Response by John Harrison of PIB-d Ltd to:

DCMS's 'Digital identity: call for evidence July 2019'

This response amounts to some 7,000 words, well above your recommending maximum of 2,000. Sorry. But I have been involved in 'identity' for more years than most, know the subject well, and wish to make certain points which seem important, and may not reach you from other directions. Other text is necessary to put these points in context.

In your response, please clarify:

a) if you're responding on behalf of an organisation or in a personal capacity

I am responding in two capacities. First, I'm a director of PIB-d Ltd, a hybrid company half owned by the UK's education sector (specifically Jisc and the University of Hertfordshire) and half owned privately. PIB-d was set up in 2011 to develop what we now call a 'Personal Data Ecosystem, starting in Education' (PDE-E), of which more below. After completing a technical feasibility study, the company was made dormant towards the end of 2012 when it became apparent that the public sector's appetite for digital identity schemes would be met by gov.uk Verify for some years to come.

Now that Verify's star is waning, the PDE-E ideas may yet be of use: they are summarised in response to question 1 (b) and 7; the consequences follow in response to other questions.

Over the years, PDE-E has been discussed with many stakeholders, not least the Department of Education and GDS. My interpretation of their views, and of the current positions of Jisc and the University of Hertfordshire, is given in response to question 5.

The second capacity in which I am responding is as a private individual, specifically one who - while PIB-d was dormant - has earned part of his living by acting (via Lloyds Register) as the tScheme assessor for most of the Verify identity providers. While this work has informed my views of the digital identity space, I would stress that I am not representing either tScheme or Lloyds Register: the views expressed here are my own, to the extent they are separate from those of PIB-d.

b) which questions you're answering, by referring to our numbering system - there's no need to respond to all of the questions if they are not all relevant to you

See below

c) whether you're willing to be contacted - if so, please provide contact details

Yes, I am willing to be contacted. I have already presented PDE-E to Andrew Elliot and Caroline France at DCMS. Further, I am a participant in the Alternative Architectures working group within the current techUK-OIX identity initiative.

My work email is john.harrison@pib-d.net; my mobile number is 07801 231 693

Questions on needs and problems

1. (a) Do you think digital identity checking will be a way to help meet the common needs of individuals and organisations referenced above?

Yes, the UK - and individuals and organisations within it - needs a better approach to digital identity and related infrastructure.

However, the experience with gov.uk Verify has shown clearly that the GDS philosophy of tackling one small issue at a time, and only then considering subsequent issues, does **NOT** work. Rather there is a need first to develop a clear shared vision of the mature infrastructure, so that each incremental step takes us in the correct direction.

Thus this response advocates one such vision: a general purpose infrastructure for user control of trustworthy personal data, including (but not limited to) identity and money.

1. (b) What other ideas or options would help?

There is, in fact, no shortage of information about digital identities. Banks know the identities of their customers and employees, as do learning providers, healthcare providers, local authorities etc. Where they differ is in the level of assurance achieved: banks undertake detailed diligence, and so achieve a reasonably high level; others often do less, according to their needs.

Thus the most efficient way to fix the 'identity' problem is not to create a market of standalone identity providers, Verify-style, but rather to enable individuals to take trustworthy personal data, including (but not limited to) identity attributes, from the organisations they already deal with, aggregate it when necessary, and show the result to others.

This is the idea of a Personal Data Service, sometimes known as an e-wallet or 'self-sovereign' or 'decentralised' identity. Defined formally, a PDS is a point in the network used by the individual to: (i) link to many different counterparties, both organisation and other individuals; and (ii) control the sharing of trusted personal data to and between them. Such data may include: authentication data (i.e. the results of the username-password process, or better); identity data; and other attributes (e.g. preferences, qualifications, prescriptions, authorizations etc).

