Open Source ID Cards?
By Jason Kitcat, j-dom.org, originally published in LinuxUser

Blunkett has gone but his legacy, the Identity Cards Bill 2005, marches on. To many it seems almost unbelievable that MPs are actually going to be debating a bill on ID cards here in the UK. Follow me on a journey to see how we got here and where, if we're lucky, we could go next.

How we got here

The 9/11 attacks on the twin towers and the Pentagon shocked the Western world into a sense of insecurity not seen since the Cold War. This public nervousness provided the political leverage the Labour government needed to bring ID cards onto the agenda. Fear of terrorism has been used by governments around the world to introduce authoritarian new measures in the name of protecting the citizenry. Here in the UK such moves coincided with the Government's long tradition of centralising control to Whitehall.

US demands for biometric passports along with mainland Europe's development of ever more comprehensive identity schemes only acted to accelerate the desire for a British scheme. With both Jack Straw and David Blunkett revealing strong authoritarian streaks whilst running the Home Office, ideas that had seemed previously unthinkable were being floated. The notion of a centralised database of people in the UK that would store photos, fingerprints and iris scans must have been more than a little tempting to both Home Secretaries.

However Straw and Blunkett shouldn't have felt under too much pressure from our international partners' apparent progress. The US suffers from massive identity fraud due to over-reliance on the single Social Security Number by banks, local authorities and other organisations. Elsewhere countries with legal systems based on the Napoleonic code have serious advantages. They have a consistent legal and institutional basis for protecting the privacy of data. They also usually have a national register of citizens meaning that introducing ID cards is a project of changing a paper booklet to a card of some kind, not the creation of a register from scratch. The controls are such that a user in Estonia, for example, can even view the data held on them and track those who have accessed this data. With highly distributed data and a culture of secrecy in government it is hard to imagine such access to our own data in the UK or the USA.

Nevertheless when the Home Office announced a consultation on ID cards few were expecting the Home Office to claim that the majority of respondents supported the proposals. In fact about 70% of responses where opposed to introducing ID cards. Yet, by arbitrarily splitting the responses, the Home Office went to the press claiming support for their proposals, bitterly disappointing the majority of nearly 10,000 submissions who were against ID cards. So oblivious to criticism the bill was drafted.

The Proposal

The Bill as it has been presented to Parliament is an extraordinary beast. It details over 50 types of data the new national register would hold, including connections to

health service, passport, drivers license and national insurance numbers. While the ID cards would not initially be compulsory the Bill creates a bizarre “superaffirmative” process to avoid primary legislation (and thus debate) thereby allowing cards to be made compulsory at a later date. Much of the bill is lacking in oversight: The costing is effectively a blank cheque and the new National Identity Scheme Commissioner’s reports can be redacted by the Home Office before being submitted to Parliament.

The bill creates incredible new powers for the Home Secretary along with a large number of new crimes some of which you may not even knowingly commit because the bill creates a presumption that data in the register will always be accurate. The new crimes carry delightful penalties from heavy fines to imprisonment.

Despite the scale of the proposed legislation, this highly complex bill, which delivers extraordinary new powers, is being rushed through parliament at a very high pace. This makes it far more likely that errors and loopholes will creep in. Loose wording in the bill has led to speculation that virtually all private transactions would be fed through the national identity register. The Regulatory Impact Assessment document which accompanied the bill states that the legislation allows for the new register to record when and who made checks to the database. These checks could be conducted by banks and insurance companies trying to prevent fraud, employers checking an immigrant’s status, by retailers trying to stop credit card fraud or even video shops wanting proof of address. As IT newspaper *Computing* reported several experts thought such a scale of ambition bordered on the absurd. Mike Rodd of the British Computer Society said that ‘to create this huge database of information starts smacking of some sort of authoritarian state. This could really cause an outrage.’

As quoted in *Computing* Professor Jim Norton went even further: ‘Recording every high-value transaction doesn’t sound like a great idea to me. The idea of having a huge database and sucking vast amounts of information into it seems to me to be remarkably naïve on one hand, and a potential major burden on business on the other.’

While financial organisations such as Visa and Mastercard can handle massive volumes of transactions daily they can do so by taking a risk management approach. They can accept that a certain percentage of transactions will be fraudulent while knowing that overall profits will outweigh the costs. A government card project is different, it needs to focus on accuracy which is remarkable expensive. Just one incorrect record could result in massive disruption to a citizen’s life. This fundamentally changes the economics and approach that needs to be taken to a national identity card project when compared with commercial implementations.

