Building a

‘personal data ecosystem’

which complements **Verify** by

- helping those who are not yet well established in society - such as the young - create a trustworthy online identity;
- protecting privacy; and
- providing a broad foundation for growth of trusted personal data services across BOTH the public and private sectors.

An alternative view, emerging from:

- the Digital Catapult’s Personal Data & Trust Programme; and
- OIX-UK’s Industry Working Group on Attribute eXchange

and supported by:

Professor Chris Hankin, Imperial College

Professor Bruce Christianson, University of Hertfordshire

Professor Jon Crowcroft, University of Cambridge

\+ +

Contents

Document control

Issue	Date	Comment
0.996	3 Dec 15	Amended list of supporters; and formatting corrections.
1.0	09 May 16	Belated formal issue

This page has been left blank intentionally.

Summary

- The Cabinet Office Verify scheme for identity assurance is a major step forward, but currently makes no provision for 'Attribute eXchange (AX)', i.e. a process by which relying parties can - with the consent of the individual - obtain further trustworthy personal data (in addition to identity) from other organisations.
- Attribute exchange is seen as being key to the release of value from 'identity-related' ecosystems.
- Two approaches to AX have been suggested, one that takes Verify as a given, and a second based on the development of an ecosystem of 'Personal Data Services (PDS)'.
- The Verify approach to AX only works for a small number of use-cases in which the required data is stored in national databases.
- The PDS approach has the potential to: (i) work for all AX use-cases, across both public and private sectors, thus creating considerable value; (ii) enhance privacy; and (iii) help fix Verify's inability to provide secure trusted identities for individuals who are not yet well established in society, particularly the young.

In consequence, the supporters of this paper urge the Government to recognise that:

i) UK citizens need a PDS ecosystem to control the flow of their data between organisations, so enhancing convenience and privacy, and providing for necessary new functionality - such as a portable personal education record, delegation, proof of student status, proof of age, reverse marketing, and many more.

ii) a personal data ecosystem would be a useful complement to Verify, helping those who are not well established in society obtain a secure (LOA2) Verify identity;

iii) development of a PDS ecosystem is best led by one or more private- or third- sector organisations under the supervision of a non-profit governance body.

iv) a PDS ecosystem is only viable if there is a development path which, although starting at the level of individual service providers (schools, local authorities, universities, GPs), has the potential to reach national scale;

v) it would thus be useful to open - at an early stage - discussions with certain government departments, particularly BIS and DfE re education applications and DCMS re proof-of-age applications; and

vi) it would helpful if - because of its dominant role in identity assurance - Cabinet Office could (i) recognise publicly that a personal data ecosystem would be a useful complement to Verify; and (ii) sponsor the discussions with other government departments, as outlined above.

About the supporters of this paper

- PIB-d Ltd is a joint-venture between parts of HE sector and the private sector, and intends to create a personal data ecosystem for the UK, starting in the education sector. http://www.pib-d.net
- Ctrl-Shift is a specialist consultancy 'helping organisations to prosper, in the new digital economy, by using information in the hands of the individual to build a trusted strategic market position through trusted digital services'. http://www.ctrl-shift.co.uk
- Mydex, a Community Interest Company, is the UK's longest-established personal data service. https://mydex.org
- PAOGA is a privately held supplier of personal data services, and is currently working with a client in the HE sector to stand-up a pilot. http://www.paoga.com/
- Chris Hankin is Director of the Institute for Security Science and Technology at Imperial College London, and a Professor of Computing Science; he was also the chair of the expert group responsible for the 2013 Government Foresight report on the 'Future of identity'. http:// www.gov.uk/government/collections/future-of-identity
- Bruce Christianson is professor of informatics at the University of Hertfordshire and takes a particular interest in identity, personal data, and the transitivity of trust. http://go.herts.ac.uk/bruce_christianson
- Jon Crowcroft is the Marconi Professor of Communications Systems in the Computer Lab, at the University of Cambridge, and a co-investigator in the Hub-of-All-Things project. See http:// http://www.cl.cam.ac.uk/~jac22/ and http://hubofallthings.com/

About the OIX-UK Attribute Exchange Working Group

The Open Identity Exchange (OIX) is a non-profit that describes itself as a 'global organisation working directly with governments and the private sector developing solutions and trust for online identity'.

