



Personal Identity in an Electronic Age

The Challenge Of Identity

In the “paper world”, most of us have a good idea of what we mean by personal identity. We are familiar with face-to-face contact, delivery of conventional mail to physical addresses and conversing on the telephone. Even though we can be deceived, signals in these transactions help to build up a perception of somebody we are dealing with in the real world. But when we consider identity in the context of electronic transactions, we are forced to think a bit harder. We may never meet the other person in the flesh and e-mails arrive in our in-box with no reliable indication of their physical source. It is an unfamiliar world and we are not sure how to behave in it to build up trust – is it indeed even a real person or organisation we are dealing with?

Key Points

- Identity is complex: there is no absolute definition of identity, only a collection of attributes and a number of alternatives. We use different combinations or derivations of those attributes in different circumstances - and can thus appear to become different people in different contexts.
- Identity is only relevant when there is someone else, known as the “relying party”, who typically needs it to provide entitlements, assign responsibilities for meeting financial obligations, or ascertain other attributes, such as trustworthiness.
- In the online world, an electronic certificate can help to provide authentication and details of an identity associated with that certificate.
- Great care is needed when using a credential outside its original context.
- Electronic forms of credentials work analogously to familiar real world and paper world examples (see last paragraph for a discussion of identification in the electronic world).
- A certificate does not last for ever and needs to be replaced every few years.

What Do We Mean By Identity?

There are two uses of the term ‘identity’, both of which are defined in the Oxford English Dictionary:

- In the abstract sense, applied to an individual’s persona.
- A label that uniquely identifies an individual – a means of identification.

In this paper, the term ‘identity’ is used in the second sense, but, to avoid confusion, some may prefer the term ‘identifier’. With this definition, an individual has many identities, e.g. a person’s given name, sports club membership number, a National Insurance Number, a bank account number. There are also role-based identities (e.g. a by-product of our current employment) and group identities, ranging from families to companies, while in practice the same identifier could be used for different people by different relying parties. Identity can thus be seen to be dependent on context.

Why Do We Need An Identity?

We need an identity in order that other people (or organisations, or things) can distinguish us. A second party is always involved: an identity on a deserted island is of no use (and, some would say, has little meaning). The second party, referred to as the ‘relying party’ in this paper, typically, needs to:

- Provide entitlements such as state benefits or the services of a club or association to which we belong.
- Assign responsibilities for meeting financial obligations, such as paying taxes, paying bills for goods or services received, or reparation of damage or injury.
- Ascertain attributes, such as trustworthiness, in relation to a particular transaction.

What Does An Identity Do?

An identity provides a unique reference to facts about an individual. This concept works in the real world: when I meet my friend John Smith in the street, I don't need to know his name because I recognise his face – the facial pattern acts as an identity for my pattern-matching brain cells. My brain can immediately gain access to a host of facts stored away over the years. These facts come to the surface as appropriate to our meeting and conversation. If John calls me on the telephone, I am likely to recognise his voice (another form of identity), but to confirm, he will probably announce his name. If he writes, I recognise his handwriting and signature. If I meet another friend who also knows John, we may need to check that we are both talking about the John Smith who works for X or lives at Y, before we are confident it is the same John Smith. This shows that it is not identity that is important, but the facts associated with an individual; the identity is only an index.

How Do I Prove Who I Am?

For an individual to demonstrate entitlement to or ownership of an identity the following elements are normally needed:

1. A registration process, to verify and record details of the claimed identity
2. An unforgeable certificate that certifies the registration and validity of the identity.
3. A unique and irreproducible characteristic (or a combination of characteristics) associated with the individual and bound to the certificate.

The certificate and the unique characteristic together are known as a credential.

For most UK citizens, an example in the paper world is the birth certificate, which demonstrates name, date of birth and parenthood. It also has a unique number. Although often used as part of a process for establishing identity, a birth certificate itself is not an identity document: it is purely a record of an event in time – a birth.

