ANNEX I

Risk register for European Digital Identity Wallets

INTRODUCTION

The risk register describes the main security and privacy risks and threats that apply to wallets, and which shall be properly addressed in every architecture and implementation of wallets. The **high-level risks** (Section I) are related to the use of wallets by users and relying parties, and they are associated to direct threats targeting the assets of wallets. In addition, a few **system-level risks** (Section II) to wallets are identified, which would typically result from a combination of threats applying to the entire wallet system.

Risk type	Risk ID	Related risk titles
High-level risks to the wallets	R1	Creation or use of an existing electronic identity
	R2	Creation or use of a fake electronic identity
	R3	Creation or use of fake attributes
	R4	Identify theft
	R5	Data theft
	R6	Data disclosure
	R7	Data manipulation
	R8	Data loss
	R9	Unauthorised transaction
	R10	Transaction manipulation
	R11	Repudiation
	R12	Transaction data disclosure
	R13	Service disruption
	R14	Surveillance
System-related risks	SR1	Wholesale surveillance
	SR2	Reputational damage
	SR3	Legal non-compliance

The register also identifies **technical threats** (Section III) targeting the implementation of the wallet solution. These threats are related to the high-level risks in the sense that each one of them could be used to trigger many high-level risks.

Threat type	Threat ID	Related threat titles	Subcategories of threats
Technical threat	TT1	Physical attacks	*1.1 Theft*
			1.2 Information leakage
			1.3 *Tampering*
	TT2	Errors and misconfigurations	*2.1 Errors made when managing an IT system*
			2.2 Application-level errors or usage errors
			2.3 Development-time errors and system misconfigurations
	TT3	Use of unreliable resources	*3.1 Erroneous use or configuration of wallet components*
	TT4	Failure and outages	*4.1 Failure or dysfunction of equipment, devices or systems*
			4.2 Loss of resources
			4.3 *Loss of support services*
	TT5	Malicious actions	5.1 *Interception of information*
			5.2 *Phishing and spoofing*
			5.3 *Replay of messages*
			5.4 *Brute-force attack*
			5.5 *Software vulnerabilities*
			5.6 *Supply chain attacks*
			5.7 *Malware*
			5.8 *Random number prediction*

Finally, the register **lists direct threats to the wallets**, and each one is associated to a (non-exhaustive) selection of risks (Section IV).

SECTION I: HIGH-LEVEL RISKS TO THE WALLETS

R1. Creation or use of an existing electronic identity
Creation or use of an existing electronic identity is defined as the creation of an electronic identity in a wallet that exists in the real world and is assigned to another user. By essence, this risk leads to the risks of Identity theft (R4), and Unauthorised transactions (R9).
R2. Creation or use of a fake electronic identity
Creation or use of a fake electronic identity is defined as the creation of an electronic identity in a wallet that does not exist in the real world.
R3. Creation or use of fake attributes
Creation or use of fake attributes is defined as the creation or use of attributes that cannot be validated to be issued by the claimed provider and cannot be trusted.
R4. Identify theft
Identity theft is defined as the unauthorised acquisition of the wallet unit or loss of authentication factors enabling to impersonate a person.
R5. Data theft
Data theft is defined as the unauthorised extraction of data. Data theft is also associated to threats, such as data interception (unauthorised capture of data in transit) and data decryption (unauthorised decoding of encrypted data), which are likely to lead in some cases to Data disclosure (R6).
R6. Data disclosure
Data disclosure is defined as the unauthorised exposure of personal data including special categories of personal data. The privacy breach risk is very similar when considered from a privacy rather than security viewpoint.
R7. Data manipulation
Data manipulation is defined as the unauthorised alteration of data.
R8. Data loss