The UK arm of OIX, known as OIX-UK, works closely with - and is largely funded by - the Cabinet Office to assist with the development of its Identity Assurance Programme, also known as the GOV.UK Verify service.

In 2014/2015, OIX-UK formed an industry working group to study the question of how Attribute eXchange (AX) functionality could be developed for the UK, and to comment on work led by Warwickshire County Council to develop an AX application using Verify as a foundation. That group has now produced an official OIX report, which can be found at http://oixuk.org/?page_id=444

John Harrison of PIB-d participated in this working group, and championed the (minority) view that identity was an attribute, and that an approach to attribute exchange based on this fact would both create useful general purpose infrastructure and help remedy some of weaknesses in Verify. Thus this paper can be seen as an alternative, or perhaps a complement, to the official OIX report.

About the Digital Catapult's Personal Data and Trust Programme

The Digital Catapult is a 'national centre to rapidly accelerate the UK's best digital ideas to market to create new products, services, jobs and value'. One of the Catapult's programmes seeks to facilitate work on the issues of online Personal Data and Trust, and is led by Dr Matt Stroud.

It should be emphasised that the Catapult is not a funding agency, and so does not attempt to 'pick winners'. Rather it is a facilitator, and seeks to assist the development of personal data and trust schemes that have originated - and may have gained some momentum - elsewhere. As part of this role, the Catapult may: (i) organise fora at which discussions can take place, particularly between organisations with AX uses cases and developers of PDT schemes; and (ii) assist with the development of the non-profit governance body required in most scheme architectures

All the supporters of this paper, save Bruce Christianson and Jon Crowcroft, have participated in one or more Catapult PDT events.

1. Introduction

In early 2015, Cabinet Office, which created the Verify scheme for identity assurance, funded an OIX-UK industry working group to look at the subject of 'attribute exchange (AX)'.

Two approaches to AX were suggested. The first takes Verify as a given. The second requires the development of an ecosystem of 'personal data services (PDSs)' - also known as 'personal data stores', 'personal information brokers', 'personal information management services' and 'life management platforms' - and can be made backward compatible with Verify. PDSs are also the subject of discussion within the Personal Data and Trust initiative hosted by the Digital Catapult.

In this paper, which is the result of discussions in the OIX working group and at the Catapult, we describe the two approaches to AX, and then argue that the development of a PDS-based ecosystem is a necessary step for the UK, offering a wide set of applications, and also remedying certain key weaknesses of Verify.

We then list briefly some of the leading AX use cases, discuss the governance and financing issues inherent in creating a PDS ecosystem, and conclude by urging Cabinet Office to support further work as a sponsor of discussions with other government departments.

In the annex, we describe in detail some of the leading AX use cases, looking specifically at Blue Badge, proof-of-age, portable-personal-education-record, proof-of-student-status, user preferences (including address), delegation / transfer of authority, foundational identity, and medical applications.

2. Why a PDS ecosystem complements Verify

In the Verify project, the Cabinet Office has shown how individuals can choose an agent, from a managed market, to prove their Key Identity Attributes (KIA)[1] online. The next step, seen as being key to releasing value[2] from 'identity ecosystems', is Attribute Exchange (AX): a process by which an organisation can obtain, online and with an individual's explicit consent, trustworthy information about that individual from other organisations.

Two approaches to AX have been proposed. The first takes Verify - in which the agent chosen by an individual is known as an 'Identity Provider (IdP)' - as a given. In the second, individuals choose a different kind of agent, known as a 'personal data service' (PDS)', from a different managed market.

The differences between an IdP and a PDS are important. An IdP checks the existence of an individual's claimed identity (in, principally, the passport, driving-licence and credit-reference databases), verifies that the individual is the real owner of that identity, and then enables the individual to show the result - a set of verified Key Identity Attributes - to organisations with whom the individual wishes to transact. The flow of information is one-way: from IdP to transacting organisations.

In contrast, a PDS can be thought of as online wallet for use by an individual to carry many kinds of trusted personal information from one organisation to another. Such information might include KIA, or qualifications, or proof of student status, or tickets, or prescriptions, etc. The flow of information is two-way: from PDS to transacting organisation, back in the reverse direction, and then outward again to other transacting organisations.

