



Cross-Border Regulatory Interoperability: Connecting the Tracks to Facilitate Communication & Commerce

White Paper
October 2006



Introduction

Regulations - and compliance with those regulations - form the foundations of society. Without laws to govern its infrastructure, societies would be unable to maintain order.

The Constitutional documents that govern countries around the world establish the basic policies and guidelines under which governments function. To be successful, those rules have to apply consistently across regional and state boundaries. A country's infrastructure has to be interoperable to be effective. For example, train tracks need to be the same size state to state or country to country for trains to effectively transport goods. A national currency enables commerce to easily occur across regional boundaries. Common electrical voltage and phone connections encourage manufacturers to produce a higher volume of products at a lower cost. As national stock exchange for equities with specialists for particular commodities or derivatives and a single national depository for these records facilitates trading.

Standards and consistency reduce time and costs; lower risk; and improve user and customer satisfaction.

The Challenge of Inconsistency

The mass acceptance of the Internet is driving the need for regulatory interoperability on a global basis. More and more companies are communicating with customers, suppliers, partners, and others located beyond their borders. However, the lack of global interoperability impedes continued growth.

"Interoperability is an important element that enables commerce," says Daniel Schutzer, then Board Chairman of the Financial Services Technology Consortium and Vice President and Director of External Standards and Advanced Technology, e-Citi, Citigroup. "Interoperability opens up markets to the greatest number of firms, lowers the barriers of entry and fosters competition and innovation. It gives customers a great choice and the service providers a much larger potential marketplace."

The regulations needed to move goods cross-border--identifying and authenticating the buyer and seller and facilitating the financing and payment regardless of where the business is being transacted--can take 90 days or more, rely heavily on paper, and, typically result in a larger number of errors. These challenges combined the language differences, measurement translation (metric vs. universal), and customs import and export regulations make the costs of cross-border selling impossibly high for most small and medium-sized enterprises.

Europe, within the Euro zone, is already addressing these challenges on two fronts: the Single Euro Payments Area (SEPA) to normalize payments and payment types and the Markets in Financial Instruments Directive (MiFID) which will have similar effect on capital markets participants investing in Euro-denominated transactions. These two directives will expedite processing and reduce overall costs.

Similar efforts are also underway in the supply chain, but the approaches are not consistent and thus producing mixed results. There are dozens of standards for e-invoices. Digital certificate rules and standards for identity authentication vary by country. Thus, just as with other non-interoperable standards, companies are cropping up to provide integration, adding layers to the infrastructure that drives up cost and complexity.

Interoperability is an important element that enables commerce.

— Daniel Schutzer
Vice President and Director
External Standards and
Advanced Technology

A viable framework for electronic commerce requires the elimination of paper-based barriers such as “writings” and “originals” and the introduction of electronic means to enter into legally binding contracts.

— Andrew J. Pincus
former general counsel
U.S. Department of Commerce

Legal Issues

Liability and legal recourse are also inconsistent when doing business cross-border. Every country has its own regulatory and legal framework and companies doing business in multiple countries must navigate the legal environment for each individual country.

Andrew J. Pincus, former general counsel to the U.S. Department of Commerce writes, “A viable framework for electronic commerce requires the elimination of paper-based barriers such as “writings” and “originals” and the introduction of electronic means to enter into legally binding contracts.”

In *Economic Perspectives*, a publication from the U.S. Department of State, Dr. Carlos Moreno, Legal Officer with UNCTAD (United Nations Conference on Trade and Development) writes, “The extent to which national and international law accepts that an electronic message can perform the same function as a paper document differs considerably. Most of the international conventions and national laws that were adopted more than twenty years ago as a general rule did not anticipate the possible use of electronic means of communication. This is largely because such means of communication did not exist when these international conventions and national laws were drafted and the necessary modifications to them have yet to be made.”

“Furthermore, many national laws also introduce uncertainty regarding the legal validity of electronic based transactions or are inconsistent in their treatment of new technologies. Also, few Courts have had the opportunity to rule on the validity of electronic documents, messages and signatures.”

Operational Headaches

In addition to regulatory and legal incompatibilities and potentially conflicting compliance requirements, there are cross-border operational differences. Varying definitions and degrees of security and access authentication make users vulnerable to fraud. Differences between the public and private sector approaches to authentication enable smart hackers to exploit those discrepancies. Recourse for victims and laws for prosecution differ by country.

These inconsistencies act as a deterrent to expansion of global e-commerce and communication. Small- and medium-sized enterprises wanting to participate in global commerce but without the wherewithal to withstand potential losses from fraud choose not to participate or to participate with only partial automation. To lower their risk, purchasers focus on known suppliers rather than searching for those that can provide the best deal or the most innovative product.

