

Consumer Identity Cards

Improved revenue flows and tracking for Anti-Money Laundering



Table of Contents

<i>Introduction</i>	3
<i>Market Opportunity</i>	4
Knowing who you are dealing with	4
<i>Government Directives</i>	7
<i>Gaining Adoption</i>	7
<i>IdenTrust</i>	8
The IdenTrust Value Proposition	8
The IdenTrust PLOT.....	11
Why the IdenTrust PLOT is Unique.....	12
<i>Anti-Money Laundering Compliance</i>	13
Credit and Debit card Devices.....	13
Contactless Payments and a Multi-Purpose Smart Card	14
Description of Solution/Services.....	15
Executive Summary	16

This document is strictly confidential, contains trade secret information of IdenTrust, and is disclosed only under the Non-Disclosure Agreement between the parties. This plan is for the Bank's information and evaluation only and may not be used or disclosed except as provided therein.

Introduction

Anti-Money Laundering (AML) is defined as having three components: 1. Placement – where illicit cash is converted to monetary instruments or deposited in the financial institution, 2. Layering – where funds are moved to other financial institutions, and 3. Integration – where funds are used to acquire assets or fund further activities. In the last year or more, there has been an increase in focus related to AML efforts that need to be in place to ensure that the debit card networks can not be violated. Auditors have begun to look for controls to be in place on IP based debit card networks, as part of their Anti-Money Laundering analysis. These debit card focused controls must be able to work in conjunction with the spectrum of approaches financial institutions are taking to address money laundering.

One example, among many, for debit card based money laundering has the launderers establishing a legitimate business in a country as a “front” for their illicit activity. They establish a bank account and obtain credit and debit cards under the name of the “front business.” Funds from their illicit activities are deposited into the bank accounts they have created in the United States and other countries. While in another country, where their U.S. based bank has affiliates, they make withdrawals from their U.S. bank account, using credit and debit cards. Money is deposited by one of their cohorts in the U.S. and is transferred to pay off the credit card loan or even prepay the credit card. The bank’s online services make it possible to transfer funds between checking and credit card accounts without connecting all of the activities related to the total transaction.

The bank that opened the account for the business should conduct appropriate due diligence as part of the account opening process. It should understand the nature of the business and the type of activity expected of the business including the size, frequency, and types of payments that are most typical of the business, and then be able to track those expectations against the use of the bank’s services by the new account holder. The bank should also be able to monitor the business for deposit activity including potential structuring. Through being able to tie the identity to all the activity associated with the identity, the bank can monitor patterns and trends on the account for significant changes. Take for example prepayments going to credit cards, the bank can detect suspicious activity and send it off for further analysis through a Suspicious Activity Report (SAR). It is also able to tie all transaction activity together based on identity rather than a specific account.

With each passing year, fraudsters become more adept at finding new ways to launder funds, requiring that the bank’s monitoring continue to be enhanced in order to respond. The more adept that banks can become at identifying the identity of the individuals involved with these transactions, the better their success will be with catching the criminals. It is with this in mind that IdenTrust presents the information that follows. Revenue projections and financials supporting the conclusions drawn in this paper will need to be developed jointly as a next step in this process.

Market Opportunity

Knowing who you are dealing with

As more financial institutions eliminate their proprietary networks in favor of those that are Internet based, the risk of network infiltration and information theft have soared. This has prompted regulators to pass legislation designed to curb the growth of online fraud, identity theft and money laundering. Well-publicized cyber crimes involving the appropriation and misuse of personal and corporate identities and the theft of privileged data have damaged consumer trust in e-commerce and threatened corporate security. Press accounts of stolen identity information being used to purchase real estate, obtain loans, charge up credit cards and illegally transfer funds from the victims' accounts have heightened consumer awareness of bank vulnerabilities. Consumers are demanding that their identities be protected. As a result, governments are putting the onus on financial institutions to authenticate and track Internet based traffic more stringently.

