Online Fix to Identity Crisis

Electronic identity verification is just around the corner, but are Australian financial institutions ready for the technical challenges it poses?

BY STEPHEN WILSON

The big banks and the Federal Government have reportedly agreed to a plan that will enable the electronic verification of customer identity using the Internet. It is envisaged the Government will use the new anti-money laundering legislation to give financial institutions an alternative to the 100-point in-person ID check.

There is a view in some quarters that since we are generally conducting so much of our working lives online, why should Internet banking continue to be restrained by traditional bricks-and-mortar rules? If we have established an electronic identity, why shouldn't we be allowed to leverage this to create new relationships, including new bank accounts?

In early September, the Justice Minister convened the third in a series of finance industry roundtables on anti-money laundering and counter-terrorist financing (CTF). Co-chaired by the Australian Bankers' Association, the latest meeting was to progress agreement on detailed principles for our new AML legislation, guided by the international Financial Action Task Force on Money Laundering (FATF). A key issue is customer due diligence (CDD) in online banking.

Apparently there has only been a minority dissenting voice at the AML/CTF roundtable thus far. Overwhelmingly – and predictably – support for online ID proofing has come from offshore institutions, keen to keep costs down when building their Australian customer bases. And US institutions in particular are more familiar than we are with independent information brokers which help confirm American customers' identities through special access to government databases.

A joint communiqué from the roundtable said that "AML/CTF legislation will set robust standards for CDD [customer due diligence] which are technology neutral with further discussion on the content of standards. It was recognised that alternative methods would need to provide the same confidence in the verification process as face-to-face procedures."

But in Australia, "technology neutral" is too often code for "hands off". When it comes to the Internet, our regulatory regime rarely imposes technology standards. In general, the light touch approach is laudable, but on occasion it can mean uncertainty and a laissez faire approach to security.

Key points

- **Banks relying on purely electronic proof of identity will need to know the data isn't stolen**
- **Customers planning to submit identity data to institutions online will need to know the websites are not fake**
- **Strong mutual authentication is the key to fully electronic verification**

If fully electronic verification is truly to retain the same confidence as face-to-face procedures, then our choice of authentication technologies may turn out to be very limited.

Electronic verification of identity documents happens to be a major government project, regardless of the AML reforms or some banks' business interests in streamlining account opening procedures. Increasingly, federal and state authorities are keen to see better cross-checking of personal details like passport, vehicle registration and driver licence numbers, to help stamp out identity fraud. To date, explicit regulatory restrictions – as well as bureaucratic red tape – have stymied the verification of data between agencies, and between agencies and business. Now, well funded initiatives involving the Department of Foreign Affairs and Trade and other agencies are removing these barriers and seeking to automate cross-checking.

But how far should we take electronic verification? Many security analysts look forward to it becoming available as a tool to assist regular face-to-face identification. High quality fake identity documents are widely available through criminal gangs; police report that whole portfolios of primary and secondary documents – including counterfeit utilities bills – may be bought on the street for a few hundred dollars. The challenge for bank staff to be able to spot these fakes is becoming hard to bear.

So how can we perform the entire identity proofing procedure online?

A bank trying to perform electronic identity verification is faced with nothing more than a collection of data – ones and zeroes. Proving that the data corresponds to real identity documents is just the beginning. How can the bank be sure that the data stream hasn't been stolen and is simply being replayed down the line? Institutions will need an authentication mechanism that provides confidence that identity data is coming direct from a trusted source.

Now put yourself in the position of the customer trying to open a bank account purely online. They will be asked to send a collection of prized identity data across the ether to a website. How can they be sure it's a genuine site and not a ghost? How do they know there isn't a "man in the middle" eavesdropping on the data stream and stealing their identity?

These problems are not insurmountable. In any case, institutions know they have to combat the man-in-the-middle attack to retain customer confidence, regardless of any future moves implied by AML reforms. The business requirement is to provide online customers with the means for mutual authentication, so that they can verify the identity of a bank server, before the bank server identifies them.

There are not many technologies that support mutual authentication. The smartcard is one, and for this reason, smartcards are favoured by the US Government for all remote authentication of federal employees.

So in my view, only once mutual authentication is widespread should institutions contemplate pure electronic verification of new customers. It will be interesting to watch how our regulators' technology-neutral approach fares with the reality that there are so few technologies that can fit the bill.

Stephen Wilson is a leading international authority on identity management and information security. In early 2004, Stephen established Lockstep Consulting to provide independent security advice and to develop new smartcard solutions to identity theft.

swilson@lockstep.com.au