IdenTrust™

Bank Assurance for Government

All You Need is One.

Enabling an eco-friendly digital world.

White Paper

INTRODUCTION

In recent years, governments worldwide have instituted laws that directly or indirectly require companies to reduce vulnerability to identity theft. In many cases, their initial rollouts have focused on the public sector but the prevalence of digital certificates and greater market awareness of identity fraud have pushed governments to now require civilian identity authentication. The United States, the European Union, Korea, Brazil, Mexico, Chile, Japan, Australia, Singapore and many other nations have drafted or implemented regulations to authenticate credentials before issuing government documents such as e-passports, marriage licenses, electronic voting ballots, visas and residence permits, citizenship, and driver's licenses. Governments are also rapidly moving to electronic invoicing and tax filing to reduce fraud, improve on collection and provide a more robust audit trail.

The volume of government-issued documents for citizens, the amount of fraud and error, and the lack of tracking available with paper-based systems makes it difficult for governments to meet their own audit regulations. They must transition to electronic processes, and this has helped to make digital signatures and certificates become mainstream. Here are just a few examples of digital signature/certificate projects that are underway:

- Online government transactions (e.g. Tax payments) with relatively high-risk profiles where active mutual authentication is important to prevent website fraud through man-in-the middle attack (refer, for example, to authentication Levels 3 and 4 in the United States National Institute of Standards and Technology (NIST) SP800-63: Electronic Authentication Guideline).
- Electronic pension / employment benefits transfer using smartcards.
- Cards may be used for a range of specific public sector applications, such as library cards or learning cards.
- Official documents may be issued in the form of smartcards, as a secure alternative to paper documents, for example, driver's licenses, electronic passports.
- Digital credentials or business licenses can be carried by smartcard.
- Identification cards may be used to identify either government employees or members of the public and provide access to buildings or computer systems.
- Employee access card with secured passwords to protect access to computer systems.
- Mass transit fare collection systems.
- Electronic toll collection systems.
- Consumer health card containing insurance eligibility and other entitlements.
- A patient's smartcard can act as a key which healthcare professionals can use to access electronic health records, with the patient's consent.
- Emergency medical data (medic alerts, allergies, drug reactions).
- Electronic prescriptions may be issued by doctors to a patient's smartcard (though probably in summary form rather than in their entirety) and thus conveyed to dispensaries.
- All-purpose multi-function student ID card, containing a variety of applica tions such as electronic purse (for vending and laundry machines), library card, record attendance at classes, concession card and logical access control for network logon.

Cross-border standardization is becoming more significant as governments issue digital certificates and signatures based on similar guidelines and policies to track cross-border fraud. Governments are trying to support increasingly mobile citizens where they live and work. In countries such as the U.S. where a robust government infrastructure exists for certificate issuance, interoperability for civilian focused systems with the existing infrastructure is critical.

"KNOWING ME, KNOWING YOU"

Terrorism continues to increase around the world and as a result, governments are implementing a variety of ways to minimize the issuance of fraudulent credentials and to identify those credentials that have already been stolen. For generations, consumers and businesses alike have trusted financial institutions to secure their most confidential data and represent them in financial transactions. Therefore, governments are working with financial institutions to issue identity credentials that utilize the identity data that they already maintain, minimizing identity data replication and expanding consistency between the public and private sectors. Reducing the number of providers of Know Your Customer (KYC) services increases control over identity data and restricts the number of parties who can violate privacy rules.

As the number of identity authentication programs increases, so does the use of erroneous data for authentication. Each new company that is awarded a contract to deploy an identity authentication infrastructure expands the replication of identity data: some of it vetted appropriately, some not. As an example, in many parts of the world authentication of individuals is based on credentials such as driver's licenses and identification cards that were issued with little or no vetting of the credentials used when the these documents were obtained. Thus, the lack of "due diligence" in the process spreads as each new issuer relies upon credentials that were issued without appropriate authentication. The extreme implications of this can be seen in situations such as the terrorists who flew planes into the World Trade Center and the Pentagon all had U.S. driver's licenses they used as identity credentials to obtain other credentials and authorizations.

GAINING ADOPTION

Traditionally, consumers and small businesses around the world used cards with a magnetic stripe containing personal information. In recent years, many countries have transitioned or have begun transitioning to chip based smart cards. Consumers routinely present these cards for payment and, in some cases, authentication. Downloading encrypted digital identity credentials (e.g. digital certificate) onto a chip in a smart card opens the opportunity to expand the card's use. By combining a PIN with the encrypted digital certificate (private key), use of the card could securely be expanded to allow cardholders to present these credentials for various government programs such as residence permits, marriage licenses, voting credentials and driver's licenses. Cardholders will also be able to digitally sign these types of documents and any related transactions, providing proof of authenticity, integrity and a non-reputable audit trail.

Because identity data on a chip is encrypted, a fraudster cannot capture this data from the card or at the device reader. By inserting the card at the government agency terminal and entering a PIN to unlock the private key encrypted on the certificate, the consumer verifies the validation with the bank. Because the bank issued the certificate based on a globally accepted set of Know Your Customer (KYC) validation rules, the agency can rely upon this validation in real time.

