Data Sharing: A Better Way for Public Services

This Mydex CIC White Paper outlines a better way for service providers to provide their services and for citizens to access these services, helping to reduce friction, effort, risk, and cost for both sides, while delivering better outcomes. It is based on research conducted for Scottish Government and operational capabilities developed by Mydex CIC.

We believe the way forward described in this White Paper represents a practical, low cost, low risk way to transform the ways in which our society and economy collect and use personal to unleash its full potential value.

Summary

The ways public and third sectors are currently delivered are highly wasteful for both service providers and users in terms of time, money and energy. Examples include ongoing reliance on paper based processes that could be digitised; on manual processes that could be automated, and widespread and unnecessary duplication and re-working of these processes. This is not the fault of front line workers but the result of the IT systems and processes they are required to work with.

Using new approaches to the collection and use of personal data it is possible to improve service quality while radically reducing friction, effort, risk and cost for both service providers and citizens.

These new approaches are based on systems for the sharing and re-use of known, checked information about citizens ('verified attributes'), under the citizen's control and in ways that protect citizens' data and privacy, to eliminate duplication of effort, reduce errors and fraud and minimise delays.

It is possible for countries like Scotland to implement these new approaches at very low cost, using systems and assets that have already been built, in ways that do not require large scale and risky changes to existing IT infrastructure and systems.

The outcome? Services that are 'just right for me' (i.e. properly personalised), that are really easy and safe to access and use, and that cost less, not more, to deliver.

Where we are now

Current ways of delivering public and third sector services can be cumbersome, costly and inefficient.They often result in poor experiences for service users, including delayed access to the services they need. This is not the fault of the people working in these organisations, who often go to the ends of the earth to provide the best service they can. The underlying reasons are structural and process-related.

- **Structural** Current ways of collecting and using the data needed for service provision rely on a large number of separate organisations each working in isolation. Across the system as a whole this creates endemic duplication of effort as each different organisation undertakes its own, separate data collection, checking, storage, and curation processes.
- **Process** Because there are no comprehensive, standardised systems in place to verify the veracity of data that citizens present about themselves when applying for services, many processes are still paper-based, requiring physical presentation and checking of paper documents. If they are not paper-based, they are often still manual. Citizens have to fill in forms manually and the data they enter has to be checked manually.

As a result, a high proportion of service providers' costs are devoted to manual checking and data processing activities, while citizens experience ongoing frustration as they find themselves having to present the same information many times over to different (or sometimes the same) service providers in ways that are costly in terms of both time, effort and travel. This creates barriers to accessing public services and delays in service delivery.

The Smart Entitlements Concept

The 'Smart Entitlement' Concept, as originally developed for the Scottish Government, tackles these structural and processes issues at source. Under the new approach, service providers:

a) mint secure electronic tokens [1] that verify facts about citizens (such as proofs of address, age, disability or educational qualification). The resulting 'verified attribute' is a piece of information about a person or performance

[1] 'Mint' refers to the act of generating a cryptographically protected electronic token that contains a verified attribute and associated metadata about its provenance and structure in and can therefore be trusted as much as the body that minted it. It is a way of transferring trust. Smart Entitlements are a form of verified attributes.

that has been generated or checked by a responsible, trustworthy body.

b) provide these tokens to citizens' personal data (or attribute) store via secure means (so that, for example, the attribute cannot be altered)

c) citizens can then share these tokens with other service providers, under their control, as and when they are needed.

Many public services already verify key attributes about citizens as part of their day-to-day activities. It is easy and cheap for these services to mint secure electronic tokens verifying this information, without interfering with any of their core operations. Doing so can and should be seen as part of the service. The necessary infrastructure for safe citizen attribute stores already exists (Mydex Community Interest Company) [2], and the technical feasibility of safe, efficient attribute sharing has already been demonstrated [3].

