PROMON

EUDI Wallet mobile security checklist for relying parties

For banks, insurers, telecom providers, public services, and digital platforms accepting EUDI credentials through a mobile journey

How to use this checklist

A trusted EUDI credential can strengthen identity assurance. It does not secure the relying party's own application, session, or subsequent transaction.

Use this checklist to review the complete journey from the wallet request to the action taken in your service.

Mark each item: Covered / Partial / Gap
Record: Owner / Evidence / Next action

1. Define the use case and relying-party role

We have documented the service journey in which EUDI Wallet data will be requested.	☐ Covered	☐ Partial	☐ Gap
We know whether we are acting directly as the Wallet Relying Party or through an intermediary.	☐ Covered	☐ Partial	☐ Gap
We have identified the teams responsible for identity, mobile security, fraud, privacy, compliance, and customer experience.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

2. Register the intended use

The Wallet Relying Party is registered through the applicable national process.	☐ Covered	☐ Partial	☐ Gap
The registration accurately describes the intended use of the wallet and the data that will be requested.[1]	☐ Covered	☐ Partial	☐ Gap
Each requested attribute is necessary for the stated purpose.	☐ Covered	☐ Partial	☐ Gap
Product changes that affect the purpose or requested data trigger a registration and privacy review.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

3. Authenticate the relying-party instance

We have defined how the Relying Party Instance authenticates itself to the Wallet Instance.	☐ Covered	☐ Partial	☐ Gap
Required access certificates are issued, stored, renewed, and revoked through controlled processes.[1]	☐ Covered	☐ Partial	☐ Gap
The wallet can verify that requests come from the registered relying party.	☐ Covered	☐ Partial	☐ Gap
Private keys and signing operations are protected from unauthorized use.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

4. Request the right information

Each presentation request asks only for the attributes required for that transaction or service.	☐ Covered	☐ Partial	☐ Gap
The purpose of the request is clear to the user.	☐ Covered	☐ Partial	☐ Gap
We have considered whether derived or selective-disclosure attributes can replace unnecessary raw personal data.	☐ Covered	☐ Partial	☐ Gap
Consent and cancellation paths are clear and do not use misleading interface patterns.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

5. Verify what the wallet returns

We validate the signatures and trust chains associated with the PID or attestation.	☐ Covered	☐ Partial	☐ Gap
We check validity, expiry, issuer trust, and revocation status where applicable.	☐ Covered	☐ Partial	☐ Gap
We confirm that the returned information matches the original request and intended use.	☐ Covered	☐ Partial	☐ Gap
Failed or incomplete verification cannot be silently treated as successful.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

6. Protect the relying party's mobile app

The mobile app can detect relevant signs of tampering, repackaging, debugging, hooking, or a hostile device environment.	☐ Covered	☐ Partial	☐ Gap
Sensitive verifier logic and decisions cannot be changed through simple runtime manipulation.	☐ Covered	☐ Partial	☐ Gap
The interface displaying requested and returned information is protected against manipulation or overlays.	☐ Covered	☐ Partial	☐ Gap
Mobile runtime controls are treated as protection for our own app, not as a claim that we control or secure the user's Wallet Instance.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

7. Bind identity to the correct session and action

The verified result is securely connected to the correct user, device, session, and service request.	☐ Covered	☐ Partial	☐ Gap
An attacker cannot reuse a valid result in another session or substitute different transaction data after verification.	☐ Covered	☐ Partial	☐ Gap
Sensitive actions such as account opening, recovery, signing, or payment approval include appropriate confirmation and step-up controls.	☐ Covered	☐ Partial	☐ Gap
We have defined how long a verification result remains valid.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

8. Respond, investigate, and minimize data

We have defined what happens when verification fails or the relying-party app reports a high-risk runtime condition.	☐ Covered	☐ Partial	☐ Gap
Fraud, security, support, and compliance teams receive enough evidence to investigate disputed events.	☐ Covered	☐ Partial	☐ Gap
We retain only the identity and security data needed for a defined legal, operational, or fraud-prevention purpose.	☐ Covered	☐ Partial	☐ Gap
Runtime evidence can be correlated with the wallet interaction without creating unnecessary user profiling.	☐ Covered	☐ Partial	☐ Gap

Owner and evidence: _____

Next step

Review the complete chain:

Request → Relying-party authentication → User approval → Credential verification → Session binding → Business action

A trusted credential can reduce uncertainty about identity. Every step around that credential still needs its own security control and accountable owner.

Source notes:

[1] EU rules require Member States to maintain registration arrangements for Wallet Relying Parties. Registration information covers the relying party's identity, intended use of the wallet, and the data it plans to request. The framework also provides for certificates used to authenticate relying parties to Wallet Instances.

[2] The ARF treats relying parties as a distinct ecosystem role with responsibilities for registration, authenticated presentation requests, and verification of the PID or attestation received.

PROMON

About Promon

Promon leads the way in proactive mobile app security. For 20 years, we've been making the world a safer place by securing any app, on any device—in no time at all. Today, we protect over 2 billion users, secure 13 billion monthly transactions, and safeguard $2.5 trillion in market cap. Promon is headquartered in Oslo, Norway, with offices in more than 15 countries around the world.

Would you like to talk to an expert?

Mobile app security is crucial to preserve and improve your business reputation. Request pricing or talk to an expert to learn more today.

Book a meeting »

promon.io

Promon AS
Cort Adelers Gate 30
0251 Oslo
Norway