Bank authenticated digital identity credentials could provide a single, consistently accepted way of proving identity authentication for a myriad of requests such as applying for telephone services, loans, cable services or memberships. Issuing credentials consistently across financial institutions facilitates commerce, communication and mobility.

IDENTRUST

The meteoric expansion of commerce over the Internet was the impetus for ten of the world's leading banks to create IdenTrust in 1999. Financial institutions around the world understood the risks inherent in financial transactions where the parties never meet and therefore must rely only upon electronic credentials. These founding IdenTrust banks felt that a common identity structure was a logical extension of their existing customer relationships. Together, these ten banks plus an additional twelve banks invested more than $170 million to create the basic IdenTrust offering.

THE IDENTRUST VALUE PROPOSITION

The IdenTrust value proposition is to provide a unique, internationally regulated approach that turns the Internet into a highly secure virtual private network. The network is based on a proprietary rule set built by, and for, the global financial services community and its customers. The rule set establishes a binding legal and regulatory framework that enables an interoperable identification and authentication process for all transactions and documents, whether business to business, business to consumer, or consumer to consumer.

The IdenTrust network gives its users the ability to do three key activities in a totally electronic fashion:

- Authenticate – Prove the identity of individuals or businesses.
  - o IdenTrust identities allow individuals or businesses to prove they are who they say they are, and conversely, it allows individuals or businesses to rely on the identity of someone initiating a transaction or document.
  - o 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.
  - o IdenTrust identities lock the contents of a transaction file and/or document, making them impossible to tamper with.
  - o IdenTrust identities scramble the information, making it impossible to read or decipher by someone not authorized to view or access it.
  - o IdenTrust identities encrypt and control the process flows so that no one can intercept or redirect the transaction or document, eliminating both phishing and man-in-the-middle attacks.
- Digitally Sign – Create a legally binding and non-repudiable electronic signature.
  - o 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.

Using these functions alone or in combination, individuals and businesses can engage in any type of electronic commerce or business activity, ranging from signing contracts to initiating payments to handling complex supply chain transactions – all with the benefit of knowing that the entire process is fully compliant with regulatory requirements such as Sarbanes-Oxley Act, HIPAA and FFIEC multifactor authentication banking guidelines, as well as global anti-money laundering (AML) and Know Your Customer (KYC) requirements.

The benefit of the IdenTrust approach is that a single identity can be used across multiple applications and in multiple environments. In much the same way a Visa or MasterCard is accepted by multiple merchants, IdenTrust bank-issued identities are accepted by multiple merchants. This means a business or individual will only need a single identity rather than multiple passwords or cards or tokens for access to different banks, businesses or applications. Businesses and individuals can use that single identity for multiple functions in more than 175 countries around the world (see chart below), making it possible to electronically sign a document while in Sweden and have it be legally binding in Singapore, New York, Tokyo or London.

UN	WTO	FATF	FATF Style	IdenTrust Eligible	Number of Countries
Recognised Country	Contract Law	AML and KYC 40+9	AML and KYC 40+9	Regulated Financial Institutions	
✓	✓	✓	-	☑	38
✓	✓	-	✓	☑	119
✓	✓	-	-	☑ Follow IdenTrust KYC	19
✓	-	-	-	-	19
				Total Countries	195

Figure 1 - Countries with IdenTrust Interoperability

IDENTRUST MEMBER ELIGIBILITY

IdenTrust requires that its members are engaged primarily in the business of providing financial services and are thus subject to substantive regulation and periodic examination by the in-country regulator and IdenTrust.

Members are required to meet one or more of the following criteria:

- Are incorporated in one of the 195 countries that recognize contracts under the law of another country.
- Located in one of the Financial Action Task Force in Money Laundering (FATF) member countries.
- Located in a country which belongs to one of the FATF-Style regional bodies committed to implementing 40 recommendations on Money Laundering and 9 special recommendations on terrorist financing.
- Not located on one of the 19 countries not recognized by the World Trade Organization or FATF.

IdenTrust is accredited in 176 countries meeting these eligibility requirements. Banks in an additional 19 countries are eligible to issue IdenTrust credentials.