Further:

- There's an open question as to whether a PDS should reside purely on an individual's personal device, or be provided as a service by an organisation: the answer is likely to require an online component, probably provided by an organisation, so as to make possible transactions – such as checking that a delegation is still valid – which do not need the individual's active participation; direct debits provide a useful parallel here.
- Assuming that organisations - PDS providers - are involved, there's a need for a managed market (or ecosystem) of such providers, so that individuals have choice. We call such a managed market a Personal Data Ecosystem (PDE), and still believe that it is likely to flourish first in the Education sector (whence PDE-E), using a Portable Personal Achievement Record as the flagship application.
- Choice between PDS providers implies the need for easy account portability. And there's also a need for PDS account inter-operability, so that one individual can set up a relationship with, and show personal data to, another. In fact, account interoperability is essential, since (i) it is necessary for delegation-type transactions; and (ii) it will enable an individual to maintain person-person relationships beyond the context - say a university or FE college or school - in which they were first established, so strengthening the motivation to maintain a PDS first acquired within that context.
- In a Personal Data Ecosystem, specialist Verify-style 'identity providers (IdPs)' are only required when the level of identity assurance available from conventional service providers (e.g. a bank, or employer, or learning provider) is insufficient to meet the needs of a new counterparty. For example, Verify currently delivers a maximum level of assurance (LOA) of

2. And yet the Land Registry needs LOA3 for high-value property purchases. An individual using a PDS able to 'deliver' LOA2, based on existing relationships, could contact a specialist IdP to uplift their identity to LOA3, based perhaps on a face-to-face interview.

- Because individual choice is provided at the PDS level, it seems likely that there would only be a need for one or two specialist IdPs, allowing useful economies of scale compared to the 5 active currently within Verify. Further, such IdPs could be selected through conventional procurement, and easily replaced at contract expiry, avoiding the need to resort to the peculiar procurement methods used for Verify.

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?**

My response to this question is split into three: benefits seen by society; by individuals; and by organisations.

Benefits seen by the whole of society

- Provision of missing functionality, principally
  - Delegation: allowing a parent to act more easily for a child, or a carer to act for a vulnerable adult, both informally and - if required - under the formal terms of a power of attorney.
  - Secure communication: since email is not regarded as secure, organisations (such as HMRC) have to send sensitive messages to a personal mail box on their own services, and alert an individual to their presence by email; a PDE would fix this problem, providing a general purpose secure comms system.
  - Attribute exchange: A system focused narrowly on 'identity' does little to help the individual convey other trustworthy information (generally called 'attributes' or - by the Americans - 'claims') between counterparties. Examples include counterparty-specific identifiers (such as NINO, NHS number, email address), a white-list DBS attribute, medical prescriptions, delegated authorizations ("keys") to enter physical or digital properties, etc. A PDE would fix this issue, being a general purpose infrastructure for user-control of attributes, defined broadly to include 'identity'.

Benefits seen by individuals

- Lower switching costs, as individuals: (i) do not have to register, and sign-on, separately for every service; and (ii) can aggregate records from, or transfer records between, such services more easily. As a result, we may see : (i) a reduction in the tendency of the web to create and sustain near monopolies - such as Amazon and Facebook - leading to healthier competition between smaller players; and (ii) individuals using one or more PDSs to maintain their own trustworthy records - in health, dentistry, education, etc - and giving professionals access, rather than vice-versa. Note that account portability *between PDS providers* will be designed in from the start.
- Privacy. There are some transactions where, using present systems, individuals are obliged to disclose more personal information than is strictly necessary, e.g. disclosing full name, and date-of-birth when: (i) buying a drink (only a photo, and a statement that age is above the threshold, should be required); (ii) visiting a STI clinic (only an attribute evidencing entitlement to NHS care should be required); and (iii) ordering goods online.

- Enhanced convenience, as individuals no longer have to manage as so many different usernames and passwords, relying instead on just one (or a small number) of PDS providers as a channel to interact with many different counterparties.
- Enhanced security, as individuals rely upon a much smaller number of online accounts, and therefore value each more highly, monitor each more closely, and are willing to implement stronger security measures.