Data loss is defined as the situation where data stored in the wallet is lost through misuse or malicious action. This risk is often a secondary risk of Data manipulation (R7) or Service disruption (R13), where all or part of the data cannot be restored.
R9. Unauthorised transaction
Unauthorised transactions are defined as operational activities conducted without the permission or knowledge of the wallet user. In many cases, an unauthorised transaction can lead to Identity theft (R4) or Data disclosure (R6). It is also related to unauthorised transactions, such as the misuse of cryptographic keys.
R10. Transaction manipulation
Transaction manipulation is defined as the unauthorised alteration of operations in the wallet. Transaction manipulation is an attack on integrity, and it is related to a data integrity breach.
R11. Repudiation
Repudiation is defined as a situation where a stakeholder can deny performing an action or being involved in a transaction, and other stakeholders do not have proper evidence to contradict them.
R12. Transaction data disclosure
Transaction data disclosure is defined as the disclosure of information related to information on a transaction between stakeholders.
R13. Service disruption
Service disruption is defined as an interruption or degradation in the normal operation of the wallet. A specific kind of service disruption is user lock-out, defined as the inability of a user to access their account or their wallet.
R14. Surveillance
Surveillance, or monitoring, is defined as the unauthorised tracking or observation of a wallet user's activities, communication, or data. Surveillance is often related to inference, which is defined as the deduction of sensitive or personal information from seemingly innocuous data.

SECTION II: SYSTEM-RELATED RISKS

These risks are not used in the list of threats, as they are usually the consequence of multiple threats, repeated in a way that threatens the full system.

SR1. Wholesale surveillance
Wholesale surveillance is defined as the tracking or observation of the activities of many users through their wallet's communication or data. Wholesale surveillance is often associated to surveillance (R14) and inference at a global scale, where information about many users is combined to deduce sensitive or personal data about users or to identify statistical trends that can be used to design further attacks.
SR2. Reputational damage
Reputational damage is defined as the harm caused to an organisation's or governmental body's reputation. Reputational damage will also stem from other risks when a breach or incident is covered by media and paints the organisation under an unfavourable light. Reputational damage can lead to further risks, such as loss of trust, stemming from the user's reasonable doubts, and loss of ecosystem, when the full ecosystem collapses.
SR3. Legal non-compliance
Legal non-compliance is defined as a situation when relevant laws, regulations or standards cannot be adhered to. In the context of the wallet, as security and privacy of the solution are legal requirements, all threats are likely to lead to some kind of legal non-compliance.

SECTION III: TECHNICAL THREATS

The technical threats are not all linked to specific risks on the wallets, because many of them are means that could be used to implement attacks corresponding to many different risks.

TT1. Physical attacks
1.1 Theft Theft is defined as the theft of devices that may alter the wallet's proper functioning (in case the device is stolen and the wallet unit is not adequately protected). This may contribute to many risks, including Identity theft (R4), Data theft (R5), and Unauthorised transactions (R9).
1.2 Information leakage Information leakage is defined as unauthorised access, information exposure, or sharing after physical access to the wallet. This may contribute in particular to Data Disclosure (R6) and Data theft (R5).
1.3 Tampering

Tampering is defined as violating the integrity of one or multiple components of the wallet unit, or of the components the wallet unit relies on, e.g., the user device or its operating system. This may contribute in particular to Data manipulation (R7), Data loss (R8) and Transaction manipulation (R10). When tampering targets software components, it may contribute to many risks.
TT2. Errors and misconfigurations
2.1 Errors made when managing an IT system Errors made when managing an IT system are defined as information leakage, sharing or damage caused by misuse of IT assets by users (lack of awareness of application features) or by improper configuration or management of IT assets.
2.2 Application-level errors or usage errors Application-level errors or usage errors are defined as dysfunctions of the application due to an error in the application itself or to an error by one of the users (wallet users and relying parties).
2.3 Development-time errors and system misconfigurations Development-time errors and system misconfigurations are defined as dysfunction or vulnerabilities caused by improperly developed or configured IT assets or business processes (inadequate specifications of IT products, inadequate usability, insecure interfaces, improper policy and procedure flows, design errors).
TT3. Use of unreliable resources
The use of unreliable resources is defined as an activity leading to unintentional damage due to ill-defined trust relationships, such as trusting a third-party provider without sufficient assurance.
3.1 Erroneous use or configuration of wallet components An erroneous use or configuration of wallet components is defined as unintentional damage to wallet components due to an erroneous use or misconfiguration by wallet users or by insufficiently trained developers, or due to lack of adaptation to changes in the threat landscape, typically the use of vulnerable third-party components or runtime platforms.
TT4. Failure and outages
4.1 Failure or dysfunction of equipment, devices or systems A failure or dysfunction of equipment is defined as unintentional damage to IT assets due to a failure or dysfunction of equipment, including the provider's infrastructure and the user devices.