A PDS can be thought of as a generalisation of an IdP, designed specifically for attribute exchange and treating proof of KIA in much the same way as proof of any other attributes, rather than as a case apart.

The benefits of creating a PDS ecosystem for attribute exchange, rather than persisting with an approach based solely on Verify, are significant, and can be described under three headings: 'any attribute from anywhere'; 'privacy'; and 'building trust'.

[1] Key Identity Attributes (KIA): name, addresses for the last three years, date-of-birth.

[2] See, for example, the Ctrl Shift report on 'Economics of Identity' available from www.ctrl-shift.co.uk; and the various WEF reports re personal data, available from www.weforum.org/projects/rethinking-personal-data

2.1 Any attribute from anywhere.

Because the Verify information flow is one-way, and limited to KIA, organisations requiring further trusted attributes - beyond KIA - cannot request it from the individual's IdP. Instead they must search elsewhere, and are only likely to succeed if the information is stored in a known place. Thus these use-cases, termed 'static AX' by the OIX working group, tend to involve unique, national-scale data sources, usually found in or near central government. The lead example, being piloted by Warwickshire County Council, is proving eligibility for 'Blue Badge' parking privileges - which can be determined from the DWP's database in about 40% of cases[3].

Looking now at the PDS approach, the data flow is two-way, both from and to an individual's PDS. Thus organisations requiring trusted information about an individual - whether 'identity' or many other types - don't have to know where to look; instead they can ask whether the information is available through the individual's PDS, as a result of PDS-enabled online relationships that an individual may have set up with any entity, ranging from national databases all the way down to a single school, hospital, doctor, professional body, bank or even another individual.

Extending the range of attribute sources, in this way - from just central databases to the whole of society - results in a far richer of set of AX applications, and weakens any case for the creation of further central databases.

2.2 Privacy

Within a PDS ecosystem, data is - in effect - carried by an individual, using a PDS, from one organisation to another. In consequence, it's the individual who makes the necessary links between personal records, and there is no absolute need to disclose an identifier (or set of attributes, KIA) that - because it's unique across many different organisations - can be used by them to link records without, necessarily, obtaining the individual's consent.

This means that, unlike Verify which requires disclosure of KIA to every organisation, a PDS ecosystem is a privacy-enhancing technology: it will enable an individual to disclose *only* the personal information required for a particular transaction.

In some cases, say opening a new bank account or linkage of a new online account to existing offline records, disclosure of KIA may be required. But in many other cases, KIA is not required, allowing the individual to act anonymously or pseudonymously. Examples include: (i) voting, disclosing only eligibility to vote, such as residence within a defined region; (ii) access to safe social networks for children, disclosing only that the individual's age is below an agreed threshold; (iii) purchase of adult material online, disclosing only that the individual is 18 or older; and (iv) sale of goods through an distributed ebay-like system, disclosing only seller reputation.

2.3 Building online trust / enabling the young to establish secure online identities

A Verify IdP proves KIA by checking to see whether a claimed identity can be found in existing databases - principally the Passport, Driving Licence, and credit reference systems - and then requiring the individual to demonstrate that he or she is indeed the owner of that identity. This works well for individuals who are established in society, and have entries in at least two of the three main databases. But it works poorly for those - often the young, the homeless, or immigrants - who have yet to become established. These individuals find it difficult, if not impossible, to obtain a Verify LOA2 identity, the first useful level. Currently, at least 50% of applications to Verify's IdPs fail [4].

Verify's difficulties are illustrated by the circularity of requiring an individual to have an LOA2 identity to apply online for a driving licence, which itself is one of the identity proofs commonly used to obtain an

[3] Figure provided by Rob Laurence, project manager of the OIX run Warwickshire Blue Badge discovery and alpha project

[4] The figure of > 50% failed applications is derived from conversations with several of the Verify IdPs.

LOA2 identity. These difficulties are compounded by the fact that, should an individual wish to switch from one IdP to another, they lose whatever trust has been built up and must start again from scratch.