Benefits seen by organisations

- Lower operating costs. A PDE can be seen as the result of convergence between payment and certain elements of 'enterprise IT' systems. Once the costs of change have been absorbed, overall operating costs should fall as organisations incur a single invoice for a service combining user authentication, user identification, and payment.
- Reduced fraud. At present, we make conventional electronic payments to bank account numbers; the name of the individual or organisation associated with the account number is secondary. This allows fraudsters an opportunity to con individuals into sending payments to their own accounts. A PDE would allow payments to be made directly to a payee, with an appropriately assured identity, so reducing the potential for fraud. It is then for the payee to determine into which bank account the money is eventually payed. Paypal (before it gained some bank-like characteristics) began to show how this might work; while Circle shows that it's possible to disassociate payment card and bank account.
- Compliance with GDPR. A PDE would empower individuals to be their own data controllers, and so would simplify the burden faced by organisations in ensuring compliance with GDPR. The Information Commissioner's Office is aware of this potential, and is generally supportive of PDE-E type schemes.

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

No answer here. The current costs and burdens are the mirror image of the benefits described above; and it is a difficult task to try and quantify them accurately. Ctrl-Shift (see their website, or speak to Liz Brandt) – and others – have tried, and generally arrive at figures in the billions. That said, an exercise to quantify the potential effects of a PDE on reducing payment fraud would be timely.

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

Many of the individuals with 'thin files' are young people, who have not yet built up a sufficient credit history, and/ or may not have acquired a passport or driving licence. This issue can be mitigated by enabling them to use data from their educational career as a contribution towards identity proofing. Not coincidentally, PIB-d's PDE-E proposal starts in education, with a Portable Personal Achievement Record as the flagship application.

We plan, in the early days, to run pilots in a secondary school (from age 11 or so), an FE college and a university. Eventually, babies may acquire a PDS - with control exercised by their parents / guardian - and use it to maintain a link to their birth certificate.

Adults who are not well established in society may also often suffer from the 'thin-file' issue, perhaps because they are recent immigrants or homeless. In these cases, the likely solution is for a trusted public sector entity - respectively the Home Office and local authorities - to vouch for them electronically, providing identity data that can then be shown to others via a PDS. Verify's planned Etive project was a step in this direction, but now is unlikely to happen - in part, I suspect, because of a poor fit with Verify's underlying architecture.

Finally, there's a risk that less able individuals - whether the young, the old, or the handicapped - might be excluded from using a PDS because of a complex user interface. The solution is first to ensure that the UI is as intuitive as possible, relying extensively on pre-set defaults; and second to ensure an effective delegation mechanism, so that a carer (or someone with power of attorney) can manage a PDS on behalf of another.

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

The technology required for a PDE can be, and is being, built; and many stakeholders in the private and education sectors support the approach. But implementation is not possible until key public sector stakeholders also lend their support – which is a big ask given the levels of risk aversion in government departments. In more detail:

- a number of leading computer science, information security, and educational technology academics are supportive: I might mention here Anthony Finkelstein (CSA for National Security); Jon Crowcroft (Cambridge); Rose Luckin (UCL); and Chris Hankin (Imperial).
- the University of Hertfordshire remains interested in leading local pilots, working with associated FE colleges and secondary schools, *provided* such pilots are seen to have the potential to roll out at national scale, i.e. they need support from central government.
- Jisc's chief exec comments – and I paraphrase - that: (i) the universities, and education sector generally, will only adopt PDE-E once it is mandated (or at least strongly recommended) by government; and that (ii) the scheme can only succeed if it offers proof of identity, as well as a portable personal achievement record, at an early stage.
- Private sector companies generally accept the logic behind PDE-E, and are willing to back the scheme - either as PDS hosts, service providers, software providers or investors - provided that there is sufficient evidence of coherent support from government.
- Senior individuals at OIX and tScheme are also aware of the proposal and are generally supportive
- Early conversations with the Open Banking community indicate that a PDE could provide the business model and route to scale which that scheme currently lacks; but further discussion is needed.
- Two government departments are relevant, in addition to DCMS, assuming that the infrastructure is first piloted in education.
  - The Department for Education is aware of PDE-E, and its potential benefits for the sector. Also it controls the Learning Records Service - which could act as a useful data funnel, and give local pilots the necessary national dimension. But DfE realises that the project amounts to new national infrastructure, and so defers to (i) Cabinet Office/ GDS, which is meant to lead in this area; and (ii) the cross-departmental Data Advisory Board, as chaired by John Manzoni.
  - Cabinet Office / GDS has been aware of PDE-E since well before 2016, but has chosen consistently to ignore the proposal and persist with Verify, despite that scheme not being fit for purpose. The result is the waste of (guess) £150 million by now. Had a fraction of that sum been devoted to PDE-E . . .

