The Role of Financial Institutions in Delivering Identity-as-a-Service for Governments

Why financial institutions make good identity service providers

In many countries, banks engender similar levels of trust to governments. In some countries they are even more trusted, with citizens investing their savings with banks or financial institutions, and many companies using banks as funding sources.

Trust

Trust itself is not binary, and the role of regulatory bodies and guarantee schemes is to help investors and borrowers keep faith. Banks and financial institutions are also protected, as they are forced into anti-money laundering (AML) and Know-Your-Customer (KYC) checks, which reduce and help quantify risk and maintain regulatory compliance. This circle of trust, powered by regulation and risk management, helps with keeping the symbiotic relationship between financial institutions and their customers. This is not similar when it comes to citizens and government, their relationship being somewhat different, with little perceived accountability and transparency. Banking regulation contributes to the Levels of Assurance (LoAs) for credentials and transactions, which can be partially mapped on to governmental LoAs determined by legislation (such as eIDAS), therefore bridging the gap between government and the finance sector, and enabling cross-purpose use.

Finance

Identity programmes need substantial take-up in order to be financially successful. That is precisely why governments prefer to use banks (among other financial institutions) as IDSPs. In developed countries, banks already have a relationship with a majority of the population, and these are coupled with KYC and AML checks. This means that the cost of enrolment may be shared with the normal financial onboarding process, thus saving substantial amounts of cost. Additionally, current authentication methods can often be re-used.

Contract

Governments are bound by rules set down by legislatures and agility is not always possible. Financial institutions, on the other hand, can have a contractually-based relationship with their customers. Service level agreements, liability caps and enhanced services such as insurance can all be offered, plus service differentiation between multiple IDSPs.

Architectures for Identity Service Providers

Direct and Derived Models

Direct Models are typical of the more basic schemes and were used by countries such as Austria, Estonia and Belgium. These schemes are based on smartcards primarily and the government acts as the IDSP. However, these have been recently utilising derived eID’s to overcome the legislative problems of mass mobile device usage, with an IDSP serving a secondary eID and using the original government eID as a major component in enrolment.

3-Corner Model

This is used by countries such as Denmark (NemID) and the Netherlands (DigiD). Here, the government contracts a third-party IDSP to provide enrolment and authentication. In the case of NemID, it also includes digital signing and the entire scheme was built and operated under contract.

Hub Model

This model is similar to the 3-Corner Model, except that the government owns and/or operates a hub(s), which accept(s) identity assertions from multiple accredited IDSPs. In the UK’s case, a user can have an enrolled identity in each IDSP. The hub acts as an air-gap between the IDSPs and the services, so that the IDSPs do not know which services are being used. Additionally, as there is no national registry, the Minimum Data Sets are relayed for each service provider to map the identity asserted to an existing user record. Germany has three private-sector owned hubs with associated IDSPs. Canada uses a single privately owned hub, accommodating private authentication (only) providers and an alternative government digital identity credential.

4-Corner Model

This is a more sophisticated model where counterparties with different IDSPs can interact through a hierarchy of trust, leading to a common ‘trust root’. In Norway’s case, it is owned by The Norwegian Financial Services and Saving Banks Associations.
In this model, the government portal is one of the many relying parties.

Examples of Banking Implementations

NemID Denmark

NemID was chosen in 2010, and it is operated in a private-public partnership between NETS and the Danish government. It is server-centric and was originally TAN (Temporary Authentication Number) card based, but now uses mobile OPT (One Time Passwords). NemID can be used for bank access as well as business and eGovernment services. It is used on average once every three days by every citizen. NemID will be connected to the Connecting Europe Facility through Denmark’s eIDAS node for mutual recognitions across the EU.

BankID Norway

With the large number of Norwegian banks, the need for a common method of authentication resulted in BankID, formed and operated by BBS (now NETS). In 2014, there was an agreement between BankID and the Norwegian government to use BankID as authentication for eGov services accessible through the government’s portal. BankID still maintains usage of about 1.4 million authentications per day (out of a total population of about 4.5 million citizens).

Barclays Bank UK

Barclays Bank is a multi-IDSP hub and one of the certified IDSPs for UK.GOV.Verify. Barclays Bank uses its enrolment and registration systems to supplement its own bespoke UK.GOV.Verify systems to provide a rich registration and strong trust branding. A minimum data set, determined by the UK government, is transmitted together with the identity assertion to enable the matching with the various UK government agencies, as there is no central registry in the UK.

Conclusions

Financial institutions, and banks in particular, are ideally placed to become the IDSPs of governments, and whilst it may not be the only business sector able to fulfil the role, they have an advantage due to their regulated environment and risk management philosophies.