THE IDENTRUST PLOT

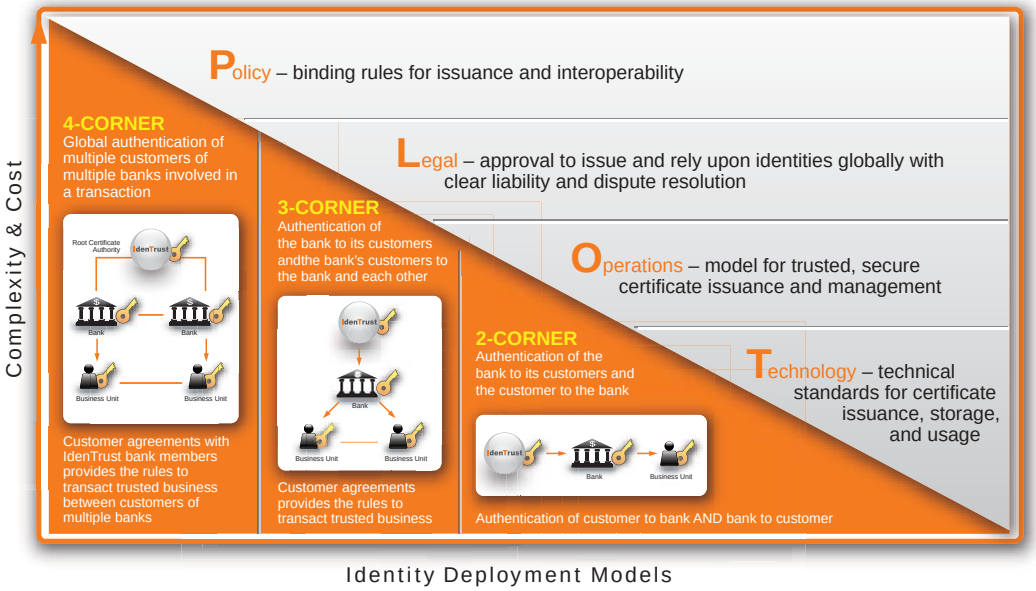
Although technology issues typically receive the most attention in the identity industry, in reality they represent just the tip of a very large iceberg. The most pressing identity dangers exist in the policy, legal and operations areas. The IdenTrust rule set is unique because it focuses on all aspects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

The IdenTrust rule set 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, along with making certain that the process is done consistently everywhere around the world.
- **Legal** issues such as what should occur when something goes wrong, setting base liability structures and guaranteeing that each identity meets the legal requirements in every jurisdiction.
- **Operations** issues such as how identities are manufactured to ensuring that the entire process is secure. This includes physical security (identities are distributed and turned out using at least two different channels – mail and email or mail and phone, for example) 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 across 175+ countries. These volumes are increasing 15% each month and include financial transactions such as payments as well as business transactions such as invoice flows.

The IdenTrust intellectual property embedded in the PLOT is also unique due to its comprehensive coverage. Other identity solutions in the marketplace today focus only on the simplest aspect of identity: the technology. IdenTrust goes beyond this, covering not the technology, but also the operational, legal and policy issues that must be addressed and which are typically handled outside the technology organization.



WHY THE IDENTRUST PLOT IS UNIQUE

- Only the total combination of the PLOT components - Policy, Legal Frame work, Operations Hosting, and Technology provides a comprehensive solution to risk management in digital transactions.
- Policies and procedures developed and agreed to by financial institutions around the world provide a comprehensive approach authenticating identities.
- IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world. Other systems rely on public law for digital signatures.
- Customer agreements are valid, binding and enforceable in countries where members offer the IdenTrust Service.
- IdenTrust delivers a complete, hosted environment to enable a full spectrum of trusted identity services.

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 in a 4-Corner Model in which a corporation uses multiple banks that are members of the IdenTrust community.

UNDERSTANDING TRUST

Understanding the right level of trust is the first step in creating the most comprehensive approach to trusted identities and identity management operations. IdenTrust helps customers and users to understand the level of trust required for specific business needs through an interactive trust score determination.

Key in the effort to detect potential money laundering earlier is knowing the identity of the individuals involved. IdenTrust is regulated as a financial institution and is overseen by the Office of the Comptroller for the Currency (OCC). Thus, the operations undergo a yearly audit similar to financial institutions. Under the IdenTrust rule set and requirements to comply with USA Patriot Act Know Your Customer (KYC) rules, the institution is held to stringent guidelines for determining the identity and authenticity of the company requesting the account and determining the legitimacy of the business. Using an IdenTrust certificate-based smart card, tracking is easier. Across the spectrum of IdenTrust and IdenTrust partner applications, there is only one single source for trust.

SUMMARY

Activities that use digital identity certificates and signatures are underway around the globe. While the initial focus has been on business to business transactions and transactions within government agencies, most European countries and most of Latin America and Asia are increasingly deploying civilian/consumer-based programs. These countries are also expanding efforts to implement better preparedness against terrorists operating in their countries and to make tracking fraud and criminal acts easier with cross-border consistency.

Each country must determine how to issue identities and manage them on an ongoing basis. This provides governments with a unique opportunity to work with their country's financial institutions to control the proliferation of identity information, retain it in an environment that consumers and corporations already trust and deploy a consistent standard for identity issuance, vetting, validation, operational handling, legal infrastructure and technology access.

The IdenTrust "two sided coin" feature provides infrastructures already deployed with bank interoperability, minimizing the cost and time to market for solution deployment. Governments can get the best of both worlds by using their own infrastructure for public sector activities and partnering with banks for the deployment of civilian identity authentication programs.

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 175 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.
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
USA
Telephone: +1.866.IDENTRUST (+1.866.433.6878)
Fax: +1.415.486.2901