In recent years, governments worldwide have instituted laws that directly or indirectly require companies to reduce vulnerability to identity theft. The United States, the European Union, Asia Pacific, and Latin America have all drafted or implemented regulations to track money transfer transactions and authenticate credentials before issuing various government documents such as: passports, marriage licenses, electronic voting, visas, citizenship, and driver's licenses. They are also rapidly moving to electronic invoicing and tax filing which not only reduces fraud, but improves controls on collection. In parallel, companies are requiring employees to present validated credentials as part of the hiring process and to gain access to confidential and highly secure data. Equally important in these directives is the need to safeguard consumer privacy, protect corporate data integrity and enhance auditing accountability. Standards to combat money laundering and terrorist financing that include customer identification have been proposed by the Financial Action Task Force (FATF), an inter-governmental organization, and have been adopted by more than 150 jurisdictions (see Figures 1 and 2 below).

The FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. It is a "policy-making body" created in 1989, which works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has published 40 recommendations on Money Laundering and 9 recommendations on Terrorist Financing in order to meet this objective. Fulfilling the requirements of the FATF recommendations ensures a consistent adoption of Know Your Customer (KYC) standards that can be relied upon in any of the FATF countries.

A number of international bodies and organizations have observer status with the FATF. These regional FATF-style bodies have similar form and functions to those of the FATF, and some FATF members are also members of these bodies:

- ✓ Asia Pacific Group for AML
- ✓ Caribbean FATF
- ✓ Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL)
- ✓ Eurasian Group
- ✓ Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- ✓ Financial Action Task Force of South America Against Money Laundering (GAFISUD)
- ✓ Middle East and North Africa Financial Action Task Force (MENAFATF)

These organizations are committed to implementing:

- ✓ Forty recommendations on Money Laundering
- ✓ Nine special recommendations on Terrorist Financing.

The international organizations listed are those that have, among other functions, a specific anti-money laundering mission or function. Fulfilling the requirements of the FATF recommendations ensures a consistent adoption of Know Your Customer (KYC) standards that can be relied upon by other countries.

In large part, these rules call for companies to adopt stronger identity authentication measures to assure governmental authorities about the veracity of their electronic transactions. Current and prospective regulations have created a boom in the interest in and use of identity authentication technologies such as digital certificates, biometrics, one-time passwords (OTP) and tokens.

- Argentina
- Australia
- Austria
- Bahrain, Kingdom of
- Belgium
- Brazil
- Canada
- China, People's Republic of
- Denmark
- Finland
- France
- Germany
- Greece
- Iceland
- Ireland
- Italy
- Japan
- Kuwait
- Luxembourg
- Mexico
- Netherlands
- New Zealand
- Norway
- Oman
- Portugal
- Qatar
- Russian Federation
- Saudi Arabia
- Singapore
- South Africa
- Spain
- Sweden
- Switzerland
- Turkey
- United Arab Emirates
- United Kingdom
- United States of America

Figure 1 - FATF Member Countries

- Albania
- Algeria
- Andorra
- Antigua and Barbados
- Armenia
- Azerbaijan
- Bahamas
- Bangladesh
- Barbados
- Belarus
- Belize
- Bolivia
- Bosnia and Herzegovina
- Botswana
- Brunei Darussalam
- Bulgaria
- Chile
- Colombia
- Costa Rica
- Croatia
- Cyprus
- Czech Republic
- Dominica
- Dominican Republic
- Egypt
- El Salvador
- Estonia
- Fiji
- Georgia
- Grenada
- Guatemala
- Guyana
- Haiti
- Honduras
- Hungary
- India
- Indonesia
- Jamaica
- Kazakhstan
- Kenya
- Korea – Republic of (South)
- Kyrgyzstan
- Latvia
- Lesotho
- Liechtenstein
- Lithuania
- Macedonia
- Malawi
- Malaysia
- Malta
- Marshall Islands
- Mauritius
- Moldova
- Montenegro
- Morocco
- Mozambique
- Namibia
- Nepal
- Nicaragua
- Pakistan
- Panama
- Paraguay
- Peru
- Philippines
- Poland
- Romania
- Saint Kitts and Nevis
- Saint Lucia
- Saint Vincent & the Grenadines
- Samoa
- San Marino
- Sao Tome and Principe
- Serbia
- Seychelles
- Slovakia
- Slovenia
- Sri Lanka
- Suriname
- Swaziland
- Syria
- Tajikistan
- Tanzania
- Thailand
- Trinidad and Tobago
- Tunisia
- Uganda
- Ukraine
- Uruguay
- Uzbekistan
- Vanuatu
- Venezuela
- Zambia
- Zimbabwe