4.2 Loss of resources The loss of resources is defined as an outage or dysfunction due to unavailability of such resources, e.g., as maintenance parts.
4.3 Loss of support services The loss of support services is defined as an outage or dysfunction due to unavailability of support services required for proper operation of the system, including network connectivity of the provider's infrastructure and of the user device.
TT5. Malicious actions
5.1 Interception of information The interception of information is defined as the capture of information improperly secured in transmission, including man-in-the-middle attacks.
5.2 Phishing and spoofing Phishing is defined as the capture of information provided by the user following a deceptive interaction, often associate to the spoofing of legitimate communication means and websites. These threats target the user and typically contribute to Identity theft (R4) and Unauthorised transactions (R9), often through Data theft (R5) or Data disclosure (R6).
5.3 Replay of messages Replay of messages is defined as the reuse of previously intercepted messages to perform unauthorised transactions, often at protocol level. This technical threat mainly contributes to unauthorised transactions, which may then lead to other risks, depending on the transaction.
5.4 Brute-force attack Brute-force attack is defined as a breach of security, often confidentiality, by performing a large number of interactions until the responses provide valuable information.
5.5 Software vulnerabilities The threat related to software vulnerabilities is a breach of security through exploitation of a software vulnerability in the components of the wallet or in the software and hardware components used in the implementation of the wallet, including published vulnerabilities and unpublished (0-day) vulnerabilities.
5.6 Supply chain attacks A supply chain attack is defined as a breach of security through attacks perpetrated on the supplier of the wallet provider or of its users to enable further attacks on the wallet itself.
5.7 Malware

Malware is defined as a breach of security through malicious applications performing unwanted and illegitimate actions on the wallet.
5.8 Random number prediction Random number prediction is defined as the enablement of brute-force attacks through partial or complete prediction of generated random numbers.

SECTION IV: THREATS TO THE WALLETS

This last section presents a selection of typical threat scenarios specific to the wallets, which are mapped to the key related high-level risks, as listed above. This list indicates threats that need to be covered, but it does not constitute an exhaustive list of threats, which depends greatly on the architecture of the selected wallet solution and on the evolution of the threat environment. Additionally, in the risk assessment and proposed measures, the wallet provider can only be responsible for those components in scope of certification (*).

ID *Identifier*	**Threat description** *Description of the identified threat* (*)	**Risk title** *Related risks*
TR1	An attacker can revoke pseudonyms without justified reason.	Creation or use of a fake electronic identity (R2)
TR2	An attacker can issue fabricated electronic identities that do not exist.	Creation or use of a fake electronic identity (R2)
TR3	An attacker can start to issue unauthorised PIDs.	Creation or use of a fake electronic identity (R2)
TR4	An attacker can get an administrator to enter a wrong PID provider into the PID provider trusted list.	Creation or use of a fake electronic identity (R2)
TR5	An attacker can bypass the remote identity proofing service.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR6	An attacker can bypass the physical identity proofing service.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR7	An attacker can bypass the identity proofing services related to the use of a remote (qualified) certificate.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR8	An attacker can get access to a wallet that is not bound to a person.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR9	An attacker can defeat technical and procedural controls to create wrong PIDs.	Creation or use of an existing electronic identity (R1) /

