DATA SECURITY

Government to create marketplace for citizens' personal identity data

The government's data sharing plans will need robust security measures to gain people's trust, writes **Mark Ballard**

The government is preparing to create a marketplace for citizens' personal data to be used for accessing online public services, according to documents that were issued to industry in preparation for the coalition's next-generation identity scheme.

The plan, obtained by Computer Weekly, may prove highly controversial, as it offers limited assurances as to how much control people would have over how their data is used.

The coalition intends to "create the commercial, legislative and regulatory environment" in which a private sector ID industry may thrive, it said in briefing papers sent to industry in April.

The proposals would create a personal data marketplace populated by banks, phone companies, the Post Office and others that may involve government departments selling access to their own citizen databases. The government has proposed that it may join the market by selling data services to private ID companies and data agents.

Government plans offer limited assurances as to how much control people would have over how their data is used

The creation of a private data market would allow the government to dismantle its own data sharing networks, said a draft technical blueprint for the proposal, a paper called *Identity Assurance (IDA) Technical Infrastructure Services*. Current data sharing arrangements include links between departments such as HM Revenue & Customs (HMRC) and the UK Border Agency.

The detailed proposal describes how the coalition intends to act as a "catalyst" on the nascent online ID industry that grew in the shadows while the Labour government was trying to build a public ID card system. The new plan would support the industry by defining universal ID standards and mandating that all government agencies must verify

DWP prepares alternative to identity cards for Universal Credit

The Department for Work and Pensions (DWP) is grooming a British tech start-up to play a key role in its £2bn Universal Credit benefits system and give shape to the coalition government's plans for identity assurance in a world without identity cards.

The start-up firm, Mydex, is developing technology that promises to take power over identity assurance out of government hands and place it with individuals, and take responsibility for identity assurance out of Whitehall and leave it to the market. The firm is being lined up as a solution to a number of public sector computing issues.

Foremost for the DWP, which is trialling Mydex as a means for people to log in, register, manage and collect their Universal Credit, is the technology's potential to save the government from trying to build its own identity assurance platform when budgets are tight, and after the Labour government's efforts on the Identity Cards scheme proved so costly and such a political and technical failure.

Steve Riley, IT director at Job Centre Plus, told Computer Weekly that DWP and HM Revenue & Customs (HMRC), which are jointly developing Universal Credit, have been given until the end of the year to establish an identity assurance blueprint for the new benefits system.

"We definitely need to crack that," he said. "And Mydex is one of the things that's in the pot. DWP is involved in a Mydex pilot with local authorities. We need to have an answer and a plan by the end of this year."

The clock is ticking on Mydex's as-yet unproven technology, just as it is on the host of government services that are counting on the Mydex pilots delivering a working identity assurance system before the winter of this parliament's term.

Mydex is aiming to have its system fully operational by the end of the year, a deadline that will coincide not only with crunch-time for Universal Credit but also the unveiling by Cabinet Office minister Francis Maude of the coalition's market-led solution to identity assurance in government.

Dane Wright, IT strategy manager at London Borough of Brent, said government agencies need to find a credible way of authenticating people's identities online now they would be unable to use identity cards. "The abandonment of the ID Scheme was positive from a data privacy point of view. But from an electronic identity assurance point of view, it's rather unfortunate," he said.

The identity cards system would have drawn from government databases a real-time authorisation that Whitehall departments could use to check someone's identity before allowing them to perform sensitive tasks such as pay council tax, claim benefit or change their address.

Mydex proposes doing the same thing, but by acting as an agent for individuals, and drawing nuggets of identity authorisation from an ecosystem that already includes credit reference agency Experian and may extend to a range of other source.

The DWP had been at the heart of the cross-government system of databases that was to underpin the Identity Card Scheme but became embroiled in intractable differences over governance, ownership and funding with HMRC that effectively made the whole project unfeasible.

people using approved private sector ID agencies.

Protecting citizens' privacy

The government is aiming for a system of "citizen-centric data sharing" of the sort it has been trialling with East London start-up Mydex (*see box*). It proposes to better protect people's privacy by allowing them to choose their identity agent and giving them a say in when and what items of their personal data is shared.

The draft *Identity Assurance Service Description*, also sent out to industry in April, suggested citizens must be able to "view an audit... describing how identity data has been used", and that the personal data market should operate transparently.

But while the Cabinet Office is drafting rules that will give people power to "view and control the personal data that is held about them by public sector", it has stopped shy of proposing those powers should have a hold over the private sector. The plans also ignored a principle laid down last year by the Council of Europe that people should have a right over the algorithms companies use to process their personal data.

Rights to personal data

Guy Herbert, general secretary of privacy campaign group No2ID, after being invited into the Cabinet Office to review the plan, said there was "absolute obscurity" over its legal framework. He was concerned people would not be given rights over their own personal data.