Figure 2 - FATF Style Regional Body Members

Government Directives

As referenced in the introduction, almost every major country in the world has initiatives underway that utilize digital identities and digital signatures to authenticate individuals and countries for various purposes. Whether its allowing companies to furnish proxy materials to shareholders through an Internet based "notice and access" model in the US, issuance of residence permits in Germany, an electronic ID card in Belgium, notarization in Hungary, e-Passports and authentication services in the Czech Republic, social security cards in Italy, biometric passports in Russia, electronic ID cards in China, transport cards in Hong Kong, e-signatures for tax filing in Spain, financial institution interoperability for their customers in Brazil through Serasa, or the dozens of other activities that are underway, digital signatures and certificates have become mainstream. Governments have recognized that the sheer tracking of government documents issued for their citizens has become so voluminous that the process must be "electronified". Additionally, the amount of fraud and error, and the lack of or inconsistent tracking that results from these paper-based systems continues to grow causing governments to have difficulty meeting their own regulations for auditing.

A Bank, through its extensive network of branches, has the opportunity to help both governments and their citizens in the adoption of digital identity certificates and signatures. The advantage exists on several fronts, but two main ones – the ability to have a consistent approach regionally, nationally and cross border, thus offering each government or agency consistency and interoperability regardless of where the transaction initiated or was received. The European Union continues to focus on standardization across the EU countries, hoping to lower risk, cost and expedite implementation thus growing business more rapidly and ultimately attracting more foreign investment. The ASEAN nations are also trying to proactively standardize on automation to encourage acceptance across borders in Asia.

The ability to use the same identification and authentication process globally, especially in response to the rapid expansion of workers being transferred to emerging markets, will assist in expediting processing in the new country and thus get them up and running more quickly. Anyone who has worked abroad knows how time consuming and paper intensive it is to set up bank accounts and gain acquire residence in a new country. In combination with its global breadth, a Bank offers governments the advantage of working with a regulated financial institution. Identities issued by a bank are done so under the Know Your Customer (KYC) regulation set by the financial regulators in each country. Additionally, a Bank can work with each country's digital certificate scheme to provide interoperability across border bringing a consistent approach to policies, legal framework, operations and technology access, thus addressing many of the inconsistencies that enable money laundering.

Gaining Adoption

Today, consumers and small businesses around the world use cards with a magnetic stripe containing some personal information, but many countries have transitioned a portion of this magnetic stripe population to smart chip cards. It is routine for consumers to present these cards for payment and, in some cases, identification and authentication. Therefore, downloading digital identity credentials onto a chip in a smart card expands the activities they are already using the card for. Since the identity data on the chip is encrypted, there is nothing for a fraudster to capture at the device. Placing identity credentials on the chip enables the cardholder to present the credentials for compliance with various government programs – e.g. driver's licenses. The

DMV verifies the validation with the bank when the user presents the credentials, thus relying upon the bank for authentication and limitation of liability. This saves time for the consumer and the DMV. This also provides a single, consistent ID, across banks (IdenTrust members) for tracking AML without issuance of a national ID, which is consistently voted down by many countries. Combining this capability with allowing drivers license applications to take their initial test or renewal online or at the DMV office and digitally signing these tests to authenticate the test taker, further automates and secures the current processing flow.

The area of electronic voting is also a consumer focused opportunity for The Bank. Being able to use Bank issued identity credentials to validate the consumer for election registration for voting. These credentials can be renewed through the bank and certified authentic by the bank.

Individuals carrying bank authenticated digital identity credentials would be able to use them as the single, consistently accepted way of proving identity authentication for a myriad of requests – applying for: phones or phone service, a loan, cable services, memberships, etc. Credentials issued consistently across financial institutions facilitate commerce, communication and mobility.

IdenTrust

The meteoric expansion of commerce over the Internet was the impetus behind the formation of IdenTrust. Financial institutions around the world understood the risks inherent in a financial transaction where the parties to the transaction never meet and must rely only upon electronic credentials to consummate their agreements. Ten of the world's leading banks created IdenTrust in 1999. The founding IdenTrust banks felt that a common identity structure was a logical extension of their existing customer relationships. Together, these banks plus another twelve spent more than \$170 million to create the basic IdenTrust offering.

