

Identity Authentication:
Increasing Confidence in
Peer-to-Peer Networks



All You Need is One.
Enabling an eco-friendly digital world.

TABLE OF CONTENTS

Introduction	3
Interoperability on a Global Basis	3
The IdenTrust Difference	4
Identity Management Requirements	4
Financial Institutions as Trusted Intermediaries	5
Combining Security and Privacy	5
Summary	6
About IdenTrust	7

INTRODUCTION

Peer-to-peer networks facilitate development of new marketplaces by creating an environment in which people bypass traditional middlemen such as financial institutions and transact business directly with each other. Peer-to-peer networks have ushered in a new way of connecting with others and expanding commerce opportunities.

The peer-to-peer phenomenon began with online auctions such as eBay; today borrowers and lenders and buyers and sellers can pay a fee to use peer-to-peer networks to barter for goods and services and facilitate business. The rapid growth of these networks validates a pent-up demand for direct electronic communications. However, electronic communications have risks, mainly: how do parties know that the people they are doing business with are who they say they are?

Identity fraud occurs globally across public, private, corporate and consumer segments. To combat fraud, new regulations are being developed. Although these regulations can decrease identity fraud, they can also have the adverse affect of hampering or slowing emerging market growth. Meeting the dual challenges of supporting rapidly growing peer-to-peer networks while protecting parties from fraud requires a global, interoperable standard for identity authentication.

Interoperability on a Global Basis

Legal inconsistency increases the challenges of global commerce: companies doing business in multiple countries must navigate multiple legal environments since every country has its own regulatory and legal framework, liability and legal recourse.

To truly expand global communication and commerce over peer-to-peer networks, participants must feel confident that an infrastructure exists to limit liabilities due to fraud. Cross-border cooperation and interoperability are critical to limiting liability, minimizing risk and creating trust. Three examples of highly-successful trusted environments operating interoperably across borders are SWIFT, Visa and MasterCard.

What makes each of these three schemes successful is the cross-border interoperability of their policies, rules and legal framework. All three environments are bank-backed and provide users with assured authentication. Participants have agreed to limit liability and to honor transactions created by companies beyond their borders based on authentication performed by other members. By working with regulators and lawyers in each country where they operate, these companies greatly reduce risk for themselves and for participating financial institutions.

Utilizing electronic rather than paper-based documents can provide much needed cross-border legal consistency as well. Indeed, cross-border purchases of real estate, fine art and other highly priced commodities will experience explosive growth as paper documents are replaced by electronic documents with identity authenticated digital signatures.

But some legal obstacles remain. Many of the international conventions and national laws adopted more than twenty years ago did not anticipate the use of electronic communications and modifications still need to be made.

The IdenTrust Difference

Similar to SWIFT, Visa and MasterCard, IdenTrust was developed by a consortium of financial institutions from around the world with the shared objective of delivering trusted electronic commerce. Working together, these institutions agreed on rules for authenticating identities and developed a set of policies and procedures to be performed prior to certificate issuance that all members can rely upon regardless of which institution performed the authentication. The result is the IdenTrust Rule Set.

Today, IdenTrust digital certificates and signatures are accepted in more than 175 countries. This number will continue to grow as more global banks join the IdenTrust network.

Expanding this consortium to include global participants ensured that identities are globally interoperable under uniform private contracts recognized around the world. Unlike most systems that require public law, IdenTrust rules also govern customer agreements and ensure that they are valid, binding and enforceable in countries where the participants do business.

Identity management requires consistent vetting, storing and validating. An enterprise approach makes it easier for customers to adapt to using digital certificates and signatures. Multiple unique approaches only cause confusion and open the door for fraudsters.

IdenTrust employs a secure operation that is audited 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.

The IdenTrust operational environment is easy to integrate with other trust-related products and services, enabling financial institutions to extend their spectrum of compliance more rapidly. Platform flexibility is also critical to allow for an open selection of technology to integrate with certificates (e.g. USB, soft certificate, smart card, encrypted USB drive with smart card chip).

Identity Management Requirements

Identity management is a key component of a comprehensive approach to risk management. Being certain that the counterparty to a transaction is who they purport to be based on support from one or more trusted intermediaries facilitates dematerialization. To be truly “trustworthy,” this risk management framework must allow parties to interact in an environment of privacy, authentication, message integrity and non-repudiation by provisioning credentials which enable authentication, encryption and digital signing.

Many identity solutions available today are called “self-signed” or “self-asserting” because the identities are not verified by an independent third-party. However, financial institutions require customers to provide multiple forms of identification before opening any type of banking, insurance or capital markets-related account or transacting payments. This federally-mandated process, called Know Your Customer (KYC) applies to both individuals and corporations and demands that the same stringent controls and level of trust be applied to digitally-issued identities. Additionally, financial institutions are subject to Anti-Money Laundering regulation adding another layer of protection for the certificate holder.