		Creation or use of a fake electronic identity (R2)
TR10	An attacker can activate a new wallet on an invalid WSCD.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2)
TR11	An attacker can bypass the identity proofing service related to the use of existing eID means.	Creation or use of an existing electronic identity (R1) / Identify theft (R4)/ Unauthorised transaction (R9)
TR12	An attacker can circumvent the verification by the PID provider that the wallet is controlled by the user and have a PID issued into a compromised wallet under the attacker's control.	Creation or use of an existing electronic identity (R1) / Identify theft (R4)/ Unauthorised transaction (R9)
TR13	An attacker can get a valid PID into an invalid wallet unit.	Creation or use of an existing electronic identity (R1) / Identify theft (R4)/ Unauthorised transaction (R9)
TR14	A PID provider can issue fabricated identities where the identity is related to an existing person.	Creation or use of an existing electronic identity (R1) / Identity theft (R4) / Unauthorised transaction (R9)
TR15	An attacker can link a PID with the wrong wallet because the PID provider is not able to link the PID to the correct wallet.	Creation or use of an existing electronic identity (R1) / Identify theft (R4) / Unauthorised transaction (R9)
TR16	An attacker can make the user approving the activation of a new wallet unit/instance under the attacker's control – with subsequent control of attestations as well.	Creation or use of an existing electronic identity (R1) / Creation or use of a fake electronic identity (R2) / Identify theft (R4) / Unauthorised transaction (R9)
TR17	An attacker can issue a PID of another state to access data / digital assets of targeted citizens.	Creation or use of an existing electronic identity (R1)/ Identity theft (R4) / Unauthorised transaction (R9)
TR18	An attacker can defeat technical and procedural controls to create fake (Q)EAAs.	Creation or use of fake attributes (R3)
TR19	An attacker can present (Q)EAAs that are not validly issued to them.	Creation or use of fake attributes (R3)
TR20	An attacker can attack the cryptographic linking mechanism of the wallet between the	Creation or use of fake attributes (R3)

	PID and a (Q)EAA that should not be issued to them.	
TR21	An attacker can use a (Q)EAA in a wallet, although the physical counterpart of the (Q)EAA is expired or invalid.	Creation or use of fake attributes (R3)
TR22	An attacker can circumvent the verification by the (Q)EAA provider that the wallet is in control of the user and have a (Q)EAA issued into a compromised wallet under the attacker's control.	Creation or use of fake attributes (R3)
TR23	An attacker can forge electronic attestations of attributes.	Creation or use of fake attributes (R3)
TR24	An attacker can inject forged electronic attestations of attributes into a wallet.	Creation or use of fake attributes (R3)
TR25	The wallet can present attributes to a relying party without the approval of a user.	Data disclosure (R6)
TR26	PID, (Q)EAAs or pseudonyms can be presented to a wrong relying party.	Data disclosure (R6)
TR27	An attacker can initiate a malicious renewal of EAA.	Data disclosure (R6)
TR28	An attacker can get a user into wrongfully approving a request for electronic attestations of attributes (phishing or other).	Data disclosure (R6)
TR29	An attacker can leak attributes from the wallet and identify the wallet user where identification is not required/allowed.	Data disclosure (R6)
TR30	An attacker can defeat technical and procedural controls to extract data.	Data disclosure (R6)
TR31	A request can be leaked to an attacker.	Data disclosure (R6)
TR32	An attacker can obtain knowledge on the embedded disclosure policy for attributes and present attributes contained in the current request by wallet units.	Data disclosure (R6)
TR33	An attacker can extract logs, or parts of them.	Data disclosure (R6)
TR34	An attacker can know whether a wallet is installed on the same device he is using, or on another one, and get information on it.	Data disclosure (R6)
TR35	An attacker can obtain a knowledge factor used for user authenticating to the WSCA.	Data disclosure (R6)
TR36	The electronic attestation of attributes about a person that is presented in multiple transactions with a relying party, or across different relying parties, unintentionally allows to link multiple transactions to the relevant person.	Data disclosure (R6)
TR37	A public attestation/relying party revocation list can contain information about the user's usage of their attestation (e.g. location, IP address…).	Data disclosure (R6)