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

See answers above.

Questions on criteria for trust

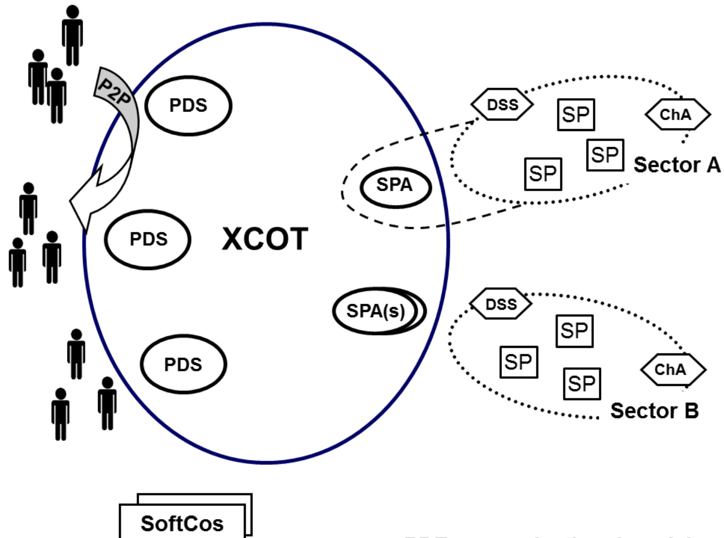
7. (i) What are the building blocks essential to creating this trust?

The 7 roles I believe to be necessary in a PDE are shown in the graphic below, which has been simplified to show just three PDS providers and two sectors of the economy. Each role is described in the following text.

a) Personal Data Services providers (PDS) compete to act as the agent of an individual. Initial PDS providers will be new starts, or big-tech companies (such as Microsoft), or evolutions of the gov.uk Verify identity providers. Subsequently, established consumer brands – especially banks & mobile network operators – may enter the market.

b) Service Providers (SPs) provide, as the name suggests, services to individuals, and may be from any sector, such as: education, healthcare, local government, national government, banking, insurance, social networking, commerce, etc. Note that service providers may also be either:

- record aggregators, such as credit bureau, or government-organised repositories of education or health records; or
- specialist attribute verifiers, whose business is to verify personal information recorded by service providers who cannot do so themselves; the first examples are likely to be evolutions of the 'identity providers' active within schemes such as gov.uk Verify or the Dutch Idensys.



PDE – organisational model

c) A Service Provider Acquirer (SPA) acts as a service provider's single point of contact to the ecosystem. The more cohesive sectors may – as shown for Sector A - choose to provide the function 'in-house'; in others – as shown for Sector B – SPAs may compete for custom.

d) Characterising Authorities (ChAs) give identity /role certificates (such as 'university', or' school') to service providers. These serve two purposes: (i) they enable relying parties (say an employer) to check that attributes released by an individual (say qualifications) were issued by an organisation entitled to do so; and (ii) they assist an individual to select the right profile of attributes for release to a SP. ChAs often already exist, but in an offline form, e.g. DfE holds the national list of recognised universities.

e) Decision Support Services (DSS) exist to help individuals choose between competing suppliers in certain sectors, e.g. UCAS for Higher Education, Confused.com for insurance, etc.

f) The eXtensible Circle of Trust (XCOT) is roughly analogous to VISA for credit cards: it will own the industry co-brand, set standards, maintain a reference code-base, and arrange for the sharing of fees and liabilities between SPAs and brokers. The XCOT is likely to be a charity or a community-interest-company. Some in OIX call XCOT 'a competent authority'.

g) Software companies will compete to serve actors in the industry: Evernym is one example, promotes the phrase 'Self-Sovereign Identity', and advocates - as anyone must - a standards-based approach. Many other companies - including Microsoft - are also involved, working under the banner of the engineering-focused Decentralised Identity Foundation (DIF, https://identity.foundation/).

As well as the organisational model above, which seems almost inevitable, there's a need for coherent funding and business models, and a route to critical mass. So far neither Evernym nor DIF has said much about these matters; but the PDE-E ideas, summarised in this document (specifically in response to questions 7 and 16), are accepted by many as coherent.