Can ID cards deliver the benefits?

Some readers may recall that the proposed identity cards were originally being sold to the public as ‘entitlement cards’. The core purpose of the cards would be to prevent illegal use of public services. Only those legally allowed in the UK would hold cards and the card would need to be presented before a service, such as health, would be delivered.

However those canny Peers in the House of Lords weren't having any of it. Many refused to use the term 'entitlement card' at all on the basis that it was just a fluffy cover for the true proposal which was for a national identity card system. So by 2003 the Government decided not to pretend any longer and we were all talking about identity cards.

The idea remains that the card will be needed to seek employment, or to use services such as benefits, health and possibly libraries. Unfortunately people pretending to be someone they aren't is a tiny proportion of fraud. The Australian Department for Social Security estimates that false identity fraud accounts for around 0.6% of benefit overpayment compared with non-reporting of income variation which accounts for 61%. Similarly Chris Pond MP, Parliamentary Under-Secretary at the Department of Work and Pensions, reported to the Home Affairs Committee that his department estimates that of £2 billion in annual benefits fraud only £50 million comes as a result of false identities. Whilst illegal immigration is a political hot potato the reality is that most fraudulent claimants are already established in the UK and know how to work the system. The vast majority of migration is legal and economically beneficial (see sidebar on Poland), the UK has more jobs that need filling than we have people. Identity fraud just isn't the problem it has been painted to be.

The Terrorism Card

Naturally crime prevention and detection agencies such as the police, the security services, customs and the immigration service are all as keen as mustard to make use of the card. The Government argues that identity cards would be an important new tool in the fight against terrorism. Home Secretary David Blunkett told Parliament that the security services advised him that 35% of terrorists use false identification.

The only research ever conducted on identity cards and terrorism had some interesting findings. The Privacy International report found that 'of the 25 countries that have been most adversely affected by terrorism since 1986, eighty per cent have national identity cards, one third of which incorporate biometrics….Almost two thirds of known terrorists operate under their true identity The remainder use a variety of techniques to forge or impersonate identity. It is possible that the existence of a high integrity identity card would provide a measure of improved legitimacy for these people.'

We need to accept that fake ID cards will appear in fairly short order. According to the NO2ID campaign prosecutions for dealing in or creating false identity documents and cards have been pursued in Britain, Hong Kong, Pakistan, Ireland, Malaysia, Yemen, Czech Republic, Venezuela, India, Italy and Sri Lanka. Furthermore the Israeli government estimates that there are hundreds of thousands of fake ID cards in the hands of its population.

How can counterfeiting be possible with hi-tech smartcards that include biometrics and cryptographic certificates? Well the smartest way to get a false ID card is to present fake documents when applying for a card or to bribe a bureaucrat. Such approaches totally bypass the technological security measures. Alternatively one

can take a high-tech approach. Blank smartcards can be bought fairly easily and so can geeks, combine the two and await your new identity. It is worth noting though that the perpetrators of recent atrocities didn't bother with any kind of identity fraud. As Privacy International notes 'terrorists have traditionally moved across borders using tourist visas (such as those who were involved in the US terrorist attacks), or they are domicile and equipped with legitimate identification cards (such as those who carried out the Madrid bombings).'

Convenience

Those who watch the political circus closely will have heard much use of 'choice' and 'convenience' in recent rhetoric from all the main parties. Well people won't have much choice over using the identity cards but, if the system actually works, it does present a convenient alternative to current arrangements for identification based on a multitude of overlapping documents.

As in other European countries (see the sidebar on Poland) the Government proposes tying the central national registry database to databases from the Driver and Vehicle Licensing Agency, the Passport Agency, Inland Revenue and National Statistics. This will provide a cross-cutting single reference number to manage the exploding number of databases government departments run. So potentially one wouldn't need to have quite so many cards and passwords to access various services. However the risk is that this creates a single point of failure which facilitates identity theft. The alternative is to use a single number but still distribute the risk so that a second number is used in each context – so we retain a passport number and national insurance number which need to be used in conjunction with the new nationally identifying number. With a little forethought numbers from EU cards could also be used in the UK without a new UK card needing to be issued. This would help to facilitate the free-flowing workforce which is one of the key proposed benefits of the union.