TR38	Not being able to prove user's consent for shared attributes, relying parties can affect the integrity of logs.	Data disclosure (R6)
TR39	An attacker can unlawfully trace wallet users using unique/traceable identifiers.	Data disclosure (R6) / Surveillance (R14)
TR40	A relying party that consists of multiple units/entities that each have a different scope of what they are allowed to request/process, can request and process data for which they do not have lawful grounds for.	Data disclosure (R6) / Unauthorised transaction (R9)
TR41	An attacker can subvert the integrity and authenticity checks by the wallet of PIDs to always return success.	Data manipulation (R7)
TR42	An attacker can bypass or subvert the performance of checks by the wallet that verify the integrity and authenticity of requested attributes to always return success.	Data manipulation (R7)
TR43	An attacker can bypass or subvert the performance of checks by the wallet that verify all requested attributes belonging to the same user to always return success.	Data manipulation (R7)
TR44	An attacker can bypass or subvert the performance of checks by the wallet that verify the PID is valid and issued by a trusted PID provider to always return success.	Data manipulation (R7)
TR45	An attacker can bypass or subvert the performance of checks by the wallet that verify that a QEAA is valid and issued by a qualified TSP, who is registered to issue the QEAA, to always return success.	Data manipulation (R7)
TR46	An attacker can bypass or subvert the performance of checks by the wallet that verify whether the PID has been revoked by the PID provider to always return success.	Data manipulation (R7)
TR47	An attacker can bypass or subvert the performance of checks by the wallet that verify whether the (Q)EAA has been revoked by the (Q)EAA provider to always return success.	Data manipulation (R7)
TR48	An attacker can modify the content of backup and recovery data that should be exclusively under the user's control.	Data manipulation (R7) / Data loss (R8)
TR49	An attacker can modify the transaction history for a given wallet instance from the activity logs.	Data manipulation (R7) / Data loss (R8)
TR50	An attacker can eavesdrop during the connection from the wallet to relying parties.	Data theft (R5) / Data disclosure (R6)
TR51	An attacker can convince a user to share personal data (i.e. PID, EAA-s, pseudonyms, electronic signatures, logs and other data) with	Data theft (R5) / Data disclosure (R6)

	the attacker or with a third party that the user did not intend to do so.	
TR52	An attacker can read the transaction history for a given wallet instance from the activity logs.	Data theft (R5) / Data disclosure (R6)
TR53	An attacker can export or extract cryptographic key material outside of the WSCD.	Data theft (R5) / Data disclosure (R6) / Unauthorised transaction (R9)
TR54	An attacker can read the content of backup and recovery data that should be exclusively under the user's control.	Data theft (R5) / Data disclosure (R6)
TR55	An attacker can bypass the user authentication method to use a pseudonym generated by a wallet unit.	Identity theft (R4)
TR56	An attacker can propose an application that mimics a specific legitimate wallet to users.	Identity theft (R4)
TR57	An attacker can export wallet data, including PID, (Q)EAAs or logs.	Identity theft (R4)
TR58	An attacker can export cryptographic binding material.	Identity theft (R4)
TR59	An attacker can take over identities through the cryptographic keys of the wallet.	Identity theft (R4)
TR60	An attacker can duplicate another user's personal wallet unit on their personal device and use it.	Identify theft (R4) / Creation or use of an existing electronic identity (R1)
TR61	Authorities of another state can ask the user to show and/or share all the wallet data in a situation of proximity, such as when crossing the border of that state.	Identify theft (R4) / Surveillance (R14)
TR62	Users cannot transfer their transaction logs after failure of a user device, resulting in a loss of traceability of previous transactions on the new wallet.	Repudiation (R11)
TR63	Users cannot recover their transaction logs after failure of a user device, resulting in a loss of traceability on the new wallet.	Repudiation (R11)
TR64	Relying parties can have difficulties proving consent for remote electronic signatures.	Repudiation (R11)
TR65	An attacker can flood the connection(s) with requests during the connection to relying parties.	Service disruption (R13)
TR66	An attacker can flood a status provisioning service with connections to relying parties.	Service disruption (R13)
TR67	An attacker can make the attribute presentation appearing as contested/denied, despite the attribute presentation stating its validity.	Service disruption (R13)

