IdenTrust™

Accountability – The Key to Expanding Global Commerce

White Paper

TABLE OF CONTENTS

INTRODUCTION

A lack of integration between the physical and financial supply chains still exists even as we approach the end of 2008. While large enterprises have made great strides in automating the physical supply chain by implementing technology such as enterprise resource planning (ERP) systems, automation is financially out of reach for most small and medium enterprises (SMEs) and they continue to rely on paper for many mainstream workflows.

For both large enterprises and SMEs, the financial "oil" that connects various supply chain participants remains a largely disconnected process of supply chain function, payments and finance. Participants continue to print and fax or email documents stored on personal computers. Signers still authenticate documents mainly with "wet signatures." Magnetic tapes and diskettes still deliver bulk payment files to financial institutions.

Global standards are critical in automating and integrating the physical and financial supply chains, reducing cost, time and risk and achieving straight through processing (STP). These standards make automation affordable for even the smallest participants by reducing ongoing expenditures and allowing them to enter markets. Large companies suffer as well as they cannot increase market penetration into developing markets by automating processes to make them accessible to the local participants.

Standards Address Infrastructure Issues

Domestic and international standards that enable many markets to function more smoothly already exist. For example, SWIFT expanded the capabilities of their financial messaging standards during the 1990s because existing standards were too restrictive and could not fully support the global movement to STP. Championing the rewards of reduced cost, processing time and risk, SWIFT was a catalyst for revising standards. Its work with other organizations resulted in ISO20022.

Today, three major organizations facilitate payments to locations and participants around the globe: Visa, MasterCard and SWIFT. Financial institutions around the world have defined and agreed to policies, a legal infrastructure and operating rules that facilitate cross-border payments. Rather than rely on each country's national payment system schemes and standards for automating domestic payment transfers between financial institutions, countries are increasingly opting for a global standard. Many choose SWIFT, taking advantage of global lessons learned, reducing costs and time to market, and, more importantly, eliminating the need to develop and maintain a unique infrastructure.

Like payment standards, standards governing identity are critical. And as with payments standards, identity standards must be globally interoperable, work consistently in all markets, be legally enforceable, and able to support STP across industries in order to replace "wet signatures" and in-person identity authentication validation with electronic identity authentication.

Lastly, identity authentication must provide authentication at the individual rather than just corporate level.

"[The successful completion a double digital signature proof of concept using the IdenTrust platform] underscores the important role that banks are playing in helping their corporate clients meet their compliance needs relating to high value transactions."

— Gary E. Greenwald
Global Head of Information Products, Global Transaction Services, Citigroup Corporate and Investment Banking

Integrating Physical and Financial Supply Chains with Standards

Organizations such as TWIST and CAST are creating corporate standards that map to the financial supply chain delivered through financial institutions. Using the published standards for financial messaging and identity will enable corporations to streamline their interactions with financial institutions.

The ISO20022 standard also aims to create a consistent cross-industry approach for financial messaging. IdenTrust, along with several banks and global corporations, continues to expand early bank mandates to develop standard bank interactions with eBAM (electronic bank account management). The eBAM initiative will provide an interoperable standard for authenticating and validating the user identities for transactions related to account opening/closing, delegation of authority, and signatory change. Corporations will no longer have to maintain multiple tokens, passwords and process for authentication with each of their banks which will provide a huge administrative time, cost and risk reduction.

Identity and physical supply chain integration standards will enable corporations to streamline the end-to-end procurement process, including shipping and customs. An electronic version of bills of lading, warehouse documents and customer forms that contain globally interoperable, legally binding digital certificates and signatures from each point in the workflow will take cost and time out of the supply chain and eliminate the risk of receiving counterfeit or fraudulent goods.

The Case for Double Signing

Commerce around the world is supported by global payments standards. Most originating payments systems require appropriate authentication and authorization validation before approving and releasing individual, high-value payments. However, most of these systems only verify access rather than identity of the person using the credentials which does not fully protect against identity fraud. Companies need to ensure that the identity of the person accessing the system was authenticated before the digital certificate was issued and validate that it is still authenticated each time it's used. Without individual identity authentication, companies cannot trust that the person accessing the system is actually the party who should have the access credentials.

Without individual identity authentication there is no individual accountability.

