alias email addresses, and telephone or equivalent contact options. Including a security.txt file per RFC 9116:2022 can make the reporting mechanism easier to discover. When designing these channels, accessibility standards as set out in EN 301 549 v3.2.1 should be observed.

Further guidance on policy elements can be found in EN ISO/IEC 29147:2020, clause 9.2.2.

Requirement CR-ID: 7.3-CR-10

A system for assigning and maintaining identifiers or tracking numbers to reported vulnerabilities shall be implemented to support ongoing traceability of each report.

Source: RCP-1-RQ-02 (40000-1-3)

Guidance

Assigning a unique identifier, label, or tracking reference to each report ensures that it can be consistently traced and referenced throughout all stakeholder communications during vulnerability handling and disclosure. Additional implementation guidance is available in EN ISO/IEC 29147:2020, clause 6.2.4.

Requirement CR-ID: 7.3-CR-11

Receipt shall be confirmed of a potential vulnerability report to the reporter within a response window that is defined and published as part of the coordinated vulnerability disclosure policy.

Source: RCP-1-RQ-03 (40000-1-3)

Guidance

Guidance on how to acknowledge receipt of vulnerability reports is available in EN ISO/IEC 29147:2020, clause 6.2.5.

Requirement CR-ID: 7.3-CR-12

Vulnerability reports submitted through channels that do not meet the security standards described in 7.1 should still be accepted rather than rejected on the basis of the submission method alone.

Source: RCP-1-RC-01 (40000-1-3)

Guidance

The purpose of this requirement is to ensure that potential vulnerabilities are not missed due to procedural issues with how they are reported. An imperfect intake channel should not outweigh the need to identify, assess, and remediate security risk. Treat the report as valid input, then move subsequent handling into the appropriate secure process.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

6.4 Intake in Vulnerability Handling

Introduction

The intake of vulnerability reports focuses on evaluation for validity, reproducibility, and applicability. The manufacturer reviews the credibility of the report, attempts to reproduce the issue, and assesses both the impact on the affected product and the severity of the vulnerability. Only positively verified vulnerabilities proceed to the security risk assessment.

Output: vulnerability handling intake processes.

Requirements

Requirement CR-ID: 7.4-CR-01

Where a vulnerability report does not contain enough detail to support assessment, the necessary additional information shall be requested from the reporter.

Source: VRF-1-RQ-01 (40000-1-3)

Guidance

If a report does not provide enough detail to carry out a meaningful evaluation, the manufacturer should take the initiative to contact the reporter and request what is missing. This could encompass technical reproduction steps, information about the environment in which the issue was observed, or clarification regarding the described impact.

Requirement CR-ID: 7.4-CR-02

A structured triage of each reported vulnerability shall be performed.

Source: VRF-1-RQ-02 (40000-1-3)

Guidance

The triage should include the following elements:

- **Credibility evaluation:** Assess whether the reported vulnerability is plausible given the product's architecture, design, and known components.
- **Reproducibility:** Attempt to reproduce the reported issue using available product information, including the software list and product context.
- **Impact analysis:** Evaluate the potential impact of the vulnerability on the affected product, taking into account the product's security architecture and existing risk assessment.
- **Severity determination:** Assign a severity rating to the vulnerability to support prioritization in subsequent steps.

Where a vulnerability is determined to be not applicable, the rationale for this determination should be documented.

In multi-party coordinated vulnerability disclosure scenarios, additional guidance from ISO/IEC TR 5895:2022 should be considered.

Requirement CR-ID: 7.4-CR-03

Risk resulting from the vulnerability shall be evaluated aligned with the methodology specified in 5.4 to 5.7.

Source:

- VRF-2-RQ-01 (40000-1-3)
- SOTA (guidance)

Guidance

Risk evaluation should be conducted in line with the existing approach so that the outcome remains coherent with the product's broader risk management framework.

For mobile applications, risk evaluation should take into account mobile-context factors (e.g., local vs. remote exploitability, dependency on user interaction, access to sensitive on-device data).

