

Facilitating Online Transactions With Digital Identities

Joe Tavella, ANZ - 19 Feb 2008

The emergence of digital identity solutions suggests that banks can further leverage their position as trusted organisations to secure and facilitate transactions other than traditional bank-to-corporate transactions.

As a financial decision maker, how many IDs and passwords and security devices do you have with each of your financial services providers? Could you have fewer? How secure are these? And what are the latest developments to ensure there are global standards, allowing you not only to transact securely with your bank but other corporates?

In the corporate-to-bank environment, Know Your Customer (KYC) is essential. In Australia, legislation such as the Anti-Money Laundering Regulations, Sarbanes-Oxley and the Financial Transactions Reforms Act reinforce the importance of KYC. With the rise of man-in-the-middle attacks, providing assurance that electronic transactions are secure, it is becoming an increasingly difficult and expensive challenge for banks.

Identity and access management comprises four key elements to provide trust and assurance:

1. Identify the individual through traditional methods such as evidence of identity checks.
2. Identify what organisation or group of organisations the individual is authorised to represent.
3. Identify what online banking applications the individual is authorised to access.
4. Authenticate the individual through a digital identity. The digital identity is then used by the individual as electronic proof of identity for Internet-based transactions.

Combining these four elements provides corporates with single sign-on capability across all online banking applications offered by their bank. The form of digital identity can vary based on the value and risk associated with the transactions. For example, low risk transactions such as viewing bank account balances might only require traditional username and password whereas higher risk transactions, such as payments might require two-factor security devices, i.e. one-time password tokens or digital signatures stored on chip card and PIN technology. Either way, single sign on will provide corporates with a single solution for all their identity management needs, eliminating the need for treasurers to remember multiple passwords or have in their possession multiple security devices.

The Intricacies of Digital Signatures

Embedding digital identities, particularly digital signatures, with product and service solutions is becoming increasingly important to transaction banks worldwide. Digital signatures are based on public key infrastructure (PKI) and provide organisations with the ability to digitally sign transaction instructions at the user-level. They are the single most secure form of transacting currently available and cannot be hacked (which other forms of security can) as they require users to be in physical possession of a PKI card as well as a password.

By combining all elements of PKI, digital signatures are legally binding in more than 200 countries globally and can replace hand-written signatures. For example, the Electronic Transaction Act in Australia gives legal recognition to the use of digital signatures and similar legislation exists worldwide. Furthermore, digital signatures stored on two-factor security devices such as chip and PIN technology enforces non-repudiation.

Eliminating Paper Trails While Maintaining Security

Replacing a hand-written signature with a personalised digital signature issued by a bank, gives rise to the concept of dematerialising paper-based processes. Today, corporates are increasingly

frustrated by the paper-based, labour-intensive processes that exist for simple bank instructions such as opening an account or applying for new products and services with each of their banking relationships. Embedding digital signatures within bank-to-corporate solutions improves customer service and satisfaction but also facilitates straight through processing by validating the identity of the initiator in real-time thereby reducing cost, time and risk. However, the benefits associated with digital signatures do not stop at bank-to-corporate transactions.

The Importance of Digital Identity in Trade Relationships

Banks play an important role when it comes to validating the identity of parties to transactions. It is the core business of banks to provide trust between parties that have not previously traded with each other. Banks are trusted intermediaries in the trade process whether the process is paper-based or electronic. The extension of bank issued digital signatures in the trade process enables trade documents such as purchase orders, invoices and bills of exchange to be validated for authenticity thereby avoiding manual processing and creating an end-to-end solution with a single digital identity.

In Australia, the Electronic Bills of Exchange Act recognises that a legally binding, non-repudiable signature is required to show authenticity of a bill of exchange document and that it is also attributable to one source. Under the Value Added Tax Directive in Europe, each party to a transaction is now able to use electronic invoicing on condition that the authenticity of the origin and integrity of the content of the invoice are guaranteed. A digital signature allows someone receiving data over open networks to determine the origin of the data and to check that the data has not been altered. Providing the party to a transaction meets this requirement, they have the right to obtain a deduction or refund in respect of VAT on the costs of the goods or services supplied.

The benefits associated with digital signatures can therefore be extended to compliance as well as other identified benefits such as increased trust, reduced operating costs and greater operational effectiveness by reducing the paper burden for corporates.

Conclusion

Corporates will often have multiple banking relationships and will require a security device for each banking relationship resulting in treasurers having drawers full of security devices. Furthermore, globalisation and cross-border trade is making the need for banks to facilitate business-to-business transactions essential. Over the next few years, digital signatures will be embedded in new product and service solutions resulting in corporates only requiring a single digital signature across all business transactions.

Banks need to agree on a global, interoperable identity solution to ensure the benefits associated with digital identities become reality. Corporates are becoming increasingly aware of the benefits of standardisation and are rejecting proprietary solutions offered by their bank. Through a common identity solution, banks will be required to compete on relationship and service rather than access platforms, providing significant choice and mobility to benefit corporates.