7 (b) How should the environment be created to enable this trust ?

Creating a PDE infrastructure - which must work across both public and private sectors - is difficult. Government working alone cannot manage the task, in part because it is not fully trusted as a guardian of an individual's data, but mainly because it has no business in creating systems for individual < > individual and individual < > private-sector-entity relationships. Similarly, no single private sector entity would ever be trusted to create the infrastructure, with the word Facebook being sufficient explanation.

Thus the right approach is probably to entrust the job to a non-profit public-interest entity, i.e. what is referred to as the XCOT in the text above. However, a non-profit is only likely to be able to raise the significant funding required by means of a grant from the government, making it - in effect - an extension of government. This seems undesirable, both for the reasons set out in the paragraph above and because it is too close to being a replica of the Verify funding model.

An alternative is for the XCOT to enter into a concession agreement with a special purpose development company (Devco), such that:

- Soon after - or in the run up to - signing the concession agreement, Devco would issue a public call for investment from potential PDS providers and social investment funds.
- With funding secured, Devco would - working in close collaboration with the XCOT - procure or develop the software components required by pilot participants, run the pilots, and operate the required clearing house for fees (see the response to Q16 for a discussion about business models.)
- Devco would also act as the initial Service Provider Acquirer (SPA) for the pilots.
- As the infrastructure develops Devco would lead sales and marketing to recruit new service providers, but would - when requested - cede this role to specialist SPAs set up for purpose by different parts of the public sector, i.e. health, education, local government, central government etc.
- In return for funding the development work (and indeed as a necessity for justifying the necessary investment) Devco would - under the terms of the Concession Agreement - have two privileges:

    (i) Devco would have sole rights to the SPA role for the commercial sector, until such time as its dominance of the role becomes a matter of concern to the Competition & Markets Authority. (Note that, initially, competition is between PDE and the old approach; competition between SPAs will only become important once PDE is clearly en route to ubiquity).

(ii) Devco would also have the right to charge new PDS providers for late entry into the ecosystem, given that (i) Devco, and its PDS provider shareholders, will have borne the cost and risk of setting up the ecosystem; and (ii) late entrants are likely to be large companies (banks, mobile network operators) who were too risk averse to participate in the initial pilots, but - once they enter - have brands strong enough to dominate the market, and wipe-out the initial (and probably small) PDS providers.

Note that the privileges above can be said to be fair because all potential PDS providers were offered the chance to invest in Devco at the outset.

Note also that the XCOT could, conceivably, enter into concession agreements with more than one Devco, so allowing independent pilots to be run in competition, before - eventually - selecting a winner. But (i) much of the private sector recognises that - at this stage - the necessary competition is not between different provider groups, but rather between the new approach and the status quo; and (ii) it would be odd to start building new trust infrastructure by using - as a first step, and without permission - the business and funding approach proposed by PIB-d; that said, the absence of hard IPR would make it difficult for PIB-d to pursue the matter at law.

7 (c) For example, what is the role of open standards (identity, technical, operational, business implementation, design requirements for consumer privacy and protection) ?

Evidently, a PDE can only function if all the participants adopt common standards for technology, operations, privacy protection etc. The standards will be developed by the Devco, and owned by the non-profit governance body, the XCOT. In payment systems, the role of standards owner is fulfilled by Visa and MasterCard - who were originally owned by the participating banks as non-profit entities, but are now fully commercial.

Whether the standards for a PDE need, in fact, to be fully 'open' is uncertain: the ecosystem itself will only be open to organisations who sign-up and obey the rules, and so the availability of the standards could be limited to such members. Indeed, restricting access to documents may help promote the growth of PDE across borders, since other countries would probably then need to cooperate closely with the UK as pioneer. On the other hand, openness helps creates trust, which is a necessary ingredient . . . .

8. How does assurance and certification help build trust?

To function, PDE needs a common brand that will be displayed by PDS providers and service providers, and will convey to users ideas of trust and interoperability. Thus the brand will serve a similar purpose to VISA or MasterCard in payment systems.