Standard scoring systems such as CVSS v3.1 or v4.0 provide a baseline but may not fully reflect mobile-specific exploitation conditions (e.g., a vulnerability exploitable only via a malicious app on the same device may score differently in a mobile context than in a server context). The OWASP Mobile Top 10(2016/2024) and OWASP MASVS risk model provide supplementary frameworks for contextualizing severity in mobile environments. The procedure should document how environmental and temporal CVSS metrics are adjusted for the mobile deployment context.

Assesment should take into account chained exploitation of the vulnerability with other vulnerabilities and not just the risk profile of the vulnerability on its own.

Requirement CR-ID: 7.4-CR-04

Each vulnerability shall be assigned a handling priority, derived from both the risk evaluation result and the risk profile specific to the product.

Source: VRF-2-RQ-02 (40000-1-3)

Guidance

EN ISO/IEC 30111:2020, clause 7.1.4 e) may be consulted for supplementary guidance on how to approach prioritization decisions.

Requirement CR-ID: 7.4-CR-05

If the assessed risk level of a vulnerability surpasses the manufacturer's defined risk threshold, the vulnerability resolution process shall be expedited.

Source: VRF-2-RQ-03 (40000-1-3)

Guidance

Expediting resolution means bringing forward one or more handling activities - including remediation development, testing, or deployment - ahead of the standard update schedule. The risk threshold that triggers this accelerated handling is determined by the manufacturer's own risk assessment framework.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 7.4-CR-06

When a vulnerability has been reported through a coordinated disclosure process, the originating reporter shall be notified of the outcome of the intake activity, if possible.

Source: VRF-2-RQ-04 (40000-1-3)

Guidance

In a coordinated vulnerability disclosure process, the reporter is an active participant in handling the issue responsibly. Informing the reporter of the verification results helps keep the process collaborative, transparent, and effective.

EN ISO/IEC 30111:2020, clause 7.1.4 f) provides supplementary guidance on how to communicate with reporters. In cases where the vulnerability concerns a third-party component, consideration should be given to also notifying the manufacturer or maintainer of that component regarding the verification findings relevant to their component.

6.5 Communication with Stakeholders in Vulnerability Handling

Introduction

On-going communication is a continuous activity throughout the vulnerability handling process, running in parallel with all phases rather than following a strict sequence. Its purpose is to maintain regular communication channels with all relevant stakeholders - including users, reporters, coordinators, manufacturers, open-source stewards, and maintainers - as appropriate to the product's life cycle and the current phase of vulnerability handling.

Output: Vulnerability handling stakeholder communication processes.

Requirements

Requirement CR-ID: 7.5-CR-01

Communication with reporters and all relevant stakeholders shall be initiated and sustained throughout the vulnerability handling process.

Source:

- PRE-4-RQ-01 (40000-1-3)
- RCP-5-RC-01 (40000-1-3) – on coordinator communication

Guidance

Communication channels should be opened at the earliest opportunity and remain active for the duration of vulnerability handling activities. Depending on the context, relevant parties may include vulnerability reporters, coordinating bodies, other manufacturers, open-source stewards, and maintainers of non-commercial open-source projects. The appropriate frequency and form of communication will depend on which phase of the vulnerability handling process is underway. Further practical guidance on structuring and sustaining stakeholder communication can be found in EN ISO/IEC 29147:2020, clause 6.5.

Where circumstances warrant it, an appropriate coordinator should be designated and actively engaged throughout the vulnerability handling process.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Coordinator involvement supports transparent and timely communication during vulnerability handling. A coordinator is particularly valuable when vulnerabilities affect multiple stakeholders or when direct communication between stakeholders is complex or otherwise not feasible. While engagement of a coordinator is optional, it can significantly ease the coordination burden in complex disclosure scenarios.

A coordinator should be considered when a vulnerability impacts several manufacturers at once, or when direct dialogue between the reporting party and the affected organization is impractical or overly complex. A coordinator provides a structured and impartial channel for communication and assists in managing the timing of disclosure. For further practical guidance on coordinator involvement, consult EN ISO/IEC 29147:2020, sections 5.5.5 and 6.6. The coordinator role is formally defined in EN ISO/IEC 29147:2020, Clause 8.

Requirement CR-ID: 7.5-CR-02

When communicating with users, communication channels and formats shall be employed that are accessible to a broad range of users.