A single unified identity is something many commercial and government service providers are desperately impatient for. For example the CORE project aims to provide a single national register of electors. It will be a key step towards making national electronic voting possible. However without an identity card it will be yet another island of information disconnected from the rest of government. During e-voting pilots in Sheffield smartcards with a unique number were issued to voters as there was no other identifying number the providers could rely on all voters having. However because only a small number of other services were tied to the card and people inevitably moved to and from the area, if another e-vote was to be held the card would need to be re-issued (see http://www.smartsheffield.com).

Implementation

No country with a Common law system as we have in the UK has ever embarked on an identity card system which includes biometrics and such a broad range of uses. In fact our European partners have much more limited schemes whilst the more strict governments in Malaysia, Singapore and Thailand do have systems similar to the proposed British register. While China is moving towards a compulsory card it

has abandoned the idea of including biometric data having concluded that biometrics are unworkable with large populations.

Even if all our government departments' systems weren't in a mess the biometric aspect of the proposals would be highly problematic. The time and cost involved in recording fingerprints and iris scans for every registered individual would be just insanely gargantuan. Furthermore biometric readers suffer from false positives (saying someone is the person on the card when they aren't) and false negatives (saying someone isn't the person on the card when in fact they are). While the error rates are numerically small, on large scales the errors become disturbing. Take an example biometric accuracy rate of 99.99% (for false negatives and positives) and a database of 40 million users. With a 0.01% error rate a single scan against the database would result in 4,000 matches. Error rates are continuously falling but recent data from the US shows that we'd still have 400 matches to deal with instead of the expected one per unique individual. Biometrics just aren't the simple solution they have been portrayed to be.

The UK government has a habit of building IT disasters. The list is a long and shameful one of the taxpayer money wasted on failed government systems. Projects are frequently poorly specified, often due to political pressures, and costings are disconnected with reality. A desperate lack of internal IT skills is compounded by the recurrent belief that government requirements are unique. Thus instead of buying packaged software that works government keeps embarking on massive bespoke development projects that are high risk and high cost.

If it ever worked we would probably end up with an expensive, closed system with mediocre security that was barely used. We can certainly see that other expensive systems, such as Transport for London's Oyster smartcard, have shown a lack of foresight. The Oyster project has put a contactless smartcard in the hands of millions and yet it runs a proprietary platform meaning that other services and providers cannot easily plug into the existing infrastructure. London boroughs are left to work on their own smartcard projects, though Newham has managed to combine their smartcard with an Oyster chip in one card.

Getting federal

It's at the borough and council levels that identity cards really get intriguing. Across the UK a large number of authorities are experimenting with smartcard technology to facilitate library use, benefits, transport, social inclusion along with a raft of other services. Much of the work has been done as part of the National Smart Card Project which tries to prevent continual re-invention of the wheel by authorities working in splendid isolation. This project, which has operated way under the radar of many ID card activists has been doing internationally pioneering work.

Some have argued that the ID card bill will eventually founder and sink. In its place would be locally issued cards based on the National Smart Card Project's work. Residents could be given standards-based cards by their local authority which would be usable in any region, no matter where a resident might move to. This idea of federation, or "citizen control of their own card" as Mick Davies, a key adviser to the National Project, puts it could help to encourage acceptance. The vision is that users

would be able to decide which private or public service could access details on the card. Those who choose not to use the smartcard for library access, for example, would be able to take a separate unlinked library card. Local authority systems would need to interoperate so that a resident from Sheffield would be identifiable when living in Portsmouth.

Much of the work for the National Project has been on the JavaCard platform and will shortly be released, according to Davies, as Crown-owned software under 'some open source licensing variants'. This is a positive sign as a report by the Institute for the Management of Information Systems noted that a first step for the introduction of an ID card would be 'the development and testing of … standards for the robust and secure inter-operability of multi-level authentication and authorisation within the public sector and of open source routines for similar inter-operability with private sector systems, particularly those of the banks, credit card companies and credit reference agencies.' The National Project is yet to deliver it's opened source, so what is available today?