The IdenTrust Value Proposition

The IdenTrust value proposition is 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, creating 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 that identity of individuals or businesses
 - IdenTrust identities allow individuals or businesses to prove that they are who they say they are, and conversely, it allows individuals or businesses to rely on that proof, being able to accept the identity of someone initiating a transaction or document.
 - Because IdenTrust identities are backed by banks around the world, if the identity turns out to be false, individuals or businesses that relied on that identity are covered by a liability structure provided by the banks (very similar to that provided in the credit card space).
- ✓ **Encrypt** – Control visibility into and integrity of transactions or documents

- IdenTrust identities lock the contents of a transaction file and/or a document, making it impossible to tamper with them once locked.
 - IdenTrust identities can also scramble the information, making it impossible to read or decipher by someone not authorized to view or access it.
 - IdenTrust identities also encrypt and control the process flows, ensuring that nobody 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
- IdenTrust identities can be used to replace “wet” signatures, allowing documents and transactions to be done entirely in electronic format with the same levels of legal protection and enforceability associated with traditional ink on 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 like Sarbanes Oxley, HIPAA, the 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. Much like in the credit card space where a single Visa or MasterCard can be accepted by multiple merchants, IdenTrust bank-issued identities are accepted by multiple merchants, meaning that a business or individual will only need a single identity. No more list of passwords, no more multiple cards or tokens for access to different banks, businesses or applications – just one simple IdenTrust identity. Best of all, that same identity can be used for multiple functions in more than 175 countries around the world based on the FATF, FATF Style, World Trade Organization (WTO) and United Nations (UN) accepted guidelines– making it possible to sign a document electronically while in Sweden and have it be legally binding in Singapore, New York, Tokyo or London.

Any financial institution that is regulated by government is eligible to become an IdenTrust Participant. Members are subject to periodic examinations and annual financial reporting requirements, and must not have been notified of regulatory non-compliance. All members are subject to capital requirements and must be able to finance their liability under the Operating Rules (minimum of \$10 million). IdenTrust Participants must also obtain required regulatory approvals and opinions of counsel (e.g. that customer agreements are enforceable), and, demonstrate compliance with the IdenTrust technical, operating and legal requirements.

The IdenTrust membership structure defines various roles and responsibilities for the financial institutions that participate. A Participant in the IdenTrust network has a) entered into a Signatory Agreement for Participants [IL-SAP] with IdenTrust and b) offers IdenTrust Services as a Registrar and/or as a Relying Participant. A Registrar is a Participant that performs the functions of a Registration Authority for digital certificates generated by an Issuer with respect to a subscribing customer with which that Registrar has entered into a Customer Agreement.

As a Registrar, financial institutions enter into Customer Agreements and are required to vet their customers under Know Your Customer (KYC) rules created with input from countries around the world. This process identifies or delegates identification of the bank customers' certificate holders and generates keys for these customers. The Registrar also requests generation of certificates from an IdenTrust Issuer and then registers and distributes the identity certificates issued to its customers. The Registrar is also responsible for distributing IdenTrust compliant software to its

customers and requesting revocation or suspension of certificates for customers that it deems are inappropriate to have them under the IdenTrust Rule Set. A Registrar Without Keys (RAWOK) may do all of these things or rely upon its contracted Registrar with Keys to do them.

The other key role within the IdenTrust structure is the Issuer. Issuers are Signatories undertaking the functions of a Certificate Authority to generate and revoke digital certificates on behalf of a Participant for the use of customers and to send and receive IdenTrust system transmissions. Issuers generate, suspend and revoke customer digital certificates on behalf of Registrars. They are required to send and reply to IdenTrust OCSP (Online Certificate Status Protocol) messages regarding certificate status. They must also comply with applicable rules, specifications policies and procedures under the IdenTrust Rule Set. And, lastly, Issuers may perform ancillary roles such as Participant support, consulting, or may contract to perform Participant roles (e.g. key generation). Issuers must also have the capital or insurance to finance their liability under the Operating Rules (\$10 million) and meet applicable regulatory requirements (e.g. local certificate authority accreditation if any).