Further, some form of external inspection and certification will be necessary to ensure that participants - primarily PDS hosts and Service Providers - comply with standards to which they have signed up. In payment systems, the certification is called PCI/DSS; in Verify, tScheme was used. It should be noted that both certification schemes are internal industry matters. The trust mark for public consumption is the scheme's brand.

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)?

Privacy will be assured because the Devco, overseen by the XCOT, will specify the software components to respect privacy principles, as set out in GDPR. Data minimisation is one example; another would to avoid reliance on any single identifier (e.g. an ID card #), since doing so facilitates back-office data sharing between organisations, outside of an individual's control.

Privacy protecting implementation will be the responsibility of participating organisations, and checked by external assessors - as discussed above.

The question of accommodating a 'range of technologies' is more difficult. The need for interoperability and account portability means that all participants must use substantially the same technical approach, and upgrade from one to the next in a coordinated way. The introductions of Chip & Pin, and then contactless, by the payment systems provide good examples.

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

Technology is only ever an enabler, not the master. The participants - the Service Providers and the PDS hosts - will not wish to escape their duty of complying with the Human Rights Act. And they, working with the XCOT, will ensure that the software components are designed accordingly, avoiding any discrimination.

That said, the participants' first priority will be to design services that appeal to the mass market, and so turn a profit; they will then be able to afford to tailor their offerings to accommodate those with protected characteristics.

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

See response to question 7(a) above.

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

See response to question 7(a) above. The rules should be developed by the Devco and owned by a special purpose non-profit entity set up for the purpose and independent of government. PIB-d has always called this entity the 'eXtensible Circle of Trust', or XCOT; while discussion within techUK and OIX currently refers to a 'Competent Authority'. But these names are only provisional: given that branding will be important, the entity should be expected to develop its own public image, working closely with the Devco.

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

If the argument for the ecosystem to be governed by a public-interest non-profit is accepted, then this question becomes - in effect - ''Who should run the non-profit?".

But first, it should be understood that - while nominally independent of each other - the fates of the non-profit and the Devco are linked: if the scheme fails, it is unlikely that either entity will be invited to 'have another go'.

To maximise the chances of success, the board of the XCOT should comprise individuals who (i) primarily represent current and future participants in the ecosystem, particularly large service providers (e.g. the NHS, education, DWP, private sector) and the general public; but also (ii) have a fair understanding of the business and technical complexities that must be tackled by the Devco. The ICO might also be persuaded to provide support. Ideally the XCOT should be lightweight, at least initially, having perhaps just a single paid chair, two or three competent staff, and relying on secondees for board membership

The Devco, for its part, need to be highly competent at specifying and delivering complex multi-party systems. It should be technically neutral, choosing the best technologies for its purpose, and only creating new software where necessary. Given its hybrid public interest/ commercial mission, it should have no difficulty in recruiting competent and motivated staff.

Questions on the role of the government

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?**

In time, digital government documents are necessary and inevitable. But the UK should be in no hurry. The first requirement is to develop and prove infrastructure - what is called here a Personal Data Ecosystem (PDE) - to enable individuals to receive, store, and then show trusted personal data to others.

Further, it makes sense to start with relatively low risk documents, such as qualifications, which lie in the middle ground between public and private. Only when the infrastructure is proven does it make sense to add higher-risk documents, such as passport and driving licence.

Note that:

- the infrastructure should be able to handle 'dynamic data', given that certain attributes can change over time. An example would be a DBS 'white list' attribute.
- in time, we may well get to the point where the online 'identity' is regarded as the most secure, such that a physical passport or driving licence are regarded simply as ephemeral versions, to be used only in contexts which cannot yet accept online transactions; in fact, the potential to reach this state is a good test of the correctness of next stage system design.

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?**

Validity checking of documents - via DCS - plays a significant part in gov.uk Verify. The process could be opened up so that any service provider - say airlines or banks - could check document validity directly. In a sense, this would be the democratic and fair thing to do.

But there is a drawback. If any service provider can request checks of documents, the incentive for such service providers to integrate with identity-related infrastructure (whether gov.uk Verify or a PDE) is reduced; and the promised benefits for individuals - in terms of greater convenience and data control - would be jeopardised. In my view, then, access to validity checking services, such as DCS, should be limited to intermediaries who propose a 'check once, use many times' approach AND are subject to suitable external governance.