A globally consistent approach to digital identity due diligence, similar to payments due diligence, provides identity transparency. Disjointed, non-interoperable identities give rise to inefficiencies, additional costs and greater risk. Identity schemes that only work within a closed system restrict growth and commerce. And, while bilateral agreements have been made between organizations within small communities, they are not scalable on a pan-European or global basis. A rules-based scheme approach wherein one contract provides watertight relationships and liabilities for all members is needed.

Financial Institutions as Trusted Intermediaries

In a world where terrorism threatens the global financial system, financial institutions are now required to perform a more comprehensive identity authentication. They are in the business of bearing the liability and risk for their customers. IdenTrust, through its history, is still regulated as a financial institution owned consortium, it is therefore subject to yearly audits of its operations. Peer-to-peer networks can procure identity services from an IdenTrust member institution and utilize this infrastructure to provide identity authentication and validation. Alternately, they can act as their own Registration Agent (RA) and procure digital certificate issuance and infrastructure services directly from IdenTrust if they qualify as a financial services organization as defined in the IdenTrust Rule Set. Acting as their own Registration Agent, they can accelerate delivery of identity authentication services to support a rapidly growing new market.

Financial institutions are best positioned to provide a globally accepted identity authentication service. While others such as governments and private organizations (e.g. VeriSign and RSA) can and do provide these services, they are problematic:

- Although governments are massive users of electronic networks and keepers of detailed electronic information (such as tax returns) and have a strictly-defined liability framework, they are not well-suited to managing commercial risks between citizens, businesses and third-parties.
- It's impractical for corporations or citizens to assert their own identities in making or receiving a payment and to manage non-repudiation and dispute resolution for multiple applications across multiple jurisdictions. Like governments, corporations and citizens do not view themselves as managers of the operational risks associated with intermediation between parties.

Financial institutions can assure that the counterparty is who they say they are. Using a credential that is accepted by financial institutions around the world and can be used for Internet-based trade, banking, insurance and brokerage expedites the movement to electronic documents.

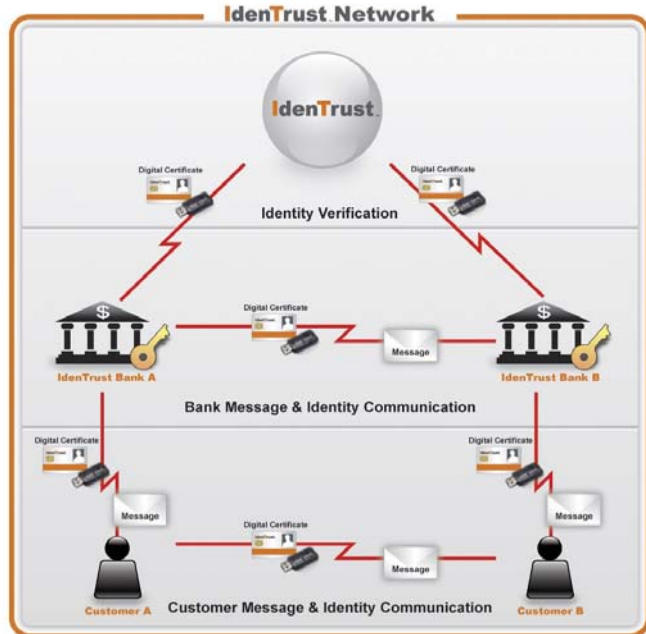
Combining Security and Privacy

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. Privacy is compromised as transactions are opened to perform authentication and verification.

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 allows only authorized users to 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 and not the data associated with the transaction. The transaction data itself is never passed to IdenTrust but remains with the banks involved.

See the figure that follows for an illustration of the data flow and the privacy protection inherent within the IdenTrust Network.



SUMMARY

Peer-to-peer networks are changing the way we communicate and do business, hastening the evolution away from traditional methods of using financial institutions and their channels that were created to lessen risk through limitation of liability, proprietary networks, and non-repudiation of all commercial transactions. However, these protections, while encouraging the highly risk averse to use them, are a closed environment, often require more procedures, and frequently stifle growth.

To encourage the growth of peer-to-peer connections while instilling trust and providing greater risk protection from fraud, a globally interoperable identity authentication standard is required. Participants in these public marketplaces and exchanges must be able to issue, authenticate, validate and rely on identities provided electronically, and make acquiring and using them simple. To do so, the digital identity must be authenticated and validated by a trusted source. Financial institutions are regulated to perform this function as part of account opening and changes. They are also regulated to control privacy and access to confidential information entrusted to them. Additionally, financial services firms meeting the definition of a financial institution in the IdenTrust Rule Set may also act as a Registration Agent (RA) for their own customers. Utilizing the IdenTrust infrastructure to provide an identity authentication and validation service ensures the authenticity of individuals and companies meeting over the Internet.

Additionally, this approach maintains the privacy of the transactions that are digitally signed and sent over the network. Combining Know Your Customer (KYC) level authentication with privacy protection delivers a reliable way for peer-to-peer networks to assure trust in "faceless" transactions and thus expand more rapidly.

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