The checking of identity documents in the digital identity ecosystem

Background

The ADVP is a trade association representing companies that provide electronic validation of identity documents in the UK. Its members deploy a wide range of technology solutions that are used across the public and private sectors to check millions of identity documents every year for a multitude of purposes including remote onboarding of customers or employees.

The ADVP has been engaged in much of the work around the development of a UK digital identity ecosystem – particularly through OIX and direct contact with GDS. Whilst there are a significant number of workstreams regarding the construct of a safe and robust digital identity ecosystem, the ADVP interest / input is focused on the electronic validation of identity documents where needed as part the creation of a digital identity.

The ADVP has a digital identity subgroup which has identified a number of areas that the ADVP could actively help in the formulation of appropriate policy regarding identity document validation and this paper aims to set those out.

Validation levels

The electronic validation of identity documents can take place several ways:

- The presentation of a physical identity document to be scanned on a specialist identity document reader.
- The presentation of a physical document to be scanned using a mobile device.
- Presentation of an image of an identity document to be checked remotely via Cloud based validation technology.
- The addition of various biometric checks (facial recognition, liveness tests) to reinforce the remote document checking processes.

Clearly the different methods described above result in a varying range of validation levels, with the scanning of physical documents on specialist readers being more robust than a Cloud based validation of an image. In the work carried out thus far by the ADVP, it is accepted that such variations of validation exist and that digital identity providers should therefore make an appropriate risk assessment before selecting the ‘appropriate’ electronic identity document validation solution. However, what is less clear is how much reference material exists to support that ‘appropriate’

selection. GPG 45 is a very detailed document and sets out the various levels of validation that can be considered, but does not match the levels (with the additional work, cost and time associated with higher levels of validation) to various user scenarios – it is left to the digital identity provider to make that ultimate decision. The first draft of BS 8626 also sets out some considerations that should be considered for identity document validation, but nowhere does it mention electronic validation as a supporting tool / option.

How the ADVP can help

The ADVP is not questioning the approach of either GPG 45 or BS 8626 but feels it can add another layer of information to help digital identity providers make a more informed decision regarding the choice of appropriate identity document validation solution. Specifically, it can help provide the following to enhance best practice in the digital identity ecosystem:

1. Intelligence

By virtue of the validation methodology being electronic, the detection of any fake documents can be easily evaluated, and intelligence developed. At a tactical level, the intelligence can inform a digital identity provider of the following:

- The number of fake documents being detected.
- What type of documents are being detected.
- What security features are being defeated.
- What purported nationalities are being used.

At a strategic level, if multiple digital identity providers shared this intelligence via their electronic identity document validation provider, the intelligence could inform:

- Specific weaknesses in the ecosystem.
- Digital identity providers at higher risk.
- Variations in detection rates across different electronic validation solutions.

The ADVP is also working with the Metropolitan Police Amberhill team to enhance the intelligence sharing between law enforcement and industry to further improve protection against the wider use of fake documents. Whilst the fake document has been detected by the digital identity provider (and hopefully all other providers would also detect and prevent its use if using similar technology) the holder may still try and access other services that do not widely deploy electronic validation systems but could check an identity document number against the Amberhill database. The sharing of intelligence would also assist in the scenario where one digital identity provider may have used a far more robust validation system with higher detection rates for its onboarding than other providers using less sophisticated tools due to their lower risk assessment and therefore the sharing of the fake data would enhance protection for all users in the ecosystem irrespective of electronic identity document validation system deployed.

2. Standards

Should the use of electronic identity document validation technology become common in the digital identity ecosystem, then there must be a set of standards by which the provider can rely on its supplier to deliver the appropriate level of validation as defined by its risk assessment. As subject matter experts, the ADVP can be central to defining and managing those standards. Possible ways of doing so could include:

- Comparison of fake document intelligence by solution type (scanner, mobile or Cloud) by independent assessors.
- Regular testing of ADVP member solutions by independent assessors with access to sufficient recently detected fake documents (original or manufactured).

3. Matching risk to most appropriate electronic identity document validation solution

By using intelligence and being certain that a supplier solution reliably validates to the level specified, a digital identity provider can make a more informed decision regarding the most appropriate solution to mitigate the defined risk. It is already an accepted fact that in certain sections of society the quality of fake documents used is very poor (e.g. Right to Work checks in construction) and it is likely these same documents will be used to access low level services should they become digitally accessible and therefore the validation requirement could be on the low end of the risk spectrum. However, organisations facing a higher risk threshold may never accept anything other than the most robust scanner enabled document validation (requiring the applicant to present their identity document in person) as part of the digital identity onboarding process.

Working with other government / law enforcement agencies (National Document Fraud Unit, Amberhill team) and interested trade bodies and organisations (Criminal Records Trade Body, CIFAS) the ADVP could create a guidance template that defines the level of detection capability of the various solution available against the risk to be mitigated.

Immediate key strategic benefits from ADVP input to the creation of a UK digital identity ecosystem

1. Provision of clear and unambiguous intelligence that can help inform appropriate government agencies considering changes to various legislation to make the non-physical presentation of original documents allowable – an important enabler of digital identity. The removal of legislative barriers to electronic document checks, where face-to-face checks involving original identity documents are mandated, would bring an immediate benefit to businesses that are obliged to carry out these checks. Legislative recognition of the importance of digital identification would also be a precursor to future

digital identity schemes; digital identification of identity documents will be a component of the creation of digital identities.
2. Provision of evidence that fake documents will be detected across all electronic validation solutions thereby giving wider comfort to users of digital identity and creating a deterrence to potential users of such documents to create false digital identities.
3. Inform current digital identity projects of the range of options and associated validation levels (and therefore risks) when considering electronic validation of identity documents as part of the secure onboarding process.

Conclusion

The ADVP membership carries out a significant percentage of in-country identity document checks. The expertise it has in identity document validation, combined with an unrivalled source of intelligence relating to fake document detection, makes it well placed to help both government and relevant private sectors to better deploy appropriate technology to ensure the UK digital identity ecosystem is secure and trusted.

29 September 2020