Report

Digital identity – Summary

November 2021

Socitm INFORM

Introducing Socitm research into digital indentity

Focused on the application of digital identity in public services, this research aims to provide evidence-based guidance for two key audiences:

1. Those involved in digital public service design about the nature of digital identity and how it can underpin the future of local public service provision.

2. Those involved in national policy and development for digital identity, particularly in DCMS, GDS and the NHS, by presenting a clear and practical local perspective on the subject.

The need

A national digital identity solution for the UK public sector has long been recognised as vital to modernising public services. For over 20 years, Socitm and its local CIO Council have advocated such a solution to support not just the provision of truly people-centred services, but also the shift to working with people before they get into crisis; prevention is better than cure.

There is also a need in many public service organisations for mechanisms which allow easier movement of staff between different services. Digital identity based on common standards and methods would help with this.

The track record

It is fair to say that the UK public sector track record in creating a single and unified digital identity method for its own employees or the public has been poor. This is partly because of the failure to address public concern about identity management systems in general, but also in not accommodating the complexity of user case needs in areas such as health and local government.

There is hope however, in that new priorities are being set by national government to prioritise a trust framework approach to digital identity, rather than a single 'all singing all dancing' solution. Local government is involved in the discussions but needs to be even more involved if the problems of the past such as the recent failed GOV.UK Verify project are to be avoided.

What is digital identity?

This is a fundamental question and has often been overlooked. It's not an ID card, or a large central database of personal attributes and authentication methods.

There are general definitions of digital identity such as 'a digital representation of who you are, providing proof as necessary for digital interactions and transactions', but the definition for a national public sector-wide identity framework needs to be based on common policies, standards, and methods. It is therefore less about specific technologies, and more about how these can be used in a common and trusted fashion in different but often related situations.

Is it all just 'too hard'?

Given the problems over many years in digital identity solutions from the UK public sector, from ID cards through to NHS systems and GDS projects such as GOV.UK Verify, it is reasonable to ask whether the challenge is just too great.

However, with developing technology, the recent success of the NHS app, and some of the innovative examples listed in the Socitm research, it is clearly feasible to create a digital identity trust framework spanning local and central public service organisations.

What will be important is to:

- **Have a clear vision about what will be achieved**, and how it will work across the different parts of the public sector

- **Create a flexible 'trust framework'**, rather than a specific targeted technology solution designed 'at and for' the centre of government
- **Address concerns** of both the public and professionals in how such solutions are developed and will be maintained, learning lessons from the past
- **Learn from some of the examples** in other countries about how to do this successfully, whilst recognising that the UK is not necessarily the same.

Getting the principles right

Much of this is about ensuring that there are some basic principles on which developments can be based. The research from Socitm proposes four:

1. Operate on a distributed basis

...not a 'big central database' or single login that could be abused or hacked as a whole, supporting the need for identity portability across the wider public sector.

2. Place the citizen in control of access, data and linkages

...a fundamental design principle and the starting point of all digital identity system developments (and their components).

3. Build on a modular basis

...so that the different aspects of access, authentication, identity management and digital records development are separated, to create simplicity, protection and adaptability.

4. Make provision for the digitally vulnerable

...understanding and including in the design process those that are digitally excluded. This means ensuring that those who are fearful or less capable of using technology are adequately supported and involved.

Central to this is **data** – cyber safety, data privacy and data ethics. GDPR goes a long way to protect individual rights, but a specific analysis is needed in relation to digital identity or access, often by vulnerable people, to sensitive information.

Digital identity: the calls from local government are clear

Local government digital and IT professionals are often frustrated because they can see the problem and opportunity of digital identity solutions from the citizen perspective (and their often-complex user needs), yet solutions are driven from a central government viewpoint. This often turns out to be commercially unviable, or too narrow and limited.

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, we need early and deep involvement from local government in national initiatives, so that they are co-designed to reflect the complexity and diversity of local public service delivery.

Our research took input from CIOs and CDOs across local government and related stakeholder organisations.

Based on the research findings, Socitm calls for:

1. 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.

2. 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.

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

4. 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.

5. 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.

6. 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.

7. 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'.

8. 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.

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

10. 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.

11. 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.

12. 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.

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

About this report

Author
Jos Creese – Independent digital consultant, researcher and analyst

Editors
Martin Ferguson – Director of policy and research
David Ogden – Communications manager

Designers
Magdalena Werner – Senior creative designer
Benjamin Hughes – Graphic designer

Special thanks to:

William Barker, Socitm

Russ Charlesworth, Socitm Advisory

Alexandra Murphy, Socitm

Ben Cheetham, MHCLG Local Digital

Geoff Connell, Norfolk CC

Paul Davidson, iStand

Tom Denman, LGA

Sheldon Ferguson, MHCLG Local Digital

Phil Swan, iNetwork

Members of the Socitm Local CIO Council

Have your say

We always welcome feedback and discussion on the contents of our publications.

Martin Ferguson
Director of policy and research
martin.ferguson@socitm.net

Nadira Hussain
Director of leadership development and research
nadira.hussain@socitm.net

Get in touch

Website: www.socitm.net
Email: inform@socitm.net
Tel: 01604 709456

Join the conversation... @Socitm | Socitm