Re-usability suffers when standards can only be shared with other countries using the same language or accepting of another country’s national approach. Inconsistencies between national standards create opportunities for fraud and thus increase risk

Regulatory Interoperability on a Global Basis

To truly expand global communication and commerce, participants must feel confident that an infrastructure is in place to protect them from fraud. Cross-border cooperation and interoperability are critical to creating trust.

Three excellent examples of trusted environments operating interoperably across borders today are SWIFT, Visa and MasterCard. All three are bank-backed and provide assured authentication to users. Participants in these three environments have agreed

to limit participant liability and to honor transactions created by companies beyond their borders by relying on the authentication performed by other members. Customers of many different financial institutions worldwide can make purchases conveniently and securely.

- From www.SWIFT.com: Industry associations and central banks have developed market infrastructures for clearing and settlement. Because they are multilateral, they need a trusted third party to provide secure, reliable and proven messaging solutions. SWIFT is increasingly used by financial institutions to fill that role.
- From www.Visa.com: The Visa USA Operating Regulations are rules that govern the use of the Visa payment system by Visa members only and do not supersede any contractual agreement between a merchant and its acquiring financial institution
- From www.MasterCard.com: There are over 23 million locations where cardholders can use their MasterCard cards. As you might imagine, a network this large must operate under specific rules and regulations. MasterCard Worldwide requires our members - banks and other financial institutions that issue cards and acquire transactions - to comply with MasterCard rules. Those members, in turn, must ensure that merchants they acquire for also comply with MasterCard rules.

What makes each of these three schemes successful is the cross-border interoperability of their policies, rules, and legal framework. Working with the regulators and lawyers in each country where these companies operate greatly reduces risk for the participating financial institutions. Global interoperability also reduces costs and processing times and provides consumers in countries around the world with access to a truly global marketplace.

The IdenTrust Difference

IdenTrust, similar to SWIFT, Visa and MasterCard, was developed by a consortium of financial institutions from around the world to deliver trusted electronic commerce. Working together, these institutions agreed on rules for authenticating identities to create an infrastructure all member banks can rely on regardless of which institution performed the authentication.

Today, IdenTrust digital certificates and signatures are accepted in over 90 countries. This number will continue to grow as more global banks are added to the membership.

As with customer relationship and risk management, identity management requires consistent vetting, storing, validating the use of and relying on the trustworthiness of the identity. Multiple unique approaches by individual only cause confusion and enable fraudsters to exploit the differences. An enterprise approach to identity management also makes it easier for customers to adopt and adapt to using digital certificates and signatures.

IdenTrust has created identity authentication best practices that govern identity vetting and ensure that identities will be consistently handled across all of the participants in a transaction. The resulting IdenTrust rule set governs the vetting performed prior to issuance of a certificate. Expanding this consortium to include global participants insured that identities are globally interoperable under uniform private contracts recognized around the world. Unlike most systems which require public law for digital signatures to be effective, IdenTrust rules also govern customer agreements and insure that they are valid, binding and enforceable in countries where the participants do business.

To simplify adoption and ensure trusted identity authentication, IdenTrust conducts a secure operation that is auditable with the same stringency applied to financial institutions. End-to-end tracking of activity, required for regulatory reporting in jurisdictions around the world, is a key part of the IdenTrust value proposition.

Also, the IdenTrust operational environment is easy to integrate with other trust-related products and services to enable financial institutions to extend their spectrum of compliance more rapidly. Platform flexibility is also critical in integrating certificate technology (e.g. USB, smart card, roaming certificate, and encrypted USB drive).

Conclusion

Technology continues to change the way we communicate and do business globally and regulations need to be globally interoperable to enable this evolution. Examples of current efforts to create global interoperability include Voice over Internet Protocol (VOIP) which must be globally interoperable and consistently secure cyberspace to support the needs of business and enable participants to rely upon authentication anywhere in the world.

Creating identity management best practices requires a comprehensive approach. Addressing technology alone, or just technology and operations, provides only a piece of the solution. Without a legal framework that includes interoperable contracts, agreed-upon policies and procedures for issuing and revoking certificates, and agreements on the liability involved, financial institutions do not have a totally trusted environment. And trust taken for granted has ruined reputations and taken down venerable financial services-related institutions and providers.

Identity assurance is one area where making the appropriate decisions initially saves both reputations and expense later.

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 (P.L.O.T.) 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 90 countries. IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Competing offerings, in contrast, rely on a dizzying 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.
795 Folsom Street, 1st Floor
San Francisco, CA 94107
USA
Telephone: +1.866.IDENTRUST (+1.866.433.6878)
Fax: +1.415.848.2745

International Office

117 Fenchurch Street
London, EC3M 5DY
United Kingdom
Telephone: +44 (0)20 3008.8330
Fax: +44 (0)20 3008.8331