Source: PRE-4-RQ-02 (40000-1-3)

Guidance

Accessibility in communication requires that both the channels selected and the formats used are suited to a wide range of user needs and capabilities. Care should be taken to ensure that information relating to vulnerabilities is conveyed in a manner that users can meaningfully receive and comprehend. Additional guidance on how to achieve accessible communication methods is available in 5.9.

6.6 Remediation in Vulnerability Handling

Introduction

The remediation decision phase encompasses the activities required to determine how identified and verified vulnerabilities will be addressed. This involves evaluating potential risk remediation measures, assessing their feasibility, and weighing their impact on the product, its users, and other stakeholders. This can result in a product update, a temporary mitigating measure, or a documented and justified choice to postpone or forgo remediation entirely.

Output: Vulnerability handling remediation processes.

Requirements

Requirement CR-ID: 7.6-CR-01

A formal remediation decision shall be made and documented for each identified vulnerability, determining the course of action to address it.

Source:

- RMD-1-RQ-01 (40000-1-3)

- SOTA (documented)

Guidance

In reaching a remediation decision, assess the available options in terms of their practicality and the effects they may have on the product, its users, and relevant stakeholders. Possible outcomes include releasing a product update, applying an interim mitigation, or making a documented and justified choice to postpone or forgo remediation. Further guidance on how to structure this decision process is available in EN ISO/IEC 30111:2020, clause 7.1.5 a).

Requirement CR-ID: 7.6-CR-02

Following the remediation decision, a concrete action plan shall be established that specifies what steps will be taken and sets a defined timeline for their completion.

Source:

- RMD-1-RQ-02 (40000-1-3)
- SOTA (**Guidance**)

Guidance

After a remediation decision has been reached, it should be converted into a practical plan of action. The plan should clearly specify the steps to be carried out and set a realistic schedule for completing them, taking into account the characteristics and severity of the vulnerability as well as the selected remediation approach.

The remediation schedule should also consider the time lag introduced by app store review processes (Apple App Store, Google Play) before a remediation reaches end users; and whether OS-vendor-provided mitigations (e.g., Android security patch levels, iOS rapid security responses) reduce the urgency or alter the preferred remediation approach. These factors should be explicitly documented in the remediation decision record.

Requirement CR-ID: 7.6-CR-03

Once a decision to remediate a vulnerability has been made, the necessary activities shall be carried out to produce that remediation.

Source: RMD-2-RQ-01 (40000-1-3)

Guidance

- The manufacturer's established internal development processes should govern how remediation is carried out.
- Remediation is not limited to software patches or code fixes. Artefacts such as updated user documentation, configuration guidance, or changes to other materials required to adequately address the vulnerability should be considered.
- Where a supplier, open-source project, or other third party has already produced a suitable remediation, the manufacturer may adopt that existing remediation in place of developing one independently.

Requirement CR-ID: 7.6-CR-04

Where it is technically feasible to do so, security updates shall be delivered independently of functional updates, rather than bundled together.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Source: RMD-2-RQ-02 (40000-1-3)

Guidance

Outputs may take various forms, including software updates, configuration changes, or documentation updates. Third parties, such as suppliers or open-source projects, may be involved in coordinating or sourcing remediation.

- When determining whether separate delivery of security updates is technically feasible, the assessment should take into account the available technology and relevant constraints, including cost, schedule, and performance limitations.
- The assessment may also encompass operational feasibility, considering whether a separately delivered security update can be successfully integrated into the product, sustained over time, and supported in the operational environment.

Requirement CR-ID: 7.6-CR-05

Any remediation applied to address a vulnerability shall undergo testing to confirm that the associated risk has been adequately reduced and that no unacceptable adverse effects on the product or its users have been introduced.

Source: RMD-3-RQ-01 (40000-1-3)

Guidance

Remediation testing ensures that a fix for a vulnerability is both effective and safe - confirming that the associated risk is adequately mitigated while not introducing adverse effects on the product or its users.

Where a fix is supplied by a third party, such as a component vendor, the manufacturer is expected to validate the remediation at the product level and confirm that normal functional behaviour is maintained, to the degree that this is reasonably achievable. Verification of the underlying component itself remains the obligation of the supplying party.

