

# Digital identity: The calls from local government are clear

Consultation alone is not enough.  
It is time for action, not words.

For a digital identity that works as a key foundation for modernising public services, Socitm research presents the case for deep involvement from local government in co-creating the emerging national framework and solutions. We call on local government itself to take the initiative and seek investment to build a sector specific capability that is interoperable with national solutions.

We've distilled the key arguments in this infographic. This follows extensive research with our partners across the public sector on the question of what it will take to create a successful digital identity that is trusted for use across the full spectrum of UK public services.



**Ensure that UK government resolves the current barriers** to a unified trust framework for digital identity that encompasses the socially inclusive requirements of the local public services sector.



**Seek investment for local government to build a sector specific capability** for local public services that is interoperable with emerging UK and devolved nation frameworks and solutions.



**Be involved in the design of policies, architectures and principles**, not just consulted on a design or prototype model.



**Ensure that the development starts with the end user.** This means avoiding the *'developing first for Whitehall and then generalizing'* approach, which does not reflect diverse citizen needs.



**Ensure that the citizen is always in control.** They can choose to allow their authentication to be shared with other services, or data linkages to be made, or data shared for whatever purpose.



**Ensure the design is both modular and adaptable.** This means separating out components such as the identifier structure, access methods, authentication, and electronic data sets/records design.



**Design identity solutions so that access can be made truly 'frictionless'** for the local service user, including those who do not have a mature digital 'footprint'.



**Build in adaptability and flexibility** in the design for future applications and use, giving the 'blueprint' to local government to use to develop local implementations with a confidence of compliance.



**Be transparent about the business case** and commercial arrangements of any solution, and on-going business model, so there are no surprises.



**Agree the issues associated with the first Verify programme** so that there is transparency and honesty in how the barriers and problems will be addressed in any future development.



**Ensure that other digital identity initiatives across Whitehall are aligned** to avoid incompatibility and weak interoperability across different projects which adds costs, risks, and barriers.



**Ensure technical interoperability**, with recognised and agreed standards, open APIs that will allow future connections and linkages to be made by councils when required. In particular, the possibility of an authenticated digital identity across related public services.



**Ensure cyber protection and resilience have the highest design priority**, with transparency and control resting with the end-user as far as possible.