There is need for a different approach, one that complements Verify by enabling individuals to build up trust online over a period of time, akin to the way in which sellers on ebay start by being pseudonymous, and can then build up a reputation as being honest and prompt. Using a PDS account, an individual will be able to accumulate vouches for identity - as well as for other attributes - from the many organisations and individuals they encounter as life progresses. And, as a condition of the trust framework imposed by the PDS ecosystem, they will be able to port that accumulated evidence from one PDS to another.

Note that not all vouches for identity are equal. More weight will be given to those that are recent; that originate from established organisations or individuals; that are the result of either face-to-face or long-term interactions; and that result from a formal check of identity proofs.

In this approach, any organisation that vouches for identity can be regarded as an 'Identity Provider', and the individual's PDS becomes the medium used to convey accumulated evidence of identity to new organisations. One could say that the PDS approach is an unbundling of the Verify model, separating the provision of identity (and other attributes) from the means by which the attributes are conveyed.

In the longer term, and because a PDS gives an individual control over disclosure, we may even reach the point where government can issue an online, foundational identity attribute - the equivalent of a birth certificate - to an individual as represented by their PDS. But that step will require (i) advances in the use of biometrics for authentication (i.e. proving ownership of a PDS account); and (ii) the development of technical and legal means to allow a parent or guardian to control, from their own PDS account, a child's account.

3. Applications for a PDS ecosystem

Some PDS applications have already been mentioned. But, to ensure completeness, we give in this section a quick overview of leading applications, starting with Blue Badge as the case that was examined by the OIX Working Group.

- Blue Badge: online applications by the less able for parking privileges
- Portable personal education record: enabling individuals to gather qualifications from many different learning providers and professional bodies, both on-line and traditional, and then use this evidence in support of applications to further learning providers and / or employers
- Trusted online identity/ reputation for young people: helping address the difficulty found by Verify in providing secure online identities for those who lack passport, driving licence, or credit record
- Foundational identity: enabling government, in the longer term, to issue the online attributes in lieu of birth certificates
- Proof of age, and proof of student status: enabling young (and older) people to gain access to age-appropriate online content / social networking, and prove eligibility for student discounts
- User preferences: enabling everyone to maintain a single source of truth for data under their own control, e.g. address, marketing preferences, contact details, etc.
- Medical applications: giving individuals online access to their medical records, user control of medical prescriptions etc.
- Internet-of-Things (IoT) applications: giving individuals control of data generated by personal internet-enabled devices, e.g. health monitors, location data from mobiles, etc.

All these applications are described in more detail in the annex.

4. Development model, governance and funding

It's not easy to set up a new, distributed, digital ecosystem for personal data and identity. The closest parallel is to the credit card networks 50+ years ago, but they only deal with a single type of use case and set of attributes: money and its movement.

The issues to be overcome include: (i) that most existing organisations have sector-specific remits, and thus do not feel able to lead a project that straddles sectoral boundaries; and (ii) that there is a need to raise significant funding, despite a degree of technical risk and the current climate of austerity.

Looking at attempts to date: **Verify** was developed - and is managed - by the Cabinet Office, with funds provided entirely from the public purse. While the scheme's lead application is proof of Key Identity Attributes to central government departments, there is an ambition to also serve other parts of the public sector and, indeed, the private sector. But it is open to question whether the ambition is entirely realistic, given that Verify was not really designed to meet the needs of service providers - such as the NHS, local government, and education - that often see their customers face-to-face, and so can easily check identity themselves.

Apart from Cabinet Office, the field is split between start-ups and research projects. Of the start-ups, **Mydex CIC** is one of the longest established. Its founders took the view that a personal data service was a public good, and so created a community-interest-company (CIC), using funding from sources seeking social benefit as well as some level of financial return. Mydex CIC has significant experience of providing services to local authorities.

A second start-up, **PAOGA,** was set up as conventional commercial company, and is currently working with a university to run a pilot of a stand-alone personal data service.

PIB-d was set up in 2011 as a joint venture between the Higher Education (HE) and private sectors. The founders contributed certain intellectual property, some private capital, and won some grant funding; the HE sector contributed further funding, and a route to critical mass in which a portable personal education record serves as the lead application. The company completed a formal feasibility study by the end of 2012, and then paused because of (i) uncertainty about Verify's future development plans; and (ii) a reorganisation, and consequent lack of clear direction, within one of its HE sector investors. Now both obstacles are clearing, and there is a possibility of progress.