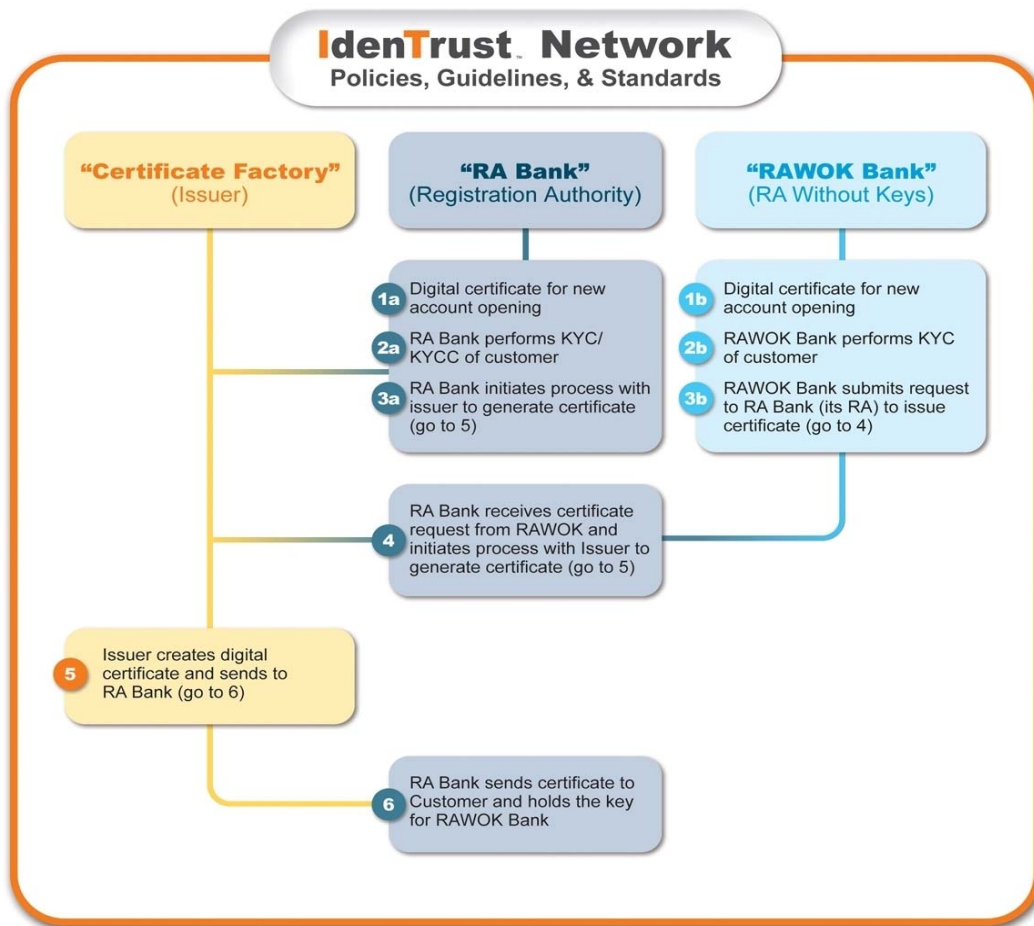


Figure 3 – The IdenTrust Roles

IdenTrust members must be engaged primarily in the business of providing financial services and is subject to substantive regulation, and periodic examination by the in-country regulator. A

member must be incorporated in a country that recognizes contracts under the law of another country: 175 countries, and located in one of the FATF member countries. Or, a member must be located in a country which belongs to one of the FATF-Style regional bodies committed to implement: 40 recommendations on Money Laundering and 9 special recommendations on terrorist financing. Alternatively, a member must be prepared to adopt the IdenTrust KYC standard. A member must not be located on one of the 19 countries that are not recognized by the World Trade Organization or FATF. IdenTrust has already been accredited in 176 countries that stand up to the eligibility requirements above.