To provide individual accountability, identity authentication must be integrated into key parts of the workflow. Identity should be authenticated before anyone receives a single sign on or is provisioned for rights to or within a system. Once provisioned, that identity should be tied to each action taken to provide end-to-end accountability.

In many corporations, employees can provide transaction history, sufficient organizational transparency, tracking of financial transfers and supporting documentation when processing runs smoothly. However, when providing historical data for exception processing and changing regulations, these same corporations stumble. Proving compliance during an audit can be challenging and accountability limitations increase financial risk to both the corporations and the banks serving them.

Corporations can miss behavior and activity patterns that could identify potential fraud by not tying individuals to the work that they do and the transactions that they generate, Tracking and accountability per individual must be enterprise-wide and comprehensive.

"Utilizing digital signatures in payment instructions gives our clients in a straight-through processing environment the visibility and control over transactions that they have come to expect in traditional web banking."

— Gary E. Greenwald
Global Head of Information Products, Global Transaction Services, Citigroup Corporate and Investment Banking

IdenTrust: Individual Accountability

Today, accountability for bulk files of payments (more than one) is only available at the corporate level. The IdenTrust value proposition enables these bulk files to utilize a unique, internationally interoperable capability that provides accountability by identifying each signature at an individual rather than company-level. IdenTrust's open standards-based, proprietary process for identity authentication and validation, the Rule Set, was developed by, and for, the global financial services community and its customers. The Rule Set provides a binding legal and regulatory framework that creates an interoperable identification and authentication process for all transactions and documents.

The IdenTrust Rule Set automates three key activities:

Authenticate – Prove the identity of individuals or businesses.

- IdenTrust identities allow individuals or businesses to prove that they are who they say they are, and conversely, allow individuals or businesses to rely on that proof.
- Because IdenTrust identities are backed by banks around the world, individuals or businesses that rely on that identity are covered by a liability structure provided by the banks (similar to the structure provided in the credit card industry) even if the identity is proven false.

Encrypt – Control visibility into and integrity of transactions or documents.

- IdenTrust identities lock the contents of a transaction file and/or document, making them impossible to tamper with.
- IdenTrust identities can also scramble information, making it impossible to read or decipher by an unauthorized person.
- IdenTrust identities also encrypt and control process flows, eliminating both phishing and man-in-the-middle attacks by ensuring that no one can intercept or redirect the transaction or document.

Digitally Sign – Create a legally binding and non-repudiable electronic signature.

- IdenTrust identities can be used to replace "wet" signatures so electronic documents and transactions have the same levels of legal protection and enforceability associated with traditional ink-based paper signatures.
- Global legal interoperability results from a closed contractual system that governs:
  - Liability and recourse among all parties (a certificate authority (CA) confirms to the relying party (RP) that the subscriber's certificate is not revoked – reducing repudiation risk)
  - Legal recognition of digital signatures
  - Electronic contract formation
  - Dispute resolution over signature validity

Using these three functions alone or in combination, corporations can hold individuals within their organization accountable for creating, transferring, reading or discarding transactions--from signing contracts to initiating payments to handling complex supply chain transactions. This entire process is fully compliant with U.S. regulatory requirements such as Sarbanes Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Financial Institutions Examination Council (FFIEC) multifactor authentication banking guidelines and global initiatives such as anti-money laundering (AML), the Single European Payments Area (SEPA) identity authentication guidelines and Know Your Customer (KYC) requirements around the world.

"To truly authenticate the identity of originators and receivers of high-value electronic transactions, financial institutions require a consistent set of policies that are legally binding and globally interoperable for authenticating and validating identities."

— Karen J. Wendel
Chief Executive Officer,
IdenTrust

IdenTrust PLOT Uniquely Identifies Individual Originators/Receivers of All Types of Files

- Only the total combination of the PLOT components--Policy, Legal Frame work, Operations and Technology--provides a comprehensive approach to identifying the originator and receiver of payment and other types of electronically transferred files.
- Policies and procedures developed and agreed to by financial institutions around the world provide a comprehensive approach to authenticating and issuing these identities.
- IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Other systems require public law for digital signatures to be effective.
- All transaction details remain private; only certificate information is validated.
- Customer agreements are valid, binding and enforceable in countries around the world.
- IdenTrust delivers a complete hosted environment to enable a full spectrum of trusted identity services.
- A single, interoperable identity accepted by multiple financial institutions across multiple applications supports more than just simple file transfer.
- The financial institutions which formed IdenTrust cooperatively defined and developed a standard for authenticating identities that uses the "Know Your Customer" regulations in use in most countries and ensure global enforceability since the digital identity certificate contracts are legally binding throughout the world.