Under this infrastructure, once a verified attribute has been minted by a service provider, it can be provided to citizens and kept safe and secure on their personal data (or attribute) store. The information is kept up-to-date and accurate via persistent, secure delivery links using APIs [4]. This means the attributes remain 'on tap', ready to be used again and again, as necessary, at virtually zero incremental cost.

Key design principles of this approach are:

- That the citizen is 'self-sovereign' in the transaction. The citizen is the party holding and presenting the verified attributes, which in turn implies that these verified attributes have already been shared with the citizen.
- That it is privacy protecting: the minimum amount of information is shared at all times (e.g. proof of age does not require date of birth), and relying parties using this information are not building up new, centralised banks of data about this individual

This new privacy protecting approach to data sharing eliminates swathes of duplicated effort and cost from the system for both service providers and citizens.

[2] Mydex CIC has independently company wide ISO 27001certification and is recognised as a bona fide supplier to services to the public sector, being listed on the UK Government's G-Cloud platform for the procurement of public services.
[3] See the Report on the Verified Attribute Prototype
[4] API - Refers to application programme interfaces that can enable secure communication and exchange between different systems across the internet.

An Implementation Roadmap and Strategy

This simple but transformational approach to the safe, privacy protecting sharing of personal data can be implemented quickly and easily with low costs and low risks.

As a first step, the Government can enable a small number of key public sector attribute providers to make a chosen set of key verified attributes available to citizens via their personal data stores. The key criterion for choosing these initial attribute provides is that they process data points that are commonly and routinely used for applications, to assess entitlements and to deliver services, e.g. data held by passport, driving licence, benefit-providing or health authorities.

The initial focus of attribute provision can be focused on one or two services, where the attributes made available make it possible to transform the way in which these particular services are accessed, delivered and used.

Once this initial implementation is complete, it can be extended incrementally. The number and range of attribute providers can be progressively broadened, along with the range of verified attributes made available and the number and range of services that can use these verified attributes. Once all public services are covered, the system can be extended even further to include private sector services too. The number and range of citizen personal data (or attribute) stores, and the services they provide, can also be extended incrementally.

Here are some key things to note about this implementation strategy:

- It is doable, now, by any Government, under its own direction and leadership, using existing resources. It does not need to wait for, ask permission or rely on other, external organisations. With the data public sector organisations have already collected, Governments already have everything they need to start. In other words, this strategy builds on existing assets, based on what has already been done. It is grounded in today's realities.
- The incremental approach means the new system for the sharing of verified attributes can deliver immediate improvements to the costs and quality of service delivery, while avoiding the risks and disruption caused by attempting to make too many changes too fast. It does not require large scale, high risk investment in long-term IT projects that are likely to cost more than initially estimated, take much longer than originally intended, and deliver much less than originally promised.

It does not require any significant changes to existing back office systems or for existing organisations to significantly change their processes, culture, operations or systems. Instead, it connects with and integrates into existing systems, adding a new layer of capability, flexibility and opportunity. In short, taking this approach minimises disruption to existing operations and builds on existing capabilities.

- By helping both service providers and citizens reduce the time, money and effort they invest in accessing or providing services it generates compelling win-wins to gain active buy-in [5].

- It builds on existing relationships between citizens and service providers and existing data protection regulations (particularly Article 20 of GDPR on data portability). It does not require the creation of new, complicated data sharing relationships between organisations that previously had nothing to do with each other, and which require them to expose their systems to external parties. Other approaches to data sharing of individuals' data, such as 'Open Banking', require new inter-organisational data sharing systems that create added cost, complexity, privacy risks and compliance issues.

- At the same time, it builds infrastructure and capabilities that enable other, new services to be developed. Rather than sacrificing long-term goals for short term gains, as many 'quick fix' strategies do, it accelerates, deepens and extends its momentum as more attribute providers join the system to provide more attributes to citizens, enabling continuous improvement in service *plus* service innovation.