The IdenTrust PLOT

This network is different from anything that exists today because it focuses on all aspects of the network – not just the technology. In the identity world, while the technology issues typically get the most attention, they are really just the tip of a very large iceberg with the bulk of its mass under the water. The major danger areas come from the policy, legal or operations areas, all of which are also covered by the IdenTrust approach. The IdenTrust identity infrastructure covers:

- ✓ **The Policy** aspects
These cover items such as who gets 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.
- ✓ **The Legal** aspects
These cover what happens when something goes wrong, including setting base liability structures and guaranteeing that each identity meets the legal requirements in every jurisdiction.
- ✓ **The Operations** aspects
These cover how the identities are manufactured, ensuring that the processes are secure every step of the way including physical security (the identities are distributed and turned out using at least two different channels – mail and email or mail and phone, for example.), and also ensuring that the network is always available.
- ✓ **The Technology** aspects
These cover the basics of how the identities and the overall network work. The technology used is standard, but the way it is put together is and controlled is proprietary to ensure even higher levels of security.

This combination of policy, legal, operations and technology (the “PLOT”) is being used for more than 40 million transactions annually across 90+ countries, with the volumes growing at the rate of 15% month over month. These transactions 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.

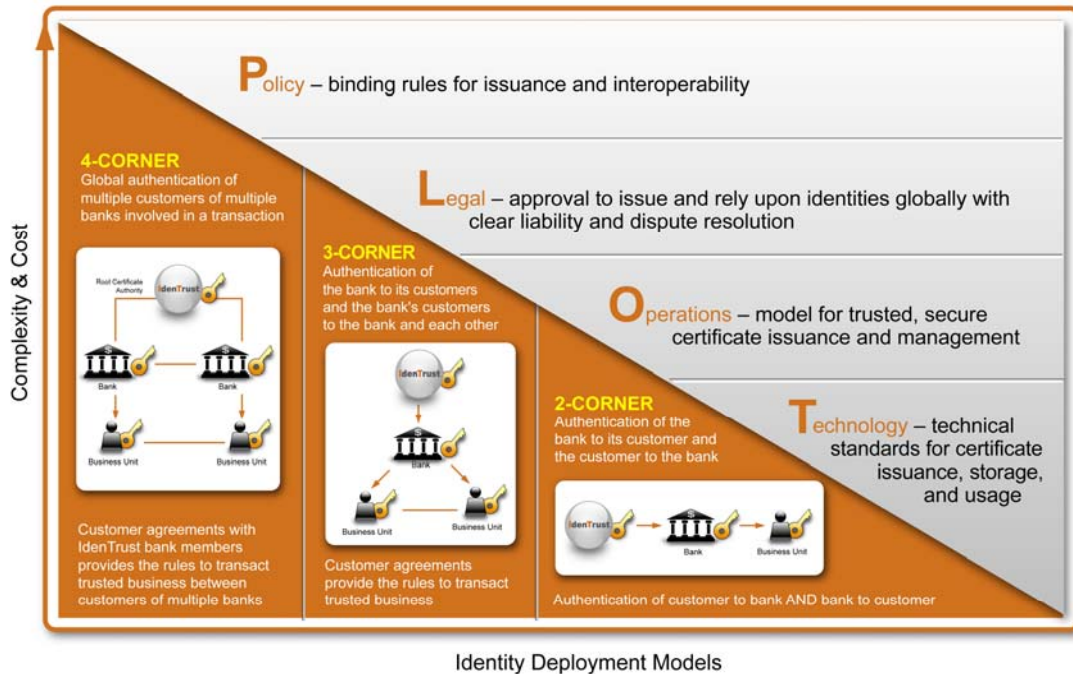


Figure 4 - The IdenTrust PLOT

Why the IdenTrust PLOT is Unique

- ✓ Only the total combination of the PLOT components - Policy, Legal Framework, Operations Hosting, or Technology, provides a comprehensive solution to risk management in digital transactions
- ✓ Policies and procedures developed and agreed to by financial institutions around the world provides a comprehensive approach authenticating 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
- ✓ 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

The value of the PLOT can be applied when a corporation is interacting only with their own bank, in a “Two Corner Model”, when interacting through their own bank with another customer of that bank in a “Three Corner Model”, and/or when interacting with corporations using multiple other banks that are all members of the IdenTrust community in a “Four Corner Model”.

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

and identity management operations. Across the spectrum of IdenTrust and IdenTrust partner applications, there is only one single source for trust.

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, the requirement to comply with USA Patriot Act Know Your Customer (KYC), rules, hold the institution to stringent guidelines for determining the identity and authenticity of the company requesting the account, and, to determine the legitimacy of the business. Using an IdenTrust, certificate based smart card, doing this type of tracking would be easier.

