

Strengthening European digital sovereignty through an EU-based app distribution and verification framework

June 2026

1. Background

Mobile applications have become critical access points for public digital services across Europe, enabling citizens to interact with essential functions such as digital identity, healthcare, and social rights. As public services increasingly depend on these applications, trust in the authenticity and integrity of client software is essential for security and citizen confidence.

Today, the dominant mechanisms for app verification are Google Play Integrity and Apple App Attest. These mechanisms offer guarantees that a given app, phone and its hardware is authentic, unmodified, and running in a trusted environment. Public backend systems use such attestation signals to protect APIs against fraud, and unauthorized access.

As it is Apple and Google offer the best services, when a high level of security is needed. While effective, it creates a sovereignty challenge, when these mechanisms are governed by third-country entities and operate under non-European jurisdiction. In other words – this creates a strategic dependency that could undermine European digital sovereignty as mobile apps become core infrastructure for public digital services.

1.1 Structural dependence on non-European platforms

The Danish public administration currently relies on Google and Apple's verification and distribution mechanisms when distributing public apps regarding digital mail service, health services and eID. This means the government lacks control over:

- App distribution
- Integrity verification signals trusted by public backend systems.

The integrity verification pertains to three levels; the app, the operating system and the hardware, which depends on different technologies for verification. The hardware attestation for example depends on physical chips in the hardware while the app and operating system can be verified by software solutions,

Dependence on proprietary third-country solutions poses long-term strategic risks. Control over essential trust anchors – including app verification and integrity attestation – cannot, under current arrangements, be fully exercised by European stakeholders at the level which is required to maintain sufficient security in some of the Danish public apps.

The challenge could be equally relevant when discussing the European Digital Identity (EUDI) Wallet where cross-border digital services require consistent and interoperable trust frameworks. Nevertheless it seems like countries across EU are applying different solutions to distribution and verification. Without a unified European approach to app verification and distribution, there might be a risk of fragmentation between Member States, undermining cross-border interoperability.

3. European need for a sovereign app attestation and distribution framework

The challenges outlined above should be tackled by common European solutions and the DC-EDIC could be a forum for collaborating in finding a solution that can underpin the security of apps in public-sector digital services. The challenge is multifaceted and there is not one solution, which is why we invite all members, observers and the DC-EDIC itself to join in further analysing the depth of the issue as well as sharing best experiences and possibly developing concrete solutions together.

Such a solution could provide app attestation, ensuring that every application accessing public services can be verified without reliance on proprietary third-country hardware and software. This in turn will grant sovereign control over the trust anchors that backend APIs depend on, allowing European governments to manage the root of trust in authenticity of apps directly. Finally, a common solution would deliver European-operated capacity for distributing public-sector applications across the mobile ecosystems, guaranteeing that citizens receive secure, trustworthy software regardless of the platform they use. Together, these capabilities would create a more resilient digital infrastructure that aligns with Europe's strategic digital sovereignty.

4. Next steps

We propose that interested countries and the DC-EDIC join us in exploring alternatives to the Google and Apples' appstores', delivery mechanisms and verification. The specific framework for the analysis would have to be decided jointly by the participating countries, but it could include the following:

- Explore different governance, legal, and technical models for how a European appstore would function.
- A market research to find existing European open source solutions. And find what solutions are missing in the market.
- Joint development or procurement of European solutions that are not currently accessible in the market.