Proposal

HMG DCS availability discovery

Requirement

HM Government issued documents and their associated attributes are an important element to a UK based identity check in both the face to face and online channels. A significant proportion of identity checks in both the private and public sectors use either a UK driving licence or passport as acceptable evidence as part of an identity check. This is due to strong document issuance processes and the presence of biometric, cryptographic and security features on the evidence.

There are a variety of private sector use cases that utilise such evidence including anti money laundering checks (e.g. finance, gambling, legal transactions etc.) and age verification checks (enabling the purchase of age restricted good and services).

The availability of a validation source for these documents is important to ascertain that the evidence has been issued by the relevant authority, to the person claiming the identity. These checks should also determine whether the document has been revoked or reported lost/stolen, and is therefore still valid as identity evidence. Valid evidence checks are an important element identity check in accordance with recognised good practice including Good Practice guide 45[1] developed by the Cabinet Office and NCSC.

The GOV.UK Verify programme within the Government Digital Service (GDS) developed the document checking service (DCS) ahead of the initial private beta in 2013 and subsequent live service. This allowed the contracted identity providers to check asserted document attributes against issuing sources (Driving licenses in England Scotland and Wales through DVLA and DVA for Northern Ireland, UK issued passports through HM Passport Office). This enabled a number of combinations of identity evidence types to be used, thus widening demographic reach for UK public sector Identity assurance as 76% of people in England and Wales hold a UK passport and 74% of people aged 17 years and over in England hold a full driving licence.

The ability to validate evidence against either an issuing or authoritative source both ensures alignment to recognised standards and allows a user to reuse their resulting digital identities across the public and potentially the private sector. The development of a standards based private sector identity ecosystem is heavily reliant on evidence validation checks for UK passports and driving licenses to ensure a wide demographic reach and success rate.

---

[1] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

 V0.2

DRAFT: Not for distribution

However, the current DCS implementation is only available to the identity providers on the GOV.UK Verify framework for use in the public sector and they are not permitted to re-use the trust elements obtained by the DCS in the private sector. Thus there is a requirement to allow the current Verify framework identity providers to use their existing checks and undertake new checks with DCS to support private sector customers (relying parties). Other, non GOV.UK Verify identity providers also have a need to create identities to support private sector customers in accordance with recognised standards using the DCS.

The establishment of a framework for sharing HMG attributes for use in the private sector will enable other government departments and agencies to make their attributes available for private sector identity checks.

Scope of work

The proposed discovery would explore:

- The economic value of the DCS attributes to the private sector
- How *existing* Verify Identity providers could use the *existing* trust from DCS (HMPO, DVLA and DV) to support private sector relying parties.
- How *existing* Verify Identity providers could create *new* digital identities in support of private sector relying parties utilising the trust from the DCS.
- How *non-Verify* identity providers could create *new* digital identities in support of private sector relying parties utilising the trust from the DCS.
- What areas need to be considered to enable the above (e.g. Policy, legal, liability, technical , performance, commercial, operational, security and privacy) ?
- Whether these are viewed as constraints and how can these these be addressed?
- Whether DCS attributes only be shared with Identity providers or should they be made available to any private sector organisation as long as certain criteria are met (e.g. process alignment to standards, security handling, information assurance etc.)?

DRAFT: Not for distribution

Proposal

HMG DCS availability discovery

ID CROWD

Expected outcomes

Recommendations on how to enable private sector re-use of DCS that considers:

- An outline economic benefits case of the DCS attributes in the private sector
- A stakeholder management strategy to mitigate policy and legal considerations
- A need for commercial strategy (including the implications of state aid, HMG data policies, potential pricing and liability considerations)
- Technical infrastructure (including mitigating potential performance and/or privacy concerns)
- Operational strategy (e.g. which bodies would develop and management the attribute sharing service and a potential transition strategy? What are the other operational requirements for instance PKI management, audit, billing etc?)
- A roadmap for implementation (including scope of an alpha)

Tasks

- Agree scope, milestones and outcomes
- Define a stakeholder engagement and management strategy
- Undertake business case analysis
- Undertake policy & legal assessments
- Undertake technical assessment
- Undertake commercial assessment
- Undertake operation assessment
- Develop a strawman for a high level framework for HMG data sharing
- Define a roadmap towards implementation
- Report on recommendations, constraints

Deliverables

Report detailing the economic benefits, recommendations, considerations and roadmap for a framework to allow certain HMG datasets to be used in the private sector for identity assurance.

Terms, conditions and requirements

- GDS will act as contact point for HMG engagement
- GDS will ensure correct stakeholders in relevant HMG departments are available including HMPO, DVLA, DCMS, DVA, HM Treasury.
- Participating organisations would be request to provide logistical support, e.g. meeting rooms.

Proposal

HMG DCS availability discovery

Why ID Crowd?

ID Crowd is a consultancy with a proven track record of defining and delivering world class, population scale trust ecosystems. Our team have been responsible for significant developments with regards to trust ecosystems, these include:

- Delivery of the GOV.UK Verify trust ecosystem since its inception with the Cabinet Office and DWP in 2011
    - Product management and design of the original document checking service (DCS) in 2013 for the GOV.UK Verify programme including stakeholder management, technical, policy and privacy elements.
    - Defining the hub architecture and SAML integration specifications.
    - Defining the scheme rules in the Operations Manual.
    - Leading identity provider procurement for both frameworks.
    - Defining the delivery assurance processes in the service delivery requirements (SDR).
    - Assuring the identity providers against the specifications, including GPGs 44 and 45.
    - Defining the contractual framework.
- Authoring and contributing to recognised digital identity standards including the UK Governments Good Practice Guide 45 (GPGs), and US Governments NIST 800-63.
- Ongoing development of a model for a UK private sector trust ecosystem.

© the ID Crowd 2019 V0.2

DRAFT: Not for distribution