Anti-Money Laundering Compliance

Auditors have become increasingly aware of a number of vulnerabilities within both proprietary and shared payment networks around money laundering. Individuals looking to launder funds using multiple low value transactions, through accounts both within and across multiple banks, are difficult to track. Utilizing the IdenTrust Trust Network for validating identities and how they are issued across member banks, would provide an additional safeguard against money laundering. Thus, the issuing bank is responsible for vetting the credentials used for opening accounts within that bank, but also, for ensuring that the credentials issued can be relied upon by other banks in the network. When the account holder uses IdenTrust credentials to open accounts at other banks, use of those credentials will enable the banks involved to track the end to end flow of the transaction. While IdenTrust does not interrogate the message itself, it does track the certificate use and that information can be uploaded into Anti-Money Laundering (AML) solutions for detecting patterns, velocity, etc. that would trigger further investigation. This is especially helpful in tracking foreign card transactions for hard to catch offshore laundering.

Knowing who is actually using the card is a big step toward identifying the perpetrators of fraud and money laundering. Using the IdenTrust certificate for end to end tracking of all parties touching the transaction, financial institutions have a single unique identifier, cross bank, thus enabling a broader spectrum of transactions to be analyzed for unusual behavior and hopefully catching more of the perpetrators.

Card Devices

While NCR and Diebold provide the vast majority of ATM devices deployed around the world, there are other manufacturers such as Wincor-Nixdorf, Fujitsu and Okidata who also own sizeable market share within particular countries. There are also independent card reading device manufacturers such as Verifone. European banks have taken the lead in implementing Internet Protocol (IP) based services for their customers; the rest of the world is still evolving their networks from Proprietary or OS2 based to the Internet. This transition offers enormous opportunity for card reading device manufacturers. Newer machines require only a board or software change to make this transition, for older ones, replacement is required. Additionally, the latest generation of machines uses Radio Frequency Identity (RFID) as a standard for contactless cards which are entering the market in pilots around the world. Many of these devices are deployed and supported by processors (e.g. ADP, EDS, Total Systems). Since they are not financial institutions, a Bank in its role as Certificate Authority (CA) can recruit them as Registration Agents or Registrars without Keys, for digital certificate issuance.

Contactless Payments and a Multi-Purpose Smart Card

IdenTrust can, through placing an encrypted certificate on an EMV standard smart card, in conjunction with site key verification, provide much stronger controls for AML. In conjunction with partners that offer site key verification, the bank can offer mutual authentication for their credit/debit card holders. Reading the smart card, a site key verification is performed. If the site is not a valid site, this is immediately noted to the cardholder. If the site is valid, a site key will be shown on the device's screen for the user to validate. Upon validation, a request for certificate validation is then sent off to IdenTrust. If the certificate is not valid, the transaction is terminated. If the certificate is valid, the transaction will proceed. With both of these validations confirmed, the card holder can then proceed with the transaction by entering a valid pin or password. Thus, the user has been authenticated to the bank and the bank's device has been authenticated to the user. Mutual authentication has been completed.

The IdenTrust digital certificate that is on the smart card, is issued based on the bank's own KYC procedures that must be in compliance with the USA Patriot Act. No certificate would be issued without the appropriate level of vetting on the part of the bank as the issuing bank takes on liability of a maximum of \$10 million annually, for the certificate as part of the IdenTrust membership. Additionally, as the certificate is used each time, the bank has Sarbanes-Oxley level tracking for SARs and other Bank Security Act (BSA) tracking.

Hong Kong, Scandinavia, Chile and Argentina, are among the countries that have implemented contactless payment systems. In Hong Kong for example, the Octopus system enables public transit travelers to flash their Octopus card (smart card) near a reader, and payment is transferred. In the last year, this program was expanded to allow parents and children to use Octopus cards to pay various fees related to school. Insuring that the identity of the cardholder is authenticated by a financial institution would enable these cards to be used for an expanded group of services including identity authentication for: entrance applications and exams, passport issuance or renewal, job applications, driver's license applications and issuance, automobile and boat registrations, memberships, and, verifying contractors and employees.