TR68	An attacker can revoke a PID without justified reason.	Service disruption (R13)
TR69	An attacker can revoke a PID without user consent.	Service disruption (R13)
TR70	An attacker can revoke a (Q)EAA without justified reason.	Service disruption (R13)
TR71	An attacker can revoke a (Q)EAA without user consent.	Service disruption (R13)
TR72	An attacker can trigger multiple identification requests without them being recognised as intentional orphan requests.	Service disruption (R13)
TR73	An attacker can send multiple requests with no follow-up transaction.	Service disruption (R13)
TR74	An attacker can allow a relying party to request identification without a matching identification (response) and full control.	Service disruption (R13)
TR75	An attacker can send a response to a request after its timeout, or similar situations leading to a service disruption.	Service disruption (R13)
TR76	A relying party can send multiple invalid requests.	Service disruption (R13)
TR77	An attacker can send multiple invalid requests to a wallet provider.	Service disruption (R13)
TR78	An attacker can make a Member State unable to revoke an untrusted PID provider from the trusted PID provider trusted list.	Service disruption (R13)
TR79	An attacker can prevent suspension or revocation of a wallet.	Service disruption (R13)
TR80	An attacker can block transactions by relying parties, users and/or PID provider.	Service disruption (R13)
TR81	An attacker can disable or make a WSCD unavailable.	Service disruption (R13)
TR82	An attacker can make the PID provider unable to revoke or suspend PIDs.	Service disruption (R13) / Unauthorised transaction (R9)
TR83	A relying party can derive the user's identity data beyond data shared with them.	Surveillance (R14)
TR84	A group of colluding relying parties or PID providers can derive the user's identity data beyond data known to them.	Surveillance (R14)
TR85	An attacker can track and trace a user by using person identification data of the user where identification of the user is not required.	Surveillance (R14)
TR86	An attacker can combine a 'forged' presentation of (Q)EAA combinations.	Transaction manipulation (R10)
TR87	An attacker can activate/take over the wallet remotely (e.g., a bank app embedding an authentication or attestation request) without the explicit consent or sole control of the user,	Transaction manipulation (R10)

	in situations where the user is unaware of (e.g., asleep), or cannot see the relying party.	
TR88	Attackers can make changes to a request's metadata (service name, usages, etc.).	Transaction manipulation (R10)
TR89	Attackers can make changes to response information (service state, nonce, etc.).	Transaction manipulation (R10)
TR90	Attackers can make changes to a request's attribute information (over asking, etc.).	Transaction manipulation (R10)
TR91	A relying party can replay elements from a previous session in another session.	Transaction manipulation (R10)
TR92	An attacker can replace or modify the PID during its transfer from the PID provider to the wallet unit.	Transaction manipulation (R10)
TR93	An attacker can replace or modify the PID during its transfer from the wallet unit to the online relying party.	Transaction manipulation (R10)
TR94	An attacker can replace or modify the PID during its transfer from the wallet unit to the offline relying party.	Transaction manipulation (R10)
TR95	An attacker can issue a PID without the user's consent.	Unauthorised transaction (R9)
TR96	An attacker can use revoked or invalid embedded disclosure policies, possibly without the relying parties' knowledge.	Unauthorised transaction (R9)
TR97	An attacker can trick the wallet into verifying wrong electronic signatures.	Unauthorised transaction (R9)
TR98	An attacker can use the wallet outside of the user's control.	Unauthorised transaction (R9)
TR99	An attacker can convince a user to authenticate and approve transactions with an attacker or unauthorised third party.	Unauthorised transaction (R9)
TR100	An attacker can make a user electronically sign without presenting the content to the user or after presenting wrong content.	Unauthorised transaction (R9)
TR101	An attacker can bypass access control of the user's account with the wallet provider.	Unauthorised transaction (R9)
TR102	An attacker can impersonate relying parties during the connection to relying parties.	Unauthorised transaction (R9) / Data disclosure (R6)
TR103	The user behind the relying party – browser connection can be different from the user behind the relying party – wallet connection.	Unauthorised transaction (R9) / Data disclosure (R6) / Identity theft (R4)
TR104	An attacker can convince the user to revoke the user's wallet without reason.	Unauthorised transaction (R9) / Service disruption (R13)
TR105	An attacker can perform man-in-the-middle attacks.	Unauthorised transaction (R9) / Data disclosure (R6) / Surveillance (R14)