Open Source ID cards

Venerable Linux activist Doc Searls has noted, digital identity is at the unfertilised egg stage of development. Yet already, in his view, a scary lineup of interests are deeply involved in developing identity technologies. He argues that open source approaches are desperately needed. While Microsoft's retreat after the uproar over their Passport initiative has given us all some time, other private interests won't wait. Fortunately there has been some open source activity but not as much as one might expect..

The Estonian Government have been leaders in using open source approaches in the introduction of the ID card infrastructure (see sidebar). To try and prevent the proliferation of non-interoperable proprietary standards the government has promoted OpenXAdES.org. Working in collaboration with the Finnish government this project develops free software relating to XML-based electronic signatures.

At the hardware level there is some activity: The wonderfully named MUSCLE (Movement for the Use of Smart Cards in a Linux Environment) provide Linux drivers and application development tools. The GNU Card Operating System (gcos) was a smart card operating system project that shutdown due to lack of interest. However there is a GPL'ed smart card operating system designed for education, SOSSE.

But what about beyond the geeky hardware level? Can the Open Source movement help with unified identity in the way that is more community-driven than any nationally imposed identification number? Is there a Creative Commons in the world of digital identity? Well sort of. In response to commercial identity schemes there are two leading projects, Identity Commons and Sxip (pronounced 'skip').

Sxip is a decentralised network which allows a single login into multiple sites using an XML-based standard. On joining the Sxip Network users are assigned one or more GUPIs (Globally Unique Persona Identifier). While not yet developed for use in smartcards Sxip provides a very robust, decentralised architecture which doesn't allow or need any communication between network nodes without the user's

permission. Potentially an ideal architecture for a localised, federated identity smartcard. However while the technology is open, the network is run by a privately held company.

Identity Commons is cooperatively owned, operated and governed by its users. It uses the open XRI/XDI architecture developed collaboratively through the OASIS standards group. From the ground up the approach is user-owned and controlled. It is based on “i-names” which are persistent identifiers for people or organisations. i-names are universal persistent private addresses that can be used for single sign-on, spam prevention and universal contact information. A single i-name can point to telephone, email or website and is compatible with any new protocols. Identity Commons are developing ‘link contracts’ that control who can access and use items of personal information. Such a combination of user-centric privacy control and a universal identifier is very attractive for identity cards. Unfortunately much of the Identity Commons network is still under development and there is only one i-name registrar. However i-names are inherently compatible with smartcards. It would only take one authority or government to use i-names in their smartcard before Identity Commons would gain serious international weight.

Conclusions

So how can we bring the Open Source community together with the Home Office’s steamroller drive towards a national biometric identity card? If the bill as it stands passes through Parliament then there’s little that can be done. However if enough MPs and Peers can prevent or at least amend the bill, we have a chance. We need to ensure that the hardware is open and interoperable. More importantly we need to, as Estonia have done, use open and accessible standards for unified identity. People need be given the opportunity to easily control and correct the data held on them for any identity scheme. By plugging into the Sxip or Identity Commons approaches not only would our identity scheme be more user driven but it would be much more useful. The whole community could benefit, not just government and their suppliers.

** Sidebar: Le smartcard

The US, Germany, Japan and Austria all played a part in the development of what became known as smartcards with patents that pre-date Frenchman Roland Moreno’s pioneering work. However during the 1970s it was the French who invested heavily in developments as part of an overall push to modernise France’s infrastructure.

Bull made the first R&D investments and hold around 60 related patents for what was known as ‘carte à memoire’. During a campaign to export the technology Roy Bright at the French government’s marketing organisation Intelimatique coined ‘smartcard’.

The two first mass deployments of smartcards were in French payphones (Télécarte) and then in debit cards (Carte Bleu). These were contact-based cards which needed a physical connection with the reader. More recent cards such as Transport for London’s Oyster card and Hong Kong’s Octupus card are contactless.

While significantly harder to fraudulently duplicate than magnetic stripe cards, there are several lines of attack that have been recently publicised, even for so called ‘tamper resistant’ cards.

Sources: Wikipedia, North East Regional Smartcard Consortium

** EOF sidebar

** Sidebar: The Polish Identity Card

In Poland the communist regime used identity papers as a key part of their authoritarian control. Russian policy was a major influence on how the Polish communists behaved and Stalin was a master at abusing papers: To control rebellious ethnic groups he would ship them far from their homes and then withhold their papers. Travelling without identity papers held penalties as severe as death.

