Government consultation: making public services work for you with your digital identity

Personal tax

June 2026



20 May 2026

The ATT has welcomed the government's ambition to modernise public services through the introduction of a national digital identity, while warning that poor design could increase fraud risk and fail to meet the needs of vulnerable taxpayers.

In our response to the consultation 'Making public services work for you with your digital identity' (tinyurl.com/3mufkwar), the ATT emphasised that any digital identity (ID) system needed to reflect how individuals interacted with government departments, including through professional agents, and must not disadvantage those unable to access digital services.

From a tax administration perspective, we recognise that a well-designed digital ID could reduce duplication in identity checks, streamline access to HMRC's online

services and support more secure interactions between taxpayers, agents and government departments.

Priority uses should include access to HMRC accounts, tax repayments, changes to bank details, agent authorisation and claims to benefits. In these areas, errors in identity verification can cause significant disruption and financial harm, meaning a secure digital ID could deliver real benefits if implemented carefully.

Fraud risk and system resilience

We cautioned that consolidating identity data within a single national system would make it an attractive target for criminals. Identity-related fraud already poses serious challenges, and the consequences of account compromise would be magnified if a digital ID was misused.

We highlighted that strong technical safeguards must be accompanied by clear accountability arrangements, transparent communication when breaches occur, and swift redress for individuals affected by identity fraud. Without this, confidence in both the digital ID system and HMRC’s wider digital services could be undermined.

Digital exclusion and practical alternatives

A central concern highlighted was that of digital exclusion. While digital ID is described as voluntary, this must be the case in practice.

Many individuals, including those with disabilities, health conditions or limited digital capability, are unable to interact digitally or rely on others to manage their affairs. For these individuals, non-digital access routes need to be sustainable, properly resourced and equivalent to digital services in terms of both timeliness and status.

We suggested that a secure physical alternative, such as a government-issued card with a digital chip, could provide an effective option for those unable to use technology. We also pointed to a potential role for local authorities in enrolment, identity verification and user support, building on existing services.

Interoperability, data protection and next steps

We noted that it is important for any digital ID system to operate across all parts of the UK, including devolved administrations, local government and other public bodies such as Companies House, while respecting differing legal and administrative frameworks.

Data minimisation was identified as a key principle. We argue that a digital ID should contain only information strictly necessary for identity verification and should not become a repository for tax or financial data, reducing risk and helping to build public trust.

Finally, the ATT strongly supported phased pilots before any large-scale rollout. These should involve tax services, authorised agents and users with differing levels of digital capability, to ensure the system works in real-world conditions.

We concluded that digital ID could only succeed if it reduces administrative burdens while protecting vulnerable users, maintaining trust and accommodating the different ways in which individuals engage with systems.

The full ATT response is available here: www.att.org.uk/ref517

Senga Prior *sprior@att.org.uk*