TR106	An attacker can present invalid or revoked attributes from a wallet that does not regularly connect to the network.	Effect on various risks
TR107	An attacker can steal information from a user by spoofing a wallet.	Effect on various risks
TR108	An attacker can impersonate the user by replaying/imitating a data request (e.g., authentication), which would appear as valid.	Effect on various risks
TR109	An attacker can replay an embedded disclosure policy towards a user, to imitate an approved request.	Effect on various risks
TR110	An attacker can exploit the lack of information of wallet users, or undue delays, after a security breach or compromise.	Effect on various risks
TR111	An attacker can modify a previously installed legitimate wallet instance to add malicious features.	Effect on various risks
TR112	An attacker can modify a legitimate wallet instance and propose it to users as a legitimate one.	Effect on various risks
TR113	An attacker can defeat the user authentication mechanism itself to bypass the authentication of the wallet user.	Effect on various risks
TR114	An attacker can introduce malicious code or backdoors into the wallet code during its deployment to the user device.	Effect on various risks
TR115	An attacker can introduce malicious code or backdoors into the wallet code during its development.	Effect on various risks
TR116	An attacker can tamper with the generation of random numbers to reduce their entropy sufficiently to enable attacks.	Effect on various risks
TR117	An attacker can tamper with user devices in the supply chain to include code or configurations that do not meet the conditions of use of the wallet.	Effect on various risks
TR118	An attacker can activate a wallet unit while using a spoofed WSCD controlled by the attackers.	Effect on various risks
TR119	An attacker can read information sent to the WSCA and/or the WSCD.	Effect on various risks
TR120	An attacker can send arbitrary information to the WSCA.	Effect on various risks
TR121	An attacker can steal information by intercepting the exchanges between the WSCA and the WSCD.	Effect on various risks
TR122	An attacker can send arbitrary information to the WSCD.	Effect on various risks

TR123	An attacker can send information to the WSCD, circumnavigating the WSCA.	Effect on various risks
TR124	An attacker can use phishing to get users to a fake wallet and PID management web application.	Effect on various risks
TR125	An attacker can replace a wallet's keys with other keys to create messages to be used in another attack.	Effect on various risks
TR126	An attacker can modify or destroy a wallet's keys, making some functions of the wallet unusable.	Effect on various risks
TR127	An attacker can control a malware to access data stored in the wallet.	Effect on various risks
TR128	An attacker can access evidence generated in the wallet.	Effect on various risks
TR129	Wallet providers can access objects in the wallet.	Effect on various risks
TR130	Wallet providers can access evidence generated in the wallet.	Effect on various risks
TR131	An attacker can steal an unlocked wallet device.	Effect on various risks
TR132	An attacker can manipulate the system to prevent certain events from being logged.	Effect on various risks
TR133	An attacker can intercept communication between the wallet instance and the WSCA, or replay/imitate a user (e.g. by hijacking authentication mechanism).	Effect on various risks