Even after communism citizens held onto their PESEL personal number. This number was automatically issued along with a passport-type identity booklet when citizens became 18. More recently however Poles have been issued modern non-smart identity cards with limited information including name, parents’ names, signature, date of birth, place of birth, height, eye colour, sex, photo and address on the card. The PESEL is also on the EU-type driving license card and passport.

However while this PESEL number links all these documents each item also has its own unique identifier. So on a passport there is an ID card number and a passport number. If any of these items are lost then those specific document numbers are invalidated and replaced. Thus the convenience of a single number is kept without providing a simple single point of failure.

For Michal, an electrical engineer coming to the UK to find work, the lack of clear identify here is bewildering. He visits a Jobcentre Plus to get a national insurance number but he’s told that he needs a job and a six month wait before he can get the number. But people don’t want to employ him without a national insurance number or a UK bank account. So he visits several banks, but they won’t accept his Polish identity book or his Polish EU-style driving license. His Polish EU-style passport is accepted but 3 other forms of identity are needed, two of which need to include an address for where he’s staying in the UK. Acceptable proof of address includes bills, but you can’t get a bill unless you have a bank account to pay for the service. Alternatives are letters from people such as teachers but again without a bank account it is hard to start a course through which a teacher could get to know Michal. A catch-22 and a long way from how Polish bureaucracy operates where Michal’s identity documents are enough to open bank accounts, get married or buy a car.

Fortunately a potential employer decides to help Michal. The employer hires Michal and provides the necessary references he needs to get a bank account and national insurance number. Within a few weeks he is enjoying his job and taking a part-time English course.

** EOF sidebar

** Sidebar: ID Cards in Europe

Estonia
A small country of only 1.35 million people, Estonia has wiped the slate clean since the Iron Curtain fell. Estonia is pioneering paperless government, electronic voting, mobile phone parking and identity smartcards. Since launching their new ID system 650,000 cards have been issued. On each card is personal data, a nationally established email address, a photo and two private keys. One of the keys is used for identifying the user and the other is for signing legally binding documents such as wills, contracts and transfers of deeds.

Epp Maaten, Adviser to the Estonian Elections Department, admits that the majority of the ID cards have not yet been used to sign anything as users need readers and software to use the signing functionality. However including the keys on the card now, he argues, allows for the development of robust applications such as e-voting in the future based on the knowledge that a solid identity infrastructure is already in the hands of citizens. Digital signatures as based on the open source OpenXAdES project which the Estonian government has helped to promote.

Estonia's cards are innovative in that they hold no applications on the card. Many have argued for cards with multiple applications on them or at least a single application. However smartcards' limited processor and memory capacities provide severe limitations. So the Government has let the cards be incredibly simple and pushed the applications onto any organisations that choose to use the card.

Sweden
Not only the country of Ikea and the England football team's philandering manager but also home to a successful national identity card project. They're so organised in Sweden that at the end of the tax year you can ask to receive a text message from the tax authority. If the figures they have calculated for you are right then send a confirmation and your tax return is done.

As in many European countries, Sweden already had a national ID register of individual 'personnummers' so it wasn't a huge leap to get cards into the hands of their citizens. Now that the cards are available they can be used in a wide variety of applications such as paying for a tram journey or secure government communications. However the cards are voluntary and so while all citizens have a 'personnummer' they do not all have to hold a card.

Using a public-key infrastructure the ID card has been used to enable a 'one-stop-shop' for 24/7 interaction with local and national authorities. In fact if a Swedish resident moves district they receive a 'goodbye' letter from their old school, health service and local council along with a 'hello' letter from the new. To anyone who has recently moved within the UK, this sounds almost scarily efficient.

For a summary of ID card progress across Europe visit:
http://www.electronic-identity.org/e-id_europe.shtml

** EOF Sidebar

** Useful Links

The National Smart Card Project
http://www.nationalsmartcardproject.org.uk

Identity Smart Cards that work on a national level
http://www.financialcryptography.com/mt/archives/000249.html

The Estonian ID card
http://www.id.ee

Identity Commons
http://identitycommons.net

Sxip
http://sxip.org

NO2ID, the campaign against ID cards has a website packed with useful information
http://www.no2id.net

Privacy International's report on ID cards and terrorism
http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf

** EOF links

Jason Kitcat (jason@swingdigital.com) is Managing Director of online community consultancy, Swing Digital.