6.7 Release of Security Updates and Information in Vulnerability Handling

Introduction

Security update release covers the collection of necessary artefacts to address vulnerabilities and their dissemination to users. Timely distribution is critical, as delays give attackers opportunity to exploit known weaknesses. Depending on the product type, its intended purpose, and its reasonably foreseeable use, updates may be applied automatically or manually. Where possible, security updates should be scoped to avoid changing other product functionality, minimizing unintended operational impacts - though some remediations inevitably require more substantial changes.

Output: Vulnerability handling security updates and information processes.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirements

Requirement CR-ID: 7.7-CR-01

Security updates shall be made available at no cost, except where a manufacturer and a business user have explicitly agreed otherwise for a purpose-built product with digital elements.

Source: RLS-1-RQ-01 (40000-1-3)

Requirement CR-ID: 7.7-CR-02

After a security update has been made ready, it shall be released to users without undue delay.

Source: RLS-1-RQ-02 (40000-1-3)

Guidance

- Updates should be handled according to the priority established in 7.4.
- Acting without undue delay means that vulnerabilities carrying the potential for broad societal harm are treated as high priority. Updates addressing critical security weaknesses should be expedited accordingly.
- Both automatic and manual distribution mechanisms are valid approaches. The appropriate choice depends on the nature of the product, its intended use, and the users it serves. Where a product supports automatic updates, that capability should be used.
- Commonly adopted industry benchmarks at the time of writing include: Critical (CVSS ≥ 9.0) - patch within 24–72 hours; High (CVSS 7.0–8.9) - patch within 7–30 days; Medium and below - patch within 90 days. For mobile applications, the procedure should account for app store review latency (typically 1–3 days for iOS App Store; shorter for Google Play) and should include a process for using expedited review requests where available.
- Server-side RDPS mitigations may be deployable independently of app store timelines and should be considered as a first-response option.
- NIST SP 800-40 Rev. 4 provides relevant patch management guidance.

Requirement CR-ID: 7.7-CR-03

Where the delivery of a security update is not entirely automated, clear installation instructions shall be supplied to users.

Source: RLS-1-RQ-03 (40000-1-3)

Guidance

When updates cannot be applied automatically, users should be given sufficient guidance to carry out installation correctly. Well-prepared instructions reduce the likelihood of errors that could disrupt the user's operational environment.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 7.7-CR-04

After a vulnerability has been resolved, information shall be provisioned in line with the coordinated vulnerability disclosure (CVD) policy established under 7.3; where suitable, such information may be presented in summarized or aggregated form, in a format readable by humans, in a widely recognized machine-readable format, and include, as a minimum, the following elements to allow recipients to assess relevance and take appropriate remediation action:

- a description of the vulnerability
- a vulnerability identifier
- information sufficient to identify the affected product
- the potential impact of the vulnerability
- the severity of the vulnerability
- detailed remediation instructions
- the date of release and any subsequent update date

Source:

- 40000-1-3: RLS-2-RQ-01, RLS-2-RQ-02(minimum), RLS-2-RQ-03 (human), RLS-2-RQ-03-RE (machine-readable), RLS-2-RC-01 (EUVD)
- SOTA (mobile app guidance)

Guidance

Clear and comprehensive publications - such as advisories or release notes - help users and stakeholders understand the nature of vulnerabilities and make informed decisions about managing associated risks. Coordination with relevant stakeholders and adherence to a coordinated vulnerability disclosure (CVD) policy are central to this process.

Organizations publishing vulnerability advisories are encouraged to consult EN ISO/IEC 29147:2020, Clause 7, for structured guidance on how to format and communicate disclosures in a clear and consistent manner.

Organizations seeking further detail on what to include in a vulnerability advisory should refer to EN ISO/IEC 29147:2020, section 7.4, which provides practical elaboration on the content and structure of advisory elements.

The required machine-readable format is defined in ISO/IEC 20153:2025. Organizations should consult this standard to ensure that published vulnerability information conforms to the specified format.