Consider a British passport: this is issued by the UK Passport Agency in a tried and tested process involving attestations and a witnessed photograph. The certificate is the passport; the identity is the passport number; the unique characteristic is a combination of the facial appearance of the individual and the ability to reproduce a signature. A copy of the face (photo) and an instance of the signing ability (a signature) are included in the passport. Normally, presentation of the facial appearance is all that is needed to prove ownership of the passport and entitlement to the other identifying information, such as date of birth, within. However, the primary purpose of the passport is to attest to nationality, not to the information contained in it.

Similar remarks apply to the latest versions of the driving licence photocard, noting that the driving licence attests to driver status and that one can't interchange a passport and a driving licence, despite the fact that they contain almost the same core information. This is because the relying parties in each case need to trust the registration processes of one of the two issuing agencies for their purpose: the lack of a consensus on a trust model is a key problem in addressing identity-related issues.

It is also instructive to note that the other information in the passport (name, date and place of birth, etc.) provides a link back to other documents, such as a birth certificate. They are not normally needed directly by immigration officials, since the information could be obtained from the UK Passport Agency by quoting the passport number. We have grown to accept that this is what passports must contain, even though we may have no wish to reveal our "real" name and date of birth at every border crossing.

What Identity Must Be Registered?

For most service organisations, it is normally sufficient to know that the person seeking a service (including sale of goods) or being pursued for a bill is the same person as signed up for the service in the first place. The service provider uses an alphanumeric identity for the customer (numbers for bank account, loyalty card or sports club, for example) or transaction (order number). Appropriate credentials are issued in each case.

Interesting issues arise at that initial signing-on, when the service provider (the relying party) needs to be satisfied that the individual can be sufficiently trusted for the service to be provided and issues the identity and credential. Except in some special cases, the real name of an individual may not be important. Where a credit card is used, the important issue is often the validity of the credit card number, not the individual's name. However, there may be other considerations:

- Banks are required to check identity to prevent money laundering (in practice this is largely a check on name and address).
- Law or regulation may restrict the service being provided: tobacco products and certain films are restricted according to age; discounts may be conditional on membership of a club or residency within the boundary of a local authority.
- A supplier may want to be sure about a delivery address, especially where the goods or service are to be delivered and may cause embarrassment or inconvenience – the ton of farmyard manure delivered to the front drive is a rather trivial example.

So, at registration, it is necessary to collect relevant facts about a person, including other identity relationships, in order to check details with other agencies, e.g. electoral roll or credit rating agency.

Cross-Community Identities

Some of us are familiar with being asked to show a driving licence (more acceptable as a credential in its photocard form) to prove our age in a pub. Also familiar to most is the use of a utility bill to support an application to open a bank account. These are examples of cross-community use of credentials. Neither the driving licence nor the utility bill were created with a secondary identifying purpose in mind, (and the latter after all can be easily faked). In both cases, the issuer has no relationship to the relying party, nor has it any involvement in the relying party's decision to accept the credential as evidence. Relying parties need to know what they can infer from the presentation of a credential issued by a third party. In particular, they should understand the issuing policy, how identity is checked and what degree of confidence there is in the checking. They should also be aware that the issuing policy could change without notice.

The situation is exemplified by the example of the UK Government, which wanted to make use of electronic credentials issued by third parties to certify the identity of individuals wishing to make use of government services. This was to avoid government having to issue its own credentials and register individuals. One issue with the model was the lack of trust between public sector organisations and the issuing parties: it was only possible for the latter to verify those aspects of identity known to the issuing party, not government identities (such as National Insurance Number). This approach failed to deliver the anticipated benefits of a single credential that could be used for a variety of electronic interactions.

Interoperability

In an ideal world, some people envisage a single credential capable of identifying them to a wide range of electronic service providers. In practice, there are significant difficulties. At the privacy and security level, it is not appropriate for the same identity to be 'broadcast' to all parties: most people, for example, would not want to use the same online identity for amazon.com that is used for access to their medical records. The various technologies may all adhere in theory to the same standards, but in practice interoperability can often prove to be an issue. Technology vendors are working to improve this and there has been recent progress in this area.