The IdenTrust PLOT

Although technology issues typically receive the most attention in the identity industry, in reality they represent just the tip of a very large iceberg. The most pressing identity dangers exist in the policy, legal and operations areas. The IdenTrust Rule Set is unique because it focuses on all aspects of identity rather than only on the technology.

The IdenTrust Rule Set

The IdenTrust Rule Set governs:

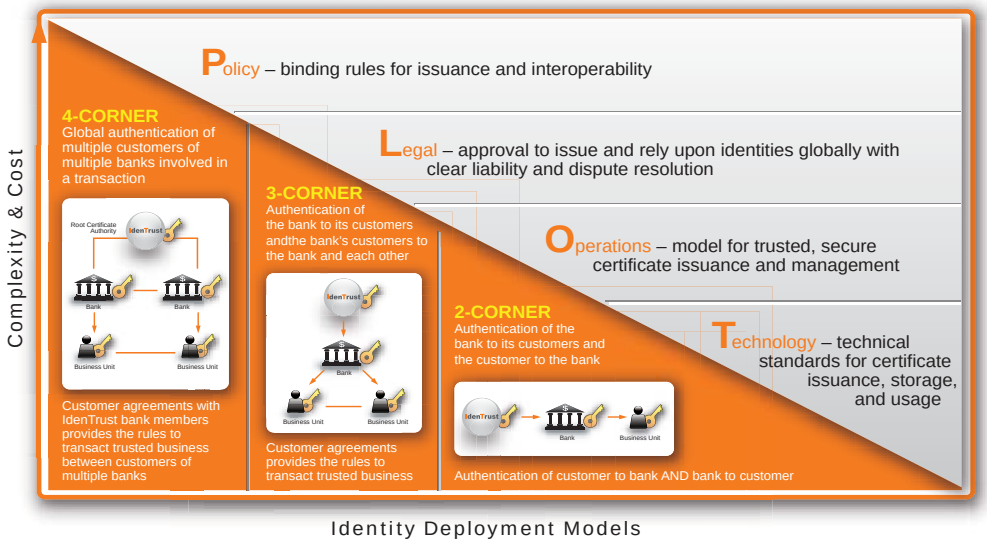
Policy issues such as who receives the identity and how each individual or business is vetted to guarantee they really are who they say they are and ensuring that the process is done consistently everywhere around the world.

Legal issues such as what should be done when something goes wrong, setting base liability structures and guaranteeing that each identity meets the legal requirements of every jurisdiction.

Operations issues such as how identities are manufactured to ensure that the entire process is secure. This includes physical security (identities are distributed and turned out using at least two different channels such as mail and email or mail and phone) and ensuring that the network is always available.

Technology issues such as the workings of the identities and the overall network. IdenTrust uses standard technology in a unique, proprietary manner to ensure even higher levels of security.

This combination of policy, legal, operations and technology (PLOT) supports more than 40 million transactions annually. These volumes are increasing 15% each month and include financial transactions such as payments as well as business transactions such as invoice flows.



PLOT works in three identity deployment models: a 2-Corner Model in which a corporation interacts only with their own bank; a 3-Corner Model in which a corporation interacts both through their own bank and another customer of that bank; or a 4-Corner Model in which a corporation interacts with multiple banks that are members of the IdenTrust community.