By way of organisational model, PIB-d has long advocated a non-profit governance body to create trust, and a for-profit operational company tasked with developing new applications and signing up new service providers. This approach is similar to that adopted by the more recent **Hub-of-All-Things (HAT)** research project, led by Professor Irene Ng at the University of Warwick, and now transitioning into start-up mode.

But, in other respects, the two projects are very different: whereas PIB-d focuses initially on 'real world' personal data, as defined by counterparties - both organisations and other individuals - with a legal persona , HAT concentrates on giving individuals control of data generated by internet-enabled devices. Thus the lead PIB applications are proof of qualification, proof of student status, proof of identity, and communications between all the entities involved; while the lead HAT applications are marketing related. However, the two projects appear to have some common applications - such as low- value payment - and may eventually converge.

A second research project, **Digital Prosumer** led by Professor Panos Louvieris at Brunel University, is – as yet – in the early stages. Like HAT, it appears to be focused on data generated by internet-enabled devices.

The final mention goes to the **Digital Catapult,** which is a 'national centre to rapidly advance the UK's best digital ideas'. The Catapult's Personal Data and Trust team is working hard to promote the development of personal data services in the UK, and is well placed - and willing - to support the creation of the non-profit governance body required in proposals for PDS ecosystems, such as PIB and HAT.

5. Conclusion and recommendations

The development of a personal data ecosystem for the UK, based on interoperable personal data services, offers benefits to all: new applications, greater convenience and improved privacy for individuals; and significant process improvements and economies for the organisations that serve them.

Such an ecosystem could also help address the challenges currently found by the Cabinet Office Verify scheme in providing secure online identities for those people - particularly the young and the homeless - who are not well established in society. However, Cabinet Office - which leads for the UK public sector on 'identity' - has yet to recognise, formally, the UK's need for a personal data ecosystem.

All the supporters of this paper urge the Government to recognise that:

i) UK citizens need a personal data ecosystem to control the flow of their data between organisations, so enhancing convenience and privacy, and providing for necessary new functionality such as delegation.

ii) a personal data ecosystem would be a useful complement to Verify, helping those who are not well established in society obtain a secure (LOA2) Verify identity; and

iii) development of a PDS ecosystem is best led by one or more private- or third- sector organisations under the supervision of a non-profit governance body.

iv) a PDS ecosystem is only viable if there is a development path which, although starting at the level of individual service providers (schools, local authorities, universities, GPs), has the potential to reach national scale;

v) in consequence, it would be useful to open - at an early stage - discussions with certain government departments, particularly BIS and DfE re the education applications, and DCMS re proof-of-age applications; and

vi) it would helpful if - because of its dominant role in the provision of identity assurance services to the public sector - Cabinet Office could (i) recognise publicly that a personal data ecosystem would be a useful complement to Verify; and (ii) sponsor discussions with other government departments, as outlined above.

Annex - Uses cases for Attribute eXchange

In the sections below, we describe a number of Attribute Exchange use-cases, showing that most require a PDS-based approach, and cannot easily be developed if Verify is mandated as the foundation.

A1. Blue Badge

Warwickshire County Council (WCC) is leading work to explore how AX can be added to the Cabinet Office Verify scheme for identity assurance. They are examining the process by which less-able residents apply for a 'Blue Badge', permitting parking privileges. To determine eligibility, it's necessary to seek information - attributes - from other organisations.

It turns out that the Department of Work & Pensions (DWP) can give a 'yes/no' answer for about 40% of applicants. This fact has led to the creation of a simple design for AX in which, once the individual has given consent, WCC sends a request (including 'identity' as supplied by the individual's Verify IdP) to DWP, via a specialised 'AX' hub; the response is sent back along the same path.

But this approach cannot be generalised - either to the 60% of Blue Badge applicants for whom DWP has no relevant information or to the many other AX uses cases. Why? Because it only works if the Relying Party - in this case WCC - knows which organisation to ask for the necessary information. In the Blue Badge case, there are many other organisations - apart from DWP - who might be in a position to provide evidence of eligibility. Examples include medical consultants, the Ministry of Defence (in its capacity as administrator of the Armed Forces Compensation Scheme), and other local authorities (who maintain registers of those with sight loss).

