Response to DCMS Digital Identity: Call for Evidence

This response has been produced by [members of] the W3C Verifiable Credentials Working Group (VC WG) and is public. We use the following terminology in this document:

- Issuer is the digital credential issuer,
- Citizen, person, user is the holder of the digital credential,
- Verifier is the recipient of the digital credential and offers a service to the holder.

1. Do you think digital identity checking will be a way to help meet the common needs of individuals and organisations referenced above? What other ideas or options would help?

We think that the needs identified in the Call are a good, albeit small, representative sample of the needs of individuals and organisations. The W3C VC WG has produced a much larger sample of use cases, in its Use Cases document, which is publicly available here:

https://www.w3.org/TR/verifiable-claims-use-cases/

This covers use cases in: finance, health care, education, retail, legal and professional. We hasten to add that this is not a complete set of use cases, but is a representative sample aimed at giving the reader the general idea of the value and need for digital identity credentials. Many more use case exist than those we have highlighted here.

2. What are the economic or social benefits or costs from developing a digital identity system in the UK which meets these needs? Can you provide examples?

The economic and social benefits are huge. There are many online tasks that cannot be performed today due to the lack of a robust, secure and privacy protecting digital identity system. One example is opening up a new bank account online. Another is <***add some more here>.*** Other tasks are currently being performed online in a sub-optimal way, for example, when only the age of someone is required, the individual has to provide an electronic copy of an entire physical credential, thereby revealing his or her name and address as well. <***add some more here>.***

Whatever digital identity system the UK chooses to implement, it needs to be international in scope rather than national, and based on international standards. Degree certificates issued in Europe or America need to be recognised in the UK, as do driving licenses, health insurance cards and the like. The W3C Verifiable Credentials Data Model recommendation is one of the essential international standard building blocks that will be needed (although we note that on its own it is insufficient to specify an entire identity eco-system).

3. What are the costs and burdens of current identity verification processes?

Some of these costs are very large. Bank KYC takes several days of human effort to verify a new customer. The NHS pays employment agencies millions of pounds a year to validate the credentials of temporary staff. One UK university spends £20,000 per annum to issue plastic ID cards to its visitors, students and staff. < ***add some more here>.***

4. How should we ensure inclusion, especially for individuals with thin files?

This is indeed a problem. But it is not a new one. Today, people without an entry in a UK credit reference bureau's files, find it impossible to enter into a mobile phone contract. The UK government can help to alleviate this problem since they have one or more records of virtually every person legally in the UK, for example: everyone born and registered in the UK, everyone working legally in the UK, everyone with a UK passport or driving license, everyone with a NHS card etc. By issuing these as digital identity credentials will help enormously to kick start the digital identity eco-system.

5. What currently prevents organisations from meeting the needs stated above?

There are several inhibiting factors. First we have the chicken and egg situation. Why issue a digital credential if there are no verifiers? Why build a system to accept digital credentials if there are no issuers? So there is a big inertia to getting started. Second, digital credential issuers do not have the motivation or business case for issuing digital credentials when the primary beneficiary is the verifier. For example, say an online seller of alcohol wants proof of the customer's age, as determined by say an electronic driving license, then the cost falls on the issuing authority whilst the benefit accrues to the verifying merchant. How can the issuer benefit from this? A third inhibitor is lack of trust. The verifier has to trust the issuer, but if this trust fails, the verifier incurs the cost. For example, if the online retailer sells alcohol to a minor due to the mis-issuing of the driving license, the retailer may be prosecuted and has no comeback on the issuer.

6. Where do you see opportunities for a reusable digital identity to add value to services? Could you provide examples.

The VC Use Cases document contains many examples. Here is one copied from there:

- Susan wants to send funds to her family in another country via a popular money transfer service. She has verifiable claims in her credential repository that can be used to share her identity profile. She has also been sent a claim from her family verifying their banking information. By sharing these with the money transfer service, it can automatically verify the source and destination of funds, thus being confident in the delivery of those funds and satisfying various regulations regarding prevention of money laundering.

7. What are the building blocks essential to creating this trust? How should the environment be created to enable this trust – for example, what is the role of open standards (identity, technical, operational, business implementation, design requirements for consumer privacy and protection)?