Re cost model, and if the restrictions above are accepted, then the volume of validity check requests received by government should be - in relative terms - quite low. The associated costs should be subsumed within the application fees paid by individuals for the original documents; indeed, it would seem bizarre for government to charge for the issue of supposedly secure documents - such as a passport or driving licence - and then charge extra to say whether any given document is actually valid.

16. **(i) For what purposes should government seek to further open up the attributes (such as age of citizens) that it holds for verification?**

See responses above. Generally, and with some limited exceptions (of which more below), citizens will wish to control positive data about themselves, such as qualifications, but not negative data, such as criminal records. Looking at particular cases:

- Proof of age is required for age-restricted purchases (alcohol, ‘adult’ entertainment, etc.) Generally, the need is not to present date-of-birth (which would breach the data minimisation principle), but rather have a trusted entity (such as a PDS provider) state that the individual’s age is over (or sometimes under) a certain threshold.
- Qualification records. Currently the Department for Education runs the Learning Records Service, a burgeoning database of qualifications (largely from secondary and FE awarding bodies) which serves no significant purpose, to which citizens have no online access, and which is not compliant with the spirit (if not the letter) of GDPR. Learners could usefully be given access, working through a PDS, so that they combine data from LRS with achievement records from other sources (universities, MOOCS, professional bodies) and use the result when making transitions, either between learning providers or from education into employment.
- Disclosure & Barring Service (DBS) data. For some time now, the DBS has been in the process of morphing from a blacklisting service (this person is not suitable) to a whitelist service (this person is suitable). A white list entry is - in effect - a qualification, and could usefully be included within a trusted CV that an individual might show when applying for a job.
- Driving licence. DVLA already offers (I think) a service allowing drivers to share driving licence details online. In time this could be integrated within a PDS infrastructure.
- Prescriptions, health records, dental records. The scope for user control of data in health is broad, starting perhaps with prescriptions - where the currents system allows a GP to direct a ‘scrip to a pharmacy of the individual’s choice, but does not allow the individual to change their mind, choosing a different pharmacy once they have left the GP’s surgery. Later on, there is potential for control - by patients who so wish - of their own health records, giving a new GP access, rather than having to wait for the cumbersome process of record transfer between GPs’ back offices. There is similar potential in dentistry.
- Vouchers. While the political appetite for such schemes remains uncertain, there is scope for user-control-of-data infrastructure to be used to give individuals secure online vouchers which they can later exchange for services. Possible applications include early years’ childcare, ‘positive’ activities for teenagers (such as NCS), etc.
- Money. There is no technical reason why an individual should not use their PDS for making low value payments, taking advantage of the functionality now offered by the Open-Banking; indeed, converging ‘identity’ and payment infrastructure will save cost, and contribute significantly to the overall business case for a PDE.

16 (ii) How should this be governed to ensure protection and citizen control of data?

See response to question 6, 7 etc above.

16 (iii) What should the cost model be?

Anyone familiar with the payments industry, or gov.uk Verify, will recognise the four cornered organisational structure shown in the figure above. The proposed business / cost model is a hybrid of the approaches used by the two schemes. Service providers will pay a per-capita periodic relationship fee to the infrastructure (via their SPA) in return for three services:

- a secure online relationship with an individual and the (automatic) update of whatever attributes (including identity) the individual has agreed to release to the SP.

- payments, up to a certain value - since service providers will, ultimately, object to funding two separate infrastructures, one for user control of trusted data, and the second for user-control of money; and
- if the service provider does not already have a relationship with the individual, the chance to enter into such a relationship: this is permissioned or reverse marketing; part of the fee paid by the SP will be retained by the DSS (see answer to question 7i above), and part will be passed to the PDE infrastructure.

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

Legislation could usefully:

- require service providers, across public and private sectors, to recognise that individuals have rights to the use of their own data, and work towards releasing such data to them via infrastructure that allows such data to be shown - by the individual - to others without alteration, so engendering trust.
- allow service providers to levy additional charges for such release of data **only** when the preparation of the data in question is the substance of the SP's service, rather than being incidental to it, e.g.
  - a dentist would not be able to charge for dental records, since the main service is dentistry not records; and
  - a bank would not be able to charge for return of identity data to the individual, since the main business is provision of banking services, rather than proof of identity; but
  - a specialist identity provider would be able to charge for identity data, since providing such data is its main business.