The Cabinet Office plan said personal data agents – known as attribute providers – will "exchange...data (attributes)" in the market "potentially/usually under the citizen's control". It gave no further assurances of any controls people would be given over the use of their personal data attributes by the market.

The documents did attempt to allay fears associated with the last government's data sharing regime by promising that it will not lead to the creation of a dedicated public sector database and that the government will create "no database of databases" or master index of citizens operating within the private ID ecosystem.

William Heath, chairman of Mydex, was sceptical about the Cabinet Office's promise to create a "customer-centric" ID marketplace. If the market was operated by large companies aiming to make money from their customer's personal data, it might still be customer-centric without actually giving people control over their own personal data, he said.

Personal data exchange

The government is weighing up whether its proposal should include building an ID and data hub, which will act like a stock exchange, brokering transactions in the personal data marketplace. The government would own the hub and the Cabinet Office is preparing to issue a call for tender for someone to build such a system in the autumn.

The Cabinet Office plans for people to be able to register to vote using private sector ID providers in time for the next General Election, in 2014.

HMRC has meanwhile been tasked with giving businesses a one-click registration using private ID providers by the end of the year, said the draft proposals. ■

Sign up to Computer Weekly to download draft government ID services plans:

Identity Assurance Service Description
computerweekly.com/246980.htm
Identity Assurance (IDA) – Technical Infrastructure Services
computerweekly.com/246979.htm

London council makes world's first citizen data transfer

In March, a London borough council conducted what it claims was the world's first live exchange between a public authority and a citizen using a personal data store.

Brent Council made the link as part of a pilot that has followed in the wake of the identity card scheme as a means for people to hold their own personal data and choose their own means of authenticating their identity.

Developed by Mydex, a not-for-profit start-up from East London's high-tech hub, the technology has the potential to make many public personal databases redundant. The Department for Work and Pensions (DWP), which keeps 60 million personal records in its customer information system, is involved in the pilot.

But the scheme faces legal barriers under the Data Protection Act. It is awaiting the outcome of an assessment from lawyers at Olswang LLP on whether and how the law must be changed to make it possible for people to wrest back some of the control the government has over their personal data.

Tony Ellis, head of IT at Brent Council, said the pilot had scored a world first. "It could be a Google moment," he said. "It's nice having the world's first personal data store. Mydex would say this is the world's first example of residents taking control of their information, but I'm more interested in having a low-level authentication platform."

The pilot involved Brent plugging its data hub into Mydex's beta system and pulling out data relating to two council staff, hub analyst Carol Copeman and records management officer Rita Scollan. Brent will next attempt the operation with up to 50 people's personal data stores.

Ellis hoped the system could become a more trusted source of real-time personal information about Brent residents than its own systems, which could contain conflicting and out of date information.

"One of the challenges for a London borough is just the mobility factor," he said. "People are constantly moving. Our council tax records have a 30% turnover every year. How we keep track of people is one of the challenges and there's cost to that.

"Every council wants to move everything online," he added. "That will involve having some sort of authentication process so we know it really is the person they say they are.

"You can see it getting quite detailed. We can build in increased levels of authentication. We get some information from you. We can also push information back about your services. That could get to where you have input into the services we provide.

"The end game would be a platform that is increasingly electronic. It's almost like an online electronic handshake with a resident. We start to develop an online relationship. And that could take us down some interesting roads," said Ellis. He anticipated this might one day allow residents to tailor their own public services.

According to Ellis, the authentication was cheaper and easier than using the Government Gateway, the official means of online authentication for government services. The Cabinet Office, which runs the current system, is also involved in the Mydex pilot. Other participants include Croydon and Windsor and Maidenhead local authorities, which, like Brent, are among the government's pathfinder councils.

Mydex, which is based on the open source Higgins platform, uses links with credit reference agency Experian to authenticate its users. It plans to establish links with other parties so users can build higher levels of authentication for sensitive transactions.

The start-up hopes people will use its system as a single online identity from which private and public organisations must seek permission to draw personal data. Once authorised links are established, a change in someone's personal circumstances could be communicated instantly to all authorised parties.

But William Heath, CEO of Mydex, said the service was an eventuality unforeseen by the Data Protection Act, which was designed for a world in which people did not have control over their own data. There may therefore be no means of establishing either protection or liability if something goes wrong.

> "Every council wants to move everything online"

"You will need changes to the Data Protection Act for people to have control of their own data," said Heath.

The Conservatives had fought last year's General Election on a manifesto that declared people should have control over their personal data "wherever possible". The matter was not taken up in the Freedom Bill now going through Parliament.