In this identity ecosystem the verifier has to trust the credential issuer, and it is in the nature of trust that when it fails, all the costs are incurred by the verifier (the trustor). Consequently, the building blocks should primarily be aimed at lowering the impact on the verifier i.e. lowering the amount of trust/risk that the verifier has to place in the identity eco-system. Mechanisms that can facilitate this are:

i) Strong cryptography which prevents credentials from being forged;

ii) Selective disclosure which helps the verifier conform to GDPR by only requesting and receiving the identity attributes that are required for the service;
iii) Having a credential ecosystem that conforms to international standards, meaning that the protocols, data structures, ontologies, cryptographic algorithms etc. have been rigorously verified by international experts and are the state of the art;
iv) Using trusted issuers that are globally trusted and have high reputations, such as governments and international organisations

8. How does assurance and certification help build trust?

All procedures that lower the risk to the verifier (and hence the amount of trust it needs to place in the eco-system) can be beneficial. So the certification of issuers could help. However, if the cost to the issuer of getting certified is prohibitive, it will have a negative effect on the ecosystem, by discouraging issuers from participating (remembering that it is the verifiers and users that usually have the most to gain from digital credentials). Certification of the software being used by issuers, users and verifiers can also help, but again, the cost must not be prohibitive.

9. How do we ensure an approach that protects the privacy of users, and is able to cover a range of technologies and respond appropriately to innovation (such as biometrics)?

The privacy of users is best protected by:

a) Selective disclosure, so that users only need to release the minimum amount of identity information that is required to obtain the service. Note that there are various technical ways of achieving this and the W3C Verifiable Credentials Implementation Guidelines provides 3 examples, see:

https://w3c.github.io/vc-imp-guide/#selective-disclosure

b) Zero knowledge proofs, meaning that the recipient gains no further knowledge from the protocol exchange between it and the user. The W3C Web Authentication Protocol is one such protocol, see

https://www.w3.org/TR/webauthn/

and work is currently underway to allow this protocol to be used to transfer W3C Verifiable Credentials. Biometrics can be used by this protocol to authenticate the user before granting them access to its cryptographic keys.

10. How do we ensure digital identities comply with the Human Rights Act and ensure people with protected characteristics are able to participate equally?

A well-constructed digital identity eco-system, like the one proposed by W3C Verifiable Credentials, ensures that no personal details have to be released to the verifier other than those that are essential to provide the service. Thus, if the protected characteristics do not need to be known to the verifier they will not be released. If they do need to be known, then a mechanism such as Trust Negotiation can be used between the user and verifier so that the user knows (s)he is talking to a trusted verifier before releasing the protected characteristics.

11. How should the roles, responsibilities and liabilities of players in the digital identity market be governed and framed to enable trust?

These should mirror the ones that are used today in the physical world. There is not a one size fits all model, but rather different identity eco-systems will have different responsibilities and liabilities. For example, when a person uses a passport to travel to another country, or a person uses a supermarket card to obtain a discount, the roles and responsibilities of the actors is quite different. Using digital credentials is essentially no different to using physical ones.

12. What's the best model to set the "rules of the road" to ensure creation of this trusted market?

As stated above there is no single best model. But rather, those that are used today in the physical world e.g. with plastic cards, driving licenses etc. should be transposed to the electronic world.

13. Who do you think should be involved in setting these rules?

Each identity ecosystem will have its own rules. The rules for using plastic credit cards are very different to those for using passports, and it will be the same in the digital world. The stakeholders in each digital identity eco-system will determine their own rules.

14. Do you think government should make government documents and/or their associated attributes available in a digital form, which could be used to help assure identity?

Absolutely. Governments have a major kickstarting role to play in all future digital identity ecosystems. The UK government is a highly trusted organisation and the issuer of critical physical credentials today such as passports, driving licenses etc. It should become the leader in the issuing of digital identities.

