

Doing business in an electronic world: The role of digital identity

By Gary E. Greenwald, managing director, head of information products, Citigroup corporate and investment banking, and Hilary L. Ward, director, identity business manager, Citigroup corporate and investment banking

A glimpse of the future

Consider this scenario: An assistant treasurer of a multi-national firm in Asia, who is an authorized signer on 100 DDA accounts across ten banks, moves to a new job at corporate headquarters. His role, as an authorized signatory, needs to be transitioned to his successor. This changeover involves contacting each bank, obtaining the appropriate forms, appending resolutions and sending the completed forms back to all the banks.

Now, consider an alternate scenario whereby a user logs on to a bank account management system where all the firm's bank accounts can be viewed. The user filters the accounts replacing the old signatory with the new one, and then uses a digital identity card to approve the transfer and provide the banks with the required authorized signature. The requested updates flow through the banking system and an acknowledgement is generated that the changes have been made.

Citigroup, along with several major corporations, the TWIST standards consortium, and IdenTrust – a bank-sponsored digital identity organization – recently collaborated to pilot this exact solution. Interestingly, the challenge was not in developing the web tool allowing the user to substitute one signatory for another, but rather ensuring that the online transaction was binding. It turns out that clicking 'OK' on a computer screen was not quite the same as a 'wet' signature.



To further illustrate this point, let's take a similar scenario in the pharmaceutical industry.

Digital identities in the pharmaceutical industry

A leading pharmaceutical company found itself faced with a major challenge. The company was drowning in paper generated by clinical research trials needed for US Food and Drug Administration approval of new medicines. These trials are typically long and complex, involving large numbers of physicians, universities and independent researchers. The FDA historically has required the results of these research trials be submitted along with documents signed by the relevant research team resulting in massive amounts of paper for each drug trial.

In an effort to reduce the paper burden, the FDA began allowing electronic submissions provided the documents were signed using legally binding digital signatures. The FDA defined detailed standards that must be followed before any researcher could be issued a digital identity card to sign documents to ensure these are what are known as high assurance identities. Some of the standards were technical, but many focused on the process by which the digital identities are issued. How do you verify an individual's identity before issuing an ID card? What is the liability framework for misuse of these identities? How do you ensure compliance with varying international digital signature regulations?

It turns out that many aspects of identity management are core competencies of banks. Banks are regulated institutions that for hundreds of years have specialized in managing risk and serving as trusted third parties. Recognizing this, this pharmaceutical company partnered with Citigroup to create and implement a solution to their 'paper' challenge. As a result, a growing number of researchers have been issued Citigroup-backed digital identity smart cards, and a set of their processes and IT applications have been reengineered to use these identities.

Digital Identities in Corporate Banking Processes

These examples are just the beginning as digital identities can be used in a variety of ways. A bank-issued digital identity can be viewed as a universal identity card with numerous applications.



It can provide login access to corporate end-users using digital certificates to identify themselves for access to a web application. It can be used for encryption purposes to lock down data and provide a trusted mechanism for information sharing.

For example, in the corporate payments arena, Citigroup, Danone, BNP, and IdenTrust recently conducted a proof-of-concept using double digital signatures for payments via the *SWIFTNet FileAct service using the IdenTrust platform as a second signature in addition to the SWIFT PKI security. The pilot was the first step in a global project designed to implement corporate payments by using personally signed files - payment or other - using a binding, interoperable identity deployment based on the IdenTrust platform.

The pilot involved Danone, a world leader in the food industry based in France, sending SWIFTNet payment instructions signed with a globally interoperable and non-repudiable IdenTrust personal digital signature. An authorized employee at Danone signed a payment file and sent it via SWIFTNet FileAct to Citigroup. Further, to demonstrate global bank interoperability, a second payment was sent via BNP Paribas, who was able to validate and rely on the Citigroup-issued digital identity. This demonstrates how globally interoperable digital signatures can be used across banks, and underscores the important role that banks are playing in helping their corporate clients meet their compliance needs relating to high value transactions.

Beyond payments, from a corporate treasury perspective, eliminating paper-based signatures in the banking process would significantly reduce the time to open and maintain bank accounts, providing greater visibility and control over key processes, and allowing for enhanced auditing procedures to meet regulatory requirements.

For its part, Citigroup plays the role of a trusted third party verifying 'who,' 'did what' and 'when' in electronic interactions. The value-add to clients is bank grade process controls around issuance and

KYC, banking system acceptance, liability for misuse, and legal enforceability.

Citigroup's membership in identity schemes like IdenTrust and SAFE is similar to today's credit card model. A Citigroup-issued identity allows interoperability with participants - such as other banks - who have agreed to the terms and conditions of the operating model, and who can rely on certificates from other participants.

Why banks? Why Citigroup?

Citigroup's work in the market highlights that Identity is the lynchpin in electronic workflows. Digital identities enable firms to know who is on the other end of the transaction, create binding transactions, and ensure the integrity of those transactions to satisfy regulatory and audit requirements. Banks, for their part, are uniquely positioned to address these issues since introducing parties and establishing trust in B-to-B transactions is a traditional role that banks have always played.

* SWIFT, S.W.I.F.T., and SWIFT-derived product and service names are trademarks of S.W.I.F.T. SCRL.



To learn more about Citigroup capabilities and services, visit us on the web at:

www.transactionservices.citigroup.com