A simplistic fix would be to persuade all relevant organisations to contribute their records to a national database. But this is a first step on a slippery path to a single database for all kinds of personal data, or at least a single database for each sector. For reasons of privacy, and because such outcome does nothing to address the question of how individuals should be identified to, and control access to, such databases, development in this direction appears unsound. Instead, an ecosystem of personal data services - which would deal natively with the identification and access control issues - appears to be a better long-term approach.

A2. Portable personal education record

Qualifications are clearly verifiable attributes, and - because there are so many learning providers and awarding bodies - it is only the individual who knows where such attributes are stored. Thus a portable personal education record (PPER) is a leading application for a PDS ecosystem.

That said, there have - over the years - been a number of attempts to create student-centric electronic education records. The most recent was the Learning Records Service (LRS), created in 2006, which aggregates records from the awarding bodies that serve secondary and further education, using a Unique Learner Number for matching purposes. The universities have been invited to contribute their records as well, but few have done so because - it would seem - all act as their own awarding bodies and see no need for a state service as an intermediary.

LRS is now almost a white-elephant. It is not used by individuals for transition between learning providers or into employment; in fact the only user is the National Careers Service, and the number of queries to the NCS is said to be very low, of the order of 100 a month.

Prior to LRS, effort was focused on what were called 'e-portfolios', defined as a point of presence in the network space which individuals could use to evidence attainment. But all such systems were provided by an individual's learning provider, meaning that the individual lost access to them on transition to a new learning provider or into employment.

As PDS based approach to a PPER promises to overcome the flaws of both LRS and e-portfolio. The scheme would be piloted within a single learning provider of each type (university, FE college, secondary school), and - if successful - could then be rolled out. Other PDS applications, such as voice and text communication, low-value payment, and alumni relations, would increase the attractiveness of the approach to learning

providers. If successful, the scheme would ultimately be used for transition between learning providers, and application for a first job.

A3. Trusted online identity for young people

As described in the main body of the paper, a young person will be able to collect - using a PDS - vouches for identity from the learning providers and other organisations they encounter as they journey through the education system and into employment. When aggregated, such vouches will be significant contribution to the identity proofing required to obtain a Verify-style LOA2 identity, and thus help address Verify's current difficulties in serving those who lack one or more of passport, driving licence, or credit file - typically the young.

A4. Foundational identity

Back in the early 2000s, the then Government tried to introduce a national identity card. But the proposal faced significant opposition, and was eventually scrapped on grounds of cost and harm to privacy. As a consequence the UK still has no modern system for providing a secure foundational identity, relying instead on paper birth certificates and various special schemes for immigrants and refugees. Thus, when a young person born in the UK opens their first bank account, they cannot do so online, but rather must present themselves at a bank, equipped - if they do not have a passport or driving licence - with their paper birth certificate.

Verify does not purport to be a secure foundational identity scheme: it merely provides a way by which an individual can make online use of an identity that is already well established - in the passport, driving licence, and credit reference databases - offline.

Going right back to the beginning, an individual's foundational identity relationships are those with their parents, who confer an identity on a new-born, register this identity with an official registrar, and receive a birth certificate in return. Thus the long-term answer to enabling young people to prove their identity on line is to give them, using a PDS or similar, the ability to show an electronic birth certificate to counterparties. Babies would acquire a PDS at birth, with the first three relationships being with the parents and the official registrar. The parents would control (see section re delegation) the child's PDS account until an agreed transition point, probably in their early teens.

While electronic birth certificates remain some way ahead, the necessary infrastructure can be developed now in support of nearer term applications. And given that a PDS ecosystem enhances privacy, the scheme is likely to be welcomed.

A5. Proof of age for young people

Online proof of age for young people is topical at the moment, with the impetus provided by a commitment in the Conservative manifesto to 'stop children's exposure to harmful sexualised content online, by requiring age verification for access to all sites containing pornographic material'. There are also use cases for proving that a child's age is under a certain threshold, principally access to 'safe' chat rooms and social networking sites. The Digital Policy Alliance is running a working group[5] on the topic.