15. i) For what purposes should government seek to further open up the validity checking of government-issued documents such as passports?
ii) How should this be governed to ensure protection and citizen control of data?
iii) What should the cost model be?

i) The government should not try to control the purposes for which its citizens use their digital identities. It does not control today what a citizen does with his/her paper passport, and it should not control what they do in the future with their digital ones. Instead, the government should try to enable its citizens to be more privacy protecting with their digital identities, by allowing them to selectively disclose any single attribute from their government issued identity, to whichever verifier they decide (without government interference). This will facilitate the growth and take up of the digital identity market.

ii) The citizens should have their digital identities on their devices, and should have total control over which attributes they release to which verifiers at which time. This is exactly in line with the W3C Verifiable Credentials Data Model.

iii) Citizens should be charged for the issuing of their digital identities, in just the same way that they are charged today for their paper or plastic credentials such as driving licenses and passports.

16. i) For what purposes should government seek to further open up the attributes (such as age of citizens) that it holds for verification?
ii) How should this be governed to ensure protection and citizen control of data?
iii) What should the cost model be?

i) The government should not try to control the purposes for which its citizens choose to reveal their ages. They do not do that today in the physical world. On the contrary, the government should provide its citizens with proof of age credentials and allow the citizens to use them for whatever purpose they choose.
ii) Legislation such as GDPR and age discrimination govern when verifiers can ask for a person's age, and what they can do with that attribute. Selective disclosure provides the holders with total control over when they will reveal their ages to verifiers.
iii) Verifiers can be made to pay the government issuer a micro-payment every time they ask for a government issued age attribute. The verifier is benefitting from using electronic credentials, and is reducing its costs by using them. Therefore, part of this benefit can be used to reward the issuer for issuing the credential.

17. What's the role of legislation and statutory regulation to grow and enforce a secure, privacy-centric and trusted digital identity market?

The UK law on adult web sites is a good example of this. The UK government requires adult web sites to only make its content available to adults over the age of 18, and it will be an offence to not do so. The government could additionally mandate that sites have to be certified before they can operate legally. Then the government lets the market decide how to achieve this certification, using whichever technologies it chooses, because the government's role is not to specify technologies. However, the government sets the criteria for certification that sites must achieve in order to be certified as trusted, privacy centric and secure. International standards will eventually be specified to reach or surpass these criteria, but until they are, proprietary technologies can be used to gain certification.

18. What legislation and guidance requires updating to enable greater use of digital identities?

No response

19. What else should government do to enable the wider use of digital identity?

We have already suggested that they should become the leaders in issuing digital identities, and pass legislation mandating stronger identity assurance for electronic services that today simply require the user to be honest about their age.

20. How could digital identity support the provision of local government services (including library cards and concessionary travel)

Wherever paper or plastic credentials are being used today, such as concessionary travel, then the digital equivalent of them can be issued to holders in parallel. A citizen would then

either show their physical or electronic credential in order to obtain the local government service. Another example is that cars (or their owners) could be given their own digital identity certificates authorising them to park in restricted areas of a town. Furthermore, new services, that are not available today, can also be devised once the basic electronic infrastructure is enabled. For example, assuming that the theft of dustbins is a costly problem for a local council, then it could have chips and identity certificates installed in them all, and they would only be emptied by the local authority if they belonged to it and the householder.

21. What is the private sector's role in helping to create a trust model (based on the criteria for trust in section 5), and how should they remain involved in its long-term sustainability (for example funding, helping create the rules of the road)?

The private sector is going to be both credential issuers and credential verifiers. Where one company plays both roles e.g. issuing/verifying a supermarket loyalty card, then it can set its own rules, and compute the cost/benefit advantage of moving to electronic credentials. (Note that some US supermarkets have already determined the benefits of this e.g. issuing discount coupons to customers as electronic credentials.) Where an industry consortium plays both roles e.g. electronic credit cards, then again it can determine the rules for its identity eco-system. Where governments and the private sector participate in the same identity eco-system then the appropriate business model is essential to make sure that all the stakeholders are winners, and that the government is not subsidising one part of the market. We have given one example earlier, where the citizen purchases the electronic credential from the government issuer, and the private verifier pays the government a micro-charge each time it is used. Depending upon the charging structure and frequency of use, it could be that citizens are even given the electronic credential for free.