More significant blockers to interoperability are issues of trust and identity. This refers back to cross-community use of identities and credentials. There is no common standard for how a name and address are presented; subtle spelling mistakes, abbreviations and so on, make matching two records of an identity unreliable in general. But the real issue is the trust model: the credential issuer is working to their own risk model, which another relying party may not share. For a variety of reasons, it may therefore be some while before a market for widely interoperable electronic identity systems emerges.

Privacy

It is generally accepted that the 'need to know' someone's identity should be proportionate to the circumstance. What degree of certainty and confidence is necessary for transactions? We may just want assurance of payment rather than someone's identity, but a simple identity suitable for payment may not be appropriate where information on criminal convictions is required. There is an obvious conflict between the need to identify and the right to confidentiality.

As discussed earlier, identity certificates often provide more information than is necessary for the transaction: for example a passport contains a date of birth. The more a single identity certificate is used, the greater the threat if it is stolen or its use monitored. For example, the use of digital signatures has serious implications for privacy, not least because 'e-trails' are left every time a signature is used.

Identification In The Electronic World

In the electronic world, we make use of technologies that, like the passport or driving licence, certify an identity. Also similarly to the real world we rely on those we trust (intermediaries) to give us confidence that the identity can be relied on. The remainder of this section discusses the electronic identities that are typically used.

The most familiar is the well-tried username and password combination. In this case, the username is unique to a community and is an index to much more information about the individual. When the individual joins the community, information is collected and stored appropriate to the service and the username is issued. Subsequent typing of the username and password combination shows that this is the same person that registered initially. Or at least, we hope it is, bearing in mind all the things that can go wrong with passwords being copied, guessed or even given away (the theft of user IDs and passwords is now a real danger, with 'phishing' attacks that lure users into handing them over in the mistaken belief they are dealing with a legitimate party when in reality they are not). Tokens, which the user must possess, can strengthen username and password systems.

Digital certificates have received considerable publicity in the context of electronic commerce. The technology is commonly referred to as public key infrastructure (PKI). In essence, a digital certificate is a non-forgeable link between an identity and a secret possessed by an individual. The individual registers an identity and is provided with a unique characteristic by a Certification Authority (CA), which is an intermediary that relying parties are likely to trust. The unique characteristic is a pair of cryptographic keys. One of these is kept secret, a so-called private key. The other key, uniquely matched, is the public key. Both keys are very long and so practically impossible to guess or memorise. They are always stored on some computer device - a PC or, best, a smart card.

An individual can sign data using the private key. Losing the private key, or having it copied, means the identity is stolen, so an effective means of protecting it is essential. Signing means digital signing, which is a cryptographic process that ensures the data cannot be modified without detection, nor can data be created by anyone other than the individual possessing the private key. The code resulting from this process is called a digital signature. The signature is uniquely and differently generated for each set of data. Checking the signature requires access to the other half of the unique characteristic, the public key. This is contained in a certificate digitally signed by the CA. The certificate itself is (normally) public and certainly must be made available to relying parties wishing to authenticate the individual and verify the identity. However, this illustrates the problem with raw PKI – it broadcasts the same identifier – the public key – to all parties, presenting serious privacy concerns.

The critical technical factors in a PKI are generating the cryptographic keys without compromising the mathematics that gives us confidence in the process and keeping the private key secret. Smart cards help in both cases, because they can do the cryptographic processing on the card so the private key never leaves the card. They are also self-contained, so we can be reasonably assured they operate correctly, and they can be made tamper-resistant. Their portability makes them very flexible. An individual needs something to identify himself to the smart card. A PIN is common, but a biometric feature, such as a fingerprint, is better.

Biometrics has been hailed as an important step forward in helping to bind individual and identity. Various forms are in use, including fingerprints, facial features, palm prints and retina patterns. All can give a high probability of uniquely identifying an individual under tightly controlled circumstances, but in real-world operational conditions, accuracy depends on how sensitively the systems are configured – with application specific compromises between speed of throughput, false positives and false negatives being common.

Technologies to enable identity to be securely registered and used are already available. The capability of the technology is broadly understood, the issues are how they will work with real people in the real world, and what trade-offs between cost, privacy and convenience are acceptable. What is often lacking however is the associated business and policy model that enables such technologies to be successfully deployed.