In the absence of any single national identity database to which children and young people have online access, the obvious source of age-related attributes for young people are schools, college and universities. Using a PDS account, a young person will be able to prove age online by calling on the records held by his learning provider.

There's also the point that, in certain proof of age cases, it's desirable to allow individuals anonymity, e.g. it should be unnecessary to require full disclosure of KIA for either (i) access by children to safe social networking sites; or (ii) access by adults to 'adult' content. A PDS-style of user controlled attribute transfer allows such protection of privacy, whereas Verify does not.

[5] See http://dpalliance.org.uk

A6. Proof of student status

Proof of student status is needed when applying for discounts. Those offered by local authorities on council tax, by transport operators on some forms of travel, and by technology companies on software are among the more significant.

It is schools, colleges and universities that determine student status. And only students themselves know which learning provider they attend. Yes, there are various centralised databases - such as the Learning Records Service and that held by the National Union of Students - but all are derivative, incomplete, and take time to be updated when status changes. Thus, on the face of it, a good solution to proof-of-student-status requires a PDS based approach.

A7. Delegation / power of attorney

At work, there are many uses cases where one individual delegates authority to act on their behalf to another. Examples include giving an individual authority to make payments, or sign contracts, possibly with a value cap. In private life, authority to act on behalf of someone who is incapable if often transferred to another, with examples being a parent acting on behalf of a child, or a lawyer acting - with power of attorney - on behalf of a client.

While many large corporations have sophisticated systems for managing delegation, there is little provision as yet for online transfer of authority between private individuals. Various architectures can be imagined: there's an organisation-centric model, in which each service provider relies solely upon its own records, but can never be sure that such records are up-to-date; and there's a user-centric approach, in which an individual (or possibly the courts acting on an individual's behalf) would record transfers of authority for different areas of life within the individual's PDS account; such details could then transmitted to new service providers, or checked by existing service providers, when necessary.

A8. User preferences, including address

In time, individuals may wish to use a network agent to inform multiple different counterparties about their preferences, such as where they choose to live, what language they find most convenient, what their interests are, and what level of general and / or interest-specific marketing material they are prepared to accept. Such applications may generate significant revenue.

The Verify design makes the usage of an IdP for these applications problematic, because a Relying Party does not know which IdP an individual has chosen to use, and therefore which IdP to regard as the source of truth for individual preferences. Put otherwise, there is no provision within Verify for an RP to request up-to-date information about an individual on the basis of previously expressed consents.

A9. Medical applications.

Family doctors, like learning providers, see their customers face-to-face, and see little need for Verify IdPs to connect patients to their local records. The argument then goes:

- 'Ah, but national health records are different, and it is there that Verify-style IdPs will be needed'.
- 'But national records are simply an aggregation of local records: why not allow individuals to aggregate their own local records, using a PDS ecosystem ? '
- 'Ah, but there are all sorts of reasons why individuals should not have charge of their own health records: the NHS needs them for research, and what about children, the infirm and the mentally ill ?

Suffice to say, it's a complex issue and not likely to be resolved soon. But there is a clear case for dynamic attribute exchange in health: the electronic transmission of prescriptions (scrips) from a GP surgery to a pharmacist. Scrips can already be sent electronically, by a GP surgery to a pharmacist specified in advance by the individual. The next step is to regard a scrip as an attribute, and enable an individual to transmit scrips, via their PDS account, to a pharmacy chosen at some later point, possibly online. A good solution would also enable individuals to request new scrips electronically, rather than having to use the paper-based approach still favoured by most surgeries.

A10. Internet of Things Applications.

Increasingly individuals are using internet-enabled devices to generate trustworthy personal data. But they lack, at the moment, any infrastructural means to control where that information is sent over the network. Examples include:

- Location data, as generated by GPS functionality often found on mobile devices.
- Health data, as generated by personal health monitoring devices
- Consumption / need data, as generated by Amazon-type buttons that can be positioned around someone's house

While there are many standalone apps that allow some degree control over the data generated by devices, all are stove-piped in one way or another. What individuals need is the means to gather data from different devices, aggregate it if they wish, and determine where the results are sent and who gets to see them. A PDS infrastructure would meet this need.