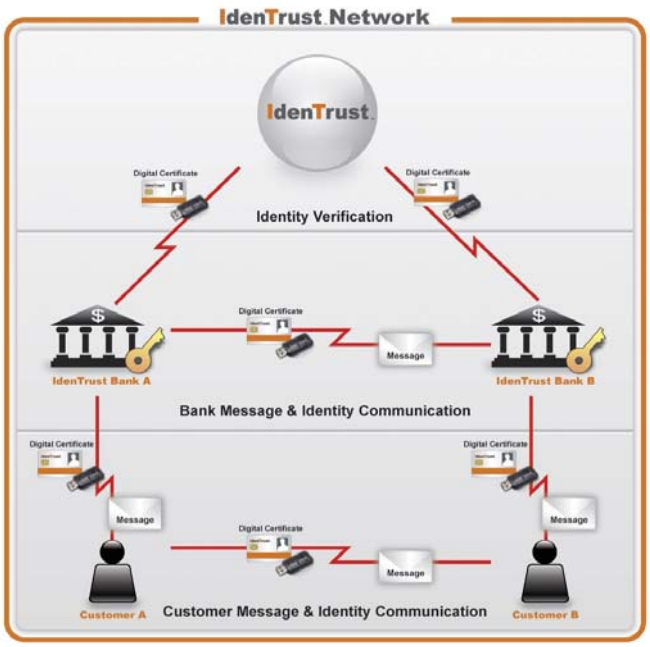
Combining Security and Privacy

Many organizations around the world use digital certificates and access tokens/software that provide high levels of authentication and validation. However, these organizations store the digital certificates and access tokens/software as part of the transaction data. As transactions are opened to perform authentication and verification, privacy is compromised.

IdenTrust does not violate the privacy of the sender or the receiver.

The IdenTrust Rule Set governs the operation of the IdenTrust Trust Network by specifying how a digital identity certificate can be issued and how it is validated. Inherent within the IdenTrust infrastructure and Rule Set is protection against unauthorized access to the transaction information: the IdenTrust infrastructure validates the certificates and only authorized users can interrogate the transaction data.

The transaction data and signed certificate are exchanged between the banks involved in the transaction. The messages related to the transaction data are exchanged between the bank customers on either end of the transaction. IdenTrust only validates the identities used by these customers, not the data associated with the transaction. The transaction data itself is never passed to IdenTrust. It remains with the banks involved.



Summary

A single, unique, globally interoperable identifier is a critical component of a comprehensive approach to identity management. It eliminates the need for corporations to maintain multiple authentication methods for communications with their financial institutions. It also expedites the processing flow and reduces risk since there is only one identifier to authenticate identity rather than just access. Using a standardized approach to identity authentication is another step toward expanding Straight Through Processing (STP).

IdenTrust enables individual identity signing of payment or other types of files transferred over public and private networks such as SWIFT and regional ACH networks such as NACHA, Isabel and Voca. This facilitates authentication of the individual identities of originators and receivers of these files. This increased level of accountability enables better regulatory reporting and comprehensive audit tracking across the entire transaction flow from initiation through completion. IdenTrust expands the transparency needed for payments processing.

Authenticating and validating each individual provides bulk file transfers with an additional level of tracking and control, improving risk controls and regulatory compliance for corporations worldwide. IdenTrust helps financial institutions and their customers expand trust to all types of payments and other communications over the Internet while still maintaining privacy. This prevents identity and other types of fraud, makes compliance easier and strengthens authentication which reduces the need for further regulation.

ABOUT IDENTRUST

IdenTrust is the global leader in trusted identity solutions, recognized by global financial institutions, government agencies and departments, and commercial organizations around the world. IdenTrust enables organizations to effectively manage the risks associated with identity authentication; work interoperably with countries around the world; minimize investment in creating their own policies and legal frameworks; and deploy a spectrum of products insuring trust, smarter, faster, and more cost effectively.

The only bank-developed identity authentication system, IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is predicated on a proprietary framework that combines policies, legal framework, trusted operations and technology (PLOT) to create a comprehensive environment for issuing trusted identities. IdenTrust is the only company to provide a solution incorporating all four of these elements. Customer agreements are valid, binding and enforceable in more than 175 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, require participants to navigate a confusing maze of public laws that vary from jurisdiction to jurisdiction. Additionally, the IdenTrust Trust Infrastructure maintains the privacy of each and every transaction processed by reading only digital certificate information, not the message itself.

Additional information can be found at www.IdenTrust.com.

Corporate Headquarters
IdenTrust Inc.
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
USA
Telephone: +1.866.IDENTRUST (+1.866.433.6878)
Fax: +1.415.486.2901
www.IdenTrust.com

European Office
IdenTrust Inc.
288 Bishopsgate
London, EC2M 4QP
United Kingdom
Telephone: +44 (0)203.008.8330
Fax: +44 (0)203.008.8331