

Consultation Response:

Strategic Market Status SMS Investigations into Apple and Google's Mobile Platforms

Case references:

- SMS Investigation into Apple's Mobile Platform (CMA, 23 January 2025)
 - SMS Investigation into Google's Mobile Platform (CMA, 23 January 2025)
-

Introduction

- We welcome the opportunity to respond to the CMA's consultations on the proposed designation of Apple and Google as holding Strategic Market Status (SMS).
- As a UK-based accredited digital identity and age assurance provider, we believe the CMA's findings have critical implications for competition, innovation, and consumer trust in emerging digital trust infrastructure.
- Digital identity and age assurance are increasingly embedded at the operating system level, meaning CMA's intervention is essential to ensure these markets remain open, competitive, and aligned with UK regulatory objectives.

Q1. Do you have any views on our proposed descriptions of the relevant digital activities, namely: the mobile operating system, native app distribution, and mobile browser and browser engine?

We agree with the CMA's description of these digital activities. As highlighted in our response, **digital identity and age assurance are increasingly embedded at the operating system level**, and their functionality is deeply shaped by both app store distribution and browser integration. This convergence means the scope of "relevant digital activities" must include not just the technical layers of the OS and browsers, but also the *identity, credential, and wallet functions* that platforms bundle into them.

Q2. Do you have any views on our provisional conclusion that it would be appropriate to treat those activities as a single digital activity, referred to as a mobile platform?

We support the CMA's conclusion. In practice, these components cannot be considered separately: Apple and Google are positioned to **bundle their own wallets, derived credentials, and age assurance tools by default** at the OS and app store levels. This bundling creates a coherent, vertically integrated "mobile platform" whose purpose is to mediate interactions between users and providers. For accredited third-party providers this means competition depends not on isolated activities, but on the way the entire platform is controlled.

Q3. Do you have views on our provisional finding that the competitive constraint on Google's mobile platform from Apple's and other rival mobile ecosystems is limited?

We agree that constraint from rival ecosystems is limited. While Apple competes with Google in attracting users, both firms act as **gatekeepers** with the ability to foreclose third-party providers. For example, if a relying party integrates with Google's DC API but only accepts the Google ID Pass, **Google gains an automatic advantage over accredited competitors**. Similarly, Apple's bundling of its own wallet solutions narrows user choice. This demonstrates that rivalry between ecosystems does little to expand opportunities for accredited providers, and therefore does not constrain Google's market power in practice.

Q4. Do you have views on our provisional finding that there are high barriers to entry and expansion for mobile platforms?

We strongly agree. The barriers are substantial and structural:

- **Control of relying party access:** Platforms may require wallet integrators to register through their systems, giving them visibility into competitors' commercial relationships.
- **Exclusive access to government datasets:** For example, National Insurance records or transport operator age credentials, if granted exclusively, risk distorting competition.
- **Technical access restrictions:** Essential APIs (camera, NFC, secure element, browser identity interfaces) may be restricted or subject to discriminatory fees.

Together, these barriers make entry and expansion by accredited providers very difficult without regulatory intervention.

Q5. Do you have views on our provisional finding that the competitive constraint on Google's mobile platform from alternatives to content distribution within Google's mobile ecosystem, and alternatives on non-mobile devices, is limited?

We agree. Alternatives such as side-loading or reliance on non-mobile devices are not realistic substitutes. In practice, platforms can **bundle their own ID and credentialing solutions by default**, and restrict visibility of accredited third-party solutions. This structural bias reduces the practical scope of alternative routes for distribution and demonstrates why the CMA's concern about limited constraint is justified.

Q6. Do you have views on our provisional conclusion that there are no expected or foreseeable developments that are likely to eliminate Google's substantial market power in the provision of its mobile platform over the next 5 years?

We agree with this assessment. Without **mandated remedies**, there is little reason to expect structural change. Market forces alone will not deliver interoperability, portability of credentials, or equal access to essential datasets. On the contrary, we see risk that platforms will entrench their position further by embedding **opaque behavioural inference systems for age assurance**, which are both privacy-intrusive and inconsistent with UK policy objectives. This confirms that Google's substantial market power is likely to persist without timely regulatory action.

Q7. Do you have views on our provisional conclusion that Google has substantial and entrenched market power (SEMP) and a position of strategic significance (POSS) in respect of its mobile platform?

Yes, we support this conclusion. Our submission explicitly recognises that Apple and Google are **entrenched gatekeepers** in identity and age assurance, with the ability to foreclose accredited providers and distort competition. Their role as both *platform provider* and *service provider* creates a structural conflict of interest. In our view, Google clearly has both SEMP and POSS in relation to its mobile platform.

Q8. Do you have any other views in relation to the assessment/evidence set out in the proposed decision?

Yes. We recommend that the CMA's conduct requirements include **identity-specific remedies**, such as:

- **Interoperability and portability:** Credential portability between wallets, ensuring users can switch providers freely.
- **Equal access to datasets:** Prohibit exclusive arrangements with government agencies or essential data holders, and guarantee transparent, non-discriminatory access.
- **Prohibition of self-preferencing:** Prevent bundling or defaulting of Apple and Google's own identity solutions; mandate non-discriminatory acceptance of accredited ID wallets.
- **Transparency:** Require OS-integrated wallets to clearly display accreditation trust marks such as UKCertifID.
- **Fair access to APIs:** Guarantee equal access to essential APIs and prohibit discriminatory fees or restrictions.

These remedies are essential to ensure competition, innovation, and consumer trust in digital identity and age assurance services.

Given the sensitive nature of our response and the potential risk of reprisal, we respectfully request that it not be disclosed publicly and will therefore be submitting it on an anonymous basis.