  A simple example of this momentum-building potential is the minting of digital copies of birth certificates during the certificate creation process. Placing them in the child's attribute store at this point means that the child now has access to this information for life, ready to use when needed. Further, new attributes can easily be added as the child grows up. Over time, these ongoing additions to the individual's personal data store result in the

[5] Some attribute providers may be reluctant to make verified attributes available to citizens, arguing that it involves them in extra costs for something which benefits other organisations. However, doing so is already widely accepted as being 'part of the service' as citizens ask for copies of documents such as birth and marriage certificates, passports or driving licences. Benefits of being a provider of verified attributes in digital form include: reducing the costs of providing paper copies of documents that are commonly requested by citizens; using the system to enable data sharing between internal systems that do not 'talk' to each other; avoiding the cyber risks associated with alternative approaches to digital data sharing e.g. from organisation to organisation; and improved compliance with the data portability requirements of GDPR.

creation of a rich, new, citizen-empowering data asset - a picture of the citizen's life. This would be held firmly by that citizen under their control, to be used by that citizen for their own purposes and further enabling the provision of more timely, more efficient, and more personalised services.

Also, as individuals accumulate more verified attributes about themselves, they can use the information to prove their identities. The UK Government has spent decades trying to crack the problem of online identity assurance. This infrastructure and approach solves the problem in a highly flexible, low cost way, as a by-product of the provision of citizen services.

In summary, this approach builds the generation and use of verified attributes into the way existing systems already work, in ways that generate close to zero risk and require minimal changes to current ways of working - but which builds momentum incrementally over time until it becomes part of how things work.

Specific implementation requirements

Of course, for any such system to work, it needs to meet certain specifications:

- Open source, based on open standards where available or open specification if not. This enables the development and deployment of reusable building blocks.
- Technology agnostic.
- Designed for interoperability.
- Minimise the need for internal systems changes to focus on the development of new layers of infrastructure and 'plug-in' tools and capabilities.
- Based on agreed definitions of verified attributes, metadata formats [6], data directories [7], and operating requirements for citizen attribute stores.

[6] Metadata is data about a piece of data (e.g. verified attribute), describing what that data contains, how it was collected, created, protected, maintained and updated and what its status is (e.g. the degree to which other parties can trust this data to be accurate and up to date). To be useful in an ecosystem based on the sharing of verified attributes, such metadata needs to be standardised as far as possible using easy-to-understand definitions that are unambiguous and precisely targeted to the context of the transactions they are used in. Such metadata must be machine readable.

[7] A data directory is a list of types of attributes (e.g. driving licence, proof of entitlement, proof of address) that are available and where they are available from - their sources. Directories do not hold the data points themselves. They hold metadata about the data - information relating to the nature and type of data that is available - plus routing information that makes it easy for those wanting to access verified attributes to find and access them. A directory is not an inventory of personal data about a citizen. An inventory is a personal list made available to the citizen when authenticated, advising them about what data they hold about them. Inventories will also

Conclusion

Thanks to the ways in which digital technologies evolved, today's data economy currently works on an entirely organisation-centric basis. Citizens, whose data is collected and used by organisations, are effectively excluded from active participation in the workings of this economy and therefore cannot directly access its benefits.

Unlike many other physical assets, data doesn't get 'used up' when it is used. It can, potentially, be used by many different parties for many different purposes. To unleash the full benefits of personal data, we need to move from a system where uses of this data are restricted to the priorities and purposes of the organisations concerned to one where citizens can also use their own data for their own purposes, including better, more efficient access to *all* those services needing to use their data.

The new approach to enabling the sharing of verified attributes described in this White Paper opens up a low risk, low cost way to make this transition from a 'one user, one use' data economy to a citizen empowered 'many users, many uses' system. This new approach, based on empowering citizens with their own personal data stores, not only provides an immediate solution to an immediate problem - the need to cut both citizens' and service providers' costs - it also opens the door to an increasingly wider range of data uses and services. It opens the door to a fairer, more innovative and richer data economy.

support GDPR implementation in relation to transparency and data portability. Data inventories are important for the future but are not required for this project.