For mobile applications, residual risk notifications to end users may be delivered through in-app notifications, app store release notes, or security advisories published on the manufacturer's website. Notifications to enterprise operators deploying the application under mobile device management (MDM) should be coordinated through established B2B communication channels. Where regulatory notification obligations apply (e.g., under the EU Cyber Resilience Act or national cybersecurity authorities), the procedure should define the responsible role and the applicable notification timeline. The content of residual risk notifications should be proportionate to the audience's technical capability and should avoid disclosing exploitation details prematurely.

Published vulnerability information should be made available through the EU Vulnerability Database (EUVD).

Where vulnerability information has been disclosed via the CVE program, it will be ingested automatically into the EUVD. In such cases, no additional submission to the EUVD is required to satisfy this requirement.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Requirement CR-ID: 7.7-CR-05

Complete publication of vulnerability information shall be deferred in order to allow adequate time for security update distribution, in case all three of the following conditions are simultaneously satisfied:

- the risks associated with full disclosure outweigh its security benefits at that time.
- Sufficient information about the resolved vulnerability is made available to users in a manner that does not enable an attacker to exploit it.
- Users are notified of the scheduled date on which all vulnerability information will be publicly disclosed.

Source:

- RLS-2-PM-01 (40000-1-3)
- SOTA (from optional to mandatory)

Guidance

Where an organization invokes this permission to defer full publication, it should record and retain the justification for doing so. Such documentation is likely to be required as evidence when this permission is exercised, as indicated by the assessment criteria associated with this section.

For mobile applications distributed via app stores, the process should account for app store review timelines when planning coordinated public disclosure.

Requirement CR-ID: 7.7-CR-06

Following the release of a remediation, post-release activities shall be executed that encompass maintaining the vulnerability case record and tracking the effectiveness of the applied remediation.

Source: PRA-1-RQ-01 (40000-1-3)

Guidance

The post-release phase encompasses activities that take place after a vulnerability has been remediated and released. This phase is concerned with monitoring the effectiveness of released security updates, capturing lessons learned from the process, and using these insights to continuously improve future development practices.

The monitoring of a remediation does not need to be conducted as a separate, standalone activity; it may be embedded within the organization's wider vulnerability management process. Practitioners seeking further elaboration on post-release practices should consult EN ISO/IEC 30111:2020, section 7.1.7, which provides additional normative context for this phase.

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

2 Colofon

Auteur	Software Improvement Group
Versie	0.95
Datum brondocument	September 9, 2026
Status	Intern gebruik

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

Annex - Requirements overview

The following overview shows all clauses and sub clauses with their individual requirements, where the key text of the requirement is shown, as it is underlined in the requirement text – to capture its essence in short.

5 Product Cybersecurity Risk Management

5.2 Product Context Documentation

1. identify and document the product context
2. RDPS explicitly reflected
3. procedure for establishing and updating the product context

5.3 Risk Acceptance Criteria

1. cybersecurity risk acceptance criteria

5.4 Product Cybersecurity Asset Identification

1. identify all cybersecurity assets
2. AI-specific assets

5.5 Product Cybersecurity Risk Identification

1. identify product cybersecurity risks
2. identify those publicly known vulnerabilities
3. documented threat modelling procedure

5.6 Product Cybersecurity Risk Analysis

1. likelihood
2. severity
3. incident scenario
4. risk analysis methodology
5. rationale

5.7 Product Cybersecurity Risk Evaluation and Risk Acceptance

1. assessed
2. acceptance
3. required user, mitigations are realistic and achievable
4. acceptance, justification

5.8 Product Cybersecurity Risk Treatment

1. apply a treatment option
2. document the treatment option
3. re-evaluate

5.9 Product Cybersecurity Risk Communication

1. language and methods appropriate to the audience
2. ensures each user can meaningfully access the information
3. address a minimum set of elements

5.10 Product Cybersecurity Risk Review

1. reviews of its product cybersecurity risk management activities
2. shall initiate a review of its risk management activities, when trigger conditions
3. documentation produced under Clause 5 shall be updated

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

6 Product Cybersecurity Lifecycle Activities

6.2 Product Cybersecurity Planning

1. cybersecurity plan
2. plan shall be kept current

6.3 Product Cybersecurity Requirements

1. cybersecurity requirements shall be derived
2. reviewed and updated
3. changes to product cybersecurity requirements shall be communicated