Such legislation, if implemented as the new infrastructure is proven, would rapidly make it uneconomic for banks (and other SPs) to carry out identity checks themselves, obliging them instead to make use of external identity sources, probably via a PDE - which would call on specialist identity providers when necessary. The individual would benefit from greater convenience, privacy etc.

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

Two pieces of legislation come to mind: Midata and RIPA.

(i) Midata

Back in 2012-ish, the department for Business, Innovation and Skills (BIS, as was) ran the Midata programme, designed to ensure that commercial service providers returned personal data to individuals in useable electronic form. Legislation was put in place to allow ministers to compel compliance, but has never been used, since the target sectors - energy, banking, and mobile - complied voluntarily.

Midata was a fair first step. But there is a need to go further (although some of the necessary ground may have been covered by the legislation implementing GDPR). Specifically, there is a need to

- extend the principle to the public sector (initially education, health)
- provide - where appropriate - for the release to be made via a tamper proof method, so that the individual can decide who sees, but cannot change, their data; and

- provide - where appropriate - for metadata to be released, so that recipients can judge whether the data is trustworthy.

To explain this last point, data about an individual's identity is only useful if the relying party knows how the identity was established, i.e. whether and when any party inspected passport and / or driving licence, whether they checked the validity of such documents, whether they established activity history, and whether they checked that the identity actually belonged to the individual in question. All this information can be conveyed as metadata.

(ii) RIPA

A PDE offers the prospect of secure online communication for all. Taken to the limit, such secure comms would contravene the RIPA requirement to allow interception by the security services. One possible answer is to design in one or more back doors for interception, such that:

- the regulatory hurdles to be overcome before a government agency is allowed to intercept are set low if an individual uses a PDS for interactions purely with other individuals, and with private sector organisations; and
- the regulatory hurdles are set much higher - perhaps requiring a judge-authorised 'search warrant' in each case - if the individual also uses their PDS to interact with government (and so has declared to government where they 'live' in the network space.)

In technical circles, this issue is highly controversial: many believe that privacy should be inviolable. However, a majority of citizens would probably accept the above compromise if implemented competently and transparently.

In an early incarnation of PDE-E, we referred to a PDS as an individual's 'Virtual Home', i.e. a point of presence in the (virtual) world from which to interact with many different counterparties. Just as existing law requires government to obtain a search warrant to enter someone's real home, so government should face a similar requirement before entering someone's Virtual Home, provided that the VH - like a real home - shows evidence of investment by the individual (i.e. user over a period of time, relationship with the state, etc.)

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

Infrastructure for user control of trusted personal data (including identity) could well become a major new industry, both providing many internal benefits, and providing the basis for an export market.

Further, it is a sector in which the UK is well placed to lead, because of our early faltering steps with Verify; and our culture, which allows for the necessary mix of state and private / third sector provision. The contrasts for this latter point are with (i) the USA, where the state plays too small a part, and the culture is overly laissez-faire; and with (ii) Germany, where 'identity-card' culture is too well embedded, and the scars of the past make them very conservative in all matters personal data.

Thus - PLEASE, PLEASE, PLEASE - treat the new infrastructure as a strategic matter, think hard about the vital issues (i.e. route to critical mass, organisational model, business model, and financing model), and take the time to build consensus across the many stakeholders, especially those in Whitehall. I would be happy to help.

20. **How could digital identity support the provision of local government services (including library cards and concessionary travel)? authorities provide many services, the more interesting questions are:**

- to what extent the services are provided by the authority as a single data controller, and so are aware of each other; versus the privacy maximising position of each service being isolated, i.e. subject to a separate data control regime, and unable to exchange data - via the back office - with other services provided by the same authority; and
- whether a particular service requires full disclosure of legal identity, or - for privacy purposes - can accept pseudonyms or anonyms. Reporting a pot hole is at one extreme; requiring assessment for social care possibly at the other; and taking out a library book somewhere in the middle. Each service needs to be looked at individually.

Question on the role of the private sector

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)?**

See answer to 7b above.