But the DWP has scheduled a legal workshop to determine the implications for public services if they make a mistake delivering someone's benefits based on incorrect data held in someone's personal store. Experts from the London School of Economics are also assessing its privacy implications.

more online

News: Multiple claims-based ID assurance services on the horizon
computerweekly.com/246951.htm

News: Government outlines plans for identity assurance services
computerweekly.com/246723.htm

Analysis: Government plans next-generation ID scheme
computerweekly.com/246856.htm

BRYAN GLICK **LEADER**

New ID policy requires careful management

Here is a story that is going to run and run. As part of its plans to create a national identity assurance scheme for online public services, the government is proposing to establish a market for our personal data, to be used as a means of confirming that we are who we say we are when dealing electronically with government (*see pages 4 and 5*).

The concept is relatively simple – since our personal data is an increasingly valuable currency, why not set up a network of identity banks, in the same way we have a network of money banks?

But even if the concept is simple, the delivery will be anything but.

Technically, it is likely to be feasible. There will be difficulties, of course, but it can be done. The big challenges will be commercial and legal, not to mention the perceptions that might be created by allowing organisations such as banks or the Post Office to act as a repository for our most sensitive identity information.

We have been here before. In 2000, the government worked with industry on a plan to use digital certificates for secure identity assurance online, but that ended in failure two years later.

There is little doubt this will be a controversial move, but it needs to be one new policy the coalition does not backtrack on. Get this right, and the UK has a secure infrastructure for ID-assured online public services. With that in place you can be sure that private sector e-commerce players will want to be in the same game, and this soon becomes a national electronic identity system – one that avoids the Big Brother nature of identity cards and helps to minimise or eliminate identity theft.

Of course, it also risks establishing the perfect target for hackers. Sony's experience with the Playstation Network hack shows the dangers of holding large quantities of sensitive data in one place. But while security is a risk, it should not be a showstopper if it is designed in from the start.

Watch this story – it is going to be big. ■

Editor's blog
computerweekly.com/editor

FABIO CERULLO **OPINION**

How PCI DSS v2.0 affects web app security testing

GOODSHOOT

Since its inception, the objective of Payment Card Industry Data Security Standards (PCI DSS) has been to provide guidelines on how to store, process or transmit credit card data in electronic format. The latest version (PCI DSS v2.0) came into effect on 1 January 2011. If you are a merchant of any size accepting credit cards, you must comply with PCI DSS v2.0 Standards from 2012.

Unfortunately, becoming PCI DSS compliant does not come cheap. Its final cost depends on a number of factors, including your business type, number of transactions processed annually, existing IT infrastructure, and current credit/debit card processing and storage practices. A recent study by Ponemon Institute highlights that merchants which undergo audits to ensure compliance with the PCS DSS are paying an average of $225,000 each year.

What's new in PCI DSS v2.0

So, what are the changes in version 2.0 that every application security tester needs to be aware of? First, you need to identify those applications that need to be compliant with PCI requirement number 6 – Application Security. These are applications with custom code that handle credit card data (internal and external websites) or likewise applications that require maintenance, patches, updates and upgrades.

To be compliant with PCI requirement 6.2, for example, you need to perform a risk-based vulnerability assessment before applying any patches/upgrades. The standard also requires in section 6.5 that measures are taken to eliminate specific known vulnerabilities, including injection flaws, misconfiguration, URL access rights and more. The Open Web Application Security Project (OWASP) compiles and maintains a Top 10 list of Application Security Risks that highlights much of what must be addressed in this requirement.

Finally, according to PCI requirement 6.6, all custom application code has to be reviewed for common vulnerabilities by an organisation that specialises in application security, or organisations must install an application-layer firewall in front of web-facing applications. Although the latter will suffice to meet the requirement, it is not a robust control on its own and it would only be recommended when budget is a constraint. Usually, having the applications undergo a code review is more appropriate and you should only hire reputable experts in the area.

Do not ignore PCI compliance

Ignoring PCI compliance is not an option. Visa fines for non-compliant Level 1 and 2 merchants (more than one million transactions per year) range from $5,000 to $25,000 per month and MasterCard Level 1 and 2 merchants must produce a Report on Compliance from a qualified security assessor (QSA) by 31 December 2011.

The first step for all online merchants and service providers which handle credit card data is to download a copy of the PCI self-assessment questionnaire to see exactly what security measures will be expected. Next, request a free scan from an approved scanning vendor (ASV). That will help you identify where the gaps are in relation to the required PCI Level. If the list of vulnerabilities is too long or you do not have the technical skills within your organisation to address these gaps, you may want to hire a QSA to help you address those vulnerabilities. ■

Fabio Cerullo, CISSP, is the current OWASP Ireland Chapter Leader, OWASP Global Education Committee and OWASP AppSec EU 2011 Chair