6.4 Cybersecurity Architecture and Design

1. specification of the product's cybersecurity architecture

6.5 Secure Implementation

1. secure development environment
2. implement all cybersecurity requirements, architecture and design
3. secure coding standard
4. identifying, reviewing, and approving the use of, memory-unsafe programming languages
5. deviations from the cybersecurity architecture and design, reviews shall be triggered
6. cryptographic mechanisms
7. secure hardware modules
8. inventorying all locations in the mobile application and its RDPS where cryptographic keys are generated, stored, used, and destroyed
9. reviewing the protocol inventory
10. security measures mitigating protocol issues

6.6 Technical Product Documentation

1. list of all integrated components, conditions that, shall be adhered to
2. a mapping of upstream dependencies and interdependencies
3. a revised SBOM
4. technical documentation
5. specification of all cryptographic mechanisms
6. links each identified threat to the security function or functions that address it

6.7 Cybersecurity Verification and Validation

1. key elements as input
2. satisfy the cybersecurity requirements
3. threat scenarios and attack profiles, advanced penetration testing
4. risks associated with integrated components
5. supply chain integrity
6. V&V process shall encompass key elements
7. SAST, DAST
8. code review
9. shall document and identify all test methods and selected test tools
10. recur
11. security test and review, plan

6.8 Secure Production and Distribution

1. protected against manipulation

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

2. access authentication for protected areas of the hosting platform; integrity protection for distribution artefacts in transit and at rest; and authenticity mechanisms for distribution artefacts
3. user-facing information and instructions distributed digitally shall be protected
4. accessible
5. code-signing process
6. Multi-factor authentication (MFA) and role-based access controls
7. product shall be made identifiable
8. communication mechanism
9. mechanism enabling security updates to be distributed

6.9 Product Cybersecurity Monitoring and Issue Management

1. procedure for, monitoring of internal and external information
2. risks, shall be assessed
3. documentation, communicate
4. timely manner
5. residual risk, shall be communicated
6. designated internal and external sources

6.10 Secure Decommissioning

1. prepared
2. instructions shall address

6.11 Third-Party Component Cybersecurity Management

1. due diligence
2. addressed within the risk assessment and risk treatment
3. validate and verify
4. monitoring
5. disclose, remediate
6. communicate that fix
7. assessed for maintenance activity

7 Vulnerability Handling

7.1 Operational Security of Vulnerability Handling

1. Operational security measures
2. Access to vulnerability information shall be, restricted

7.2 Facilities for Vulnerability Handling

1. vulnerability handling policy
2. policy shall describe
3. continuous monitoring
4. disclosure policy
5. documented process for evaluating, approving, and recording decisions to delay full vulnerability publication

7.3 Coordinated Vulnerability Disclosure Facilities

1. coordinated vulnerability disclosure policy
2. multiple sensory modalities
3. what parties can expect with respect to ongoing communication
4. CVD policy should address each of the following areas
5. not made public
6. secure communication mechanisms for vulnerability disclosure

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme

7. without disclosing their identity
8. not create unreasonable barriers
9. reporting channel shall be made available
10. identifiers or tracking numbers
11. receipt shall be confirmed
12. still be accepted rather than rejected on the basis of the submission method alone.

7.4 Intake in Vulnerability Handling

1. necessary additional information shall be requested from the reporter
2. verification
3. risk shall be evaluated
4. assigned a handling priority
5. expedited
6. originating reporter shall be notified of the outcome

7.5 Communication with Stakeholders in Vulnerability Handling

1. communication with reporters and all relevant stakeholders
2. accessible
3. coordinator should be designated and actively engaged

7.6 Remediation in Vulnerability Handling

1. determining the course of action to address it
2. action plan
3. produce that remediation
4. security updates shall be delivered independently
5. testing

7.7 Release of Security Updates and Information in Vulnerability Handling

1. security updates shall be made available at no cost
2. without undue delay
3. clear installation instructions
4. provision of information, in line with the coordinated vulnerability disclosure (CVD) policy
5. may defer complete publication of vulnerability information
6. made available through the EU Vulnerability Database
7. post-release activities

EUDIW CERTIFICATION SYSTEM MANAGEMENT BOARD NL
Ensuring High Assurance of EUDI Wallets & the NL National eID Scheme