With an IdenTrust certificate based smart card, banks can also supply the Department of Motor Vehicles (DMV) around the US with authenticated credentials upon which driver's licenses can be issued. The Real ID program, currently being discussed in the US Congress, requires consumers to present authenticated identity credentials in order to be issued a driver's license or renewal. Consumers holding an "Identity" card with an encrypted IdenTrust identity certificate on it can utilize the card for many more purposes and thus drive additional revenue for the banks. Other government programs also requiring validated credentials for consumers are around electronic passports, and authentication of workers whose private sector jobs must integrate with government agencies and programs.

Going beyond these types of programs, the identity card can also be used by employees to assist corporations in gaining accountability down to the individual level. Thus, e-mail, instant messaging, Voice mail retrieval, web conference participation etc. can also be authenticated to ensure that only the authorized, authenticated party is participating or accessing information. Trust is expanded to these activities while adding end-to-end audit tracking for compliance purposes if needed.

These are just a few of the myriad of possibilities for the Bank-issued identity card with an IdenTrust identity certificate on it. Whether utilized in a chip reading device or not, between the public and private sector, there will be demand for identity authentication that is interoperable not only between countries, but also between different systems domestically.

Description of Solution/Services

IdenTrust currently provides a solution in which Diebold utilizes certificates for device authentication and remote key transport encryption between a device and a Host Bank. During the manufacturing cycle, the pin pads on the ATMs are embedded with digital certificates from IdenTrust. The Host Bank Server communicates to the SSL secured ATM pin pad using certificate based authentication and encryption. Using this secure method of communication, the Host Bank Server can manage the transport keys that are utilized for encrypting communication to/from the card devices. IdenTrust will need to work with NCR and others to determine how to provide similar secure socket layer security with their various devices.

Working together with a Bank, IdenTrust and other card device manufacturers supporting a Bank's network of correspondent banks can provide Certificate Authority (CA) services for those not wanting to stand up their own, but wanting strong authentication for their IP- based devices. Through CA services, a Bank provides digital certificates on EMV compliant smart cards that can be used in chip readers on the devices. The correspondent bank registers its customers and then they can use these certificate lifecycle management services to:

- Comply with multi factor authentication recommendation for strong authentication for transactions initiated and completed via the Internet
- Secure its various card devices with true multi-factor authentication on top of the IdenTrust SSL based certificates. This offers Financial Institutions a unique, comprehensive level of identity authentication and trust differentiates it from any other Internet based approach
- Offer customers identity security across a range of debit card based transactions completed over the Internet in conjunctions with the banks and which meets KYC guidelines
- Establish legally enforceable non-repudiation on any transactions utilizing bank issued IdenTrust digitally signed certificates
- Provide limitation of liability for correspondent banks utilizing these services through a Bank network

IdenTrust will establish and operate an infrastructure in conjunction with a Bank and its device vendors. Additionally, IdenTrust will work with that Bank to secure a chip card issuer and card management system if these have not already been identified. We partner with Gemalto, Safenet, Oberthur, Thales, Texas Instruments, Phillips, Intercede and others for these solutions. The Bank can either issue the cards, or work with the card issuing bank acting as Registration Agent (RA). Those financial institutions electing to not maintain the trusted keys will leave that responsibility to the Bank acting as Certificate Authority (CA)

- **Device Provider** will need to work with the Bank and/or the card issuer (either IdenTrust or the bank acting as CA), to assist in the successful upgrade and rollout of the chip cards and machines. To validate the assumptions made in this proposal, IdenTrust proposes a proof of concept with the Bank, either using EMV based machines deployed in Europe or Latin America, or upgrading a small group of devices and customers in the US. Upon successful completion of that pilot, IdenTrust, the Bank and the device provider will upgrade the existing network to accommodate chip cards.
- **IdenTrust** will work with the Bank and the device provider to develop the appropriate marketing collateral, programs, press and analyst communications and events to increase the market's understanding and awareness of the problem and the solution. Additionally, IdenTrust will work with the Bank to complete a return on investment analysis (completed by a third party) to have real savings and costs quantified.
- **Each FI** customer that wishes to receive the benefits outlined above will serve as a Registration Agent either directly or under the Bank. As such, each FI will confirm the identity of each certificate holder (Person or Device) under the KYC guidelines, for the

purpose of issuing a digital certificate to the cardholder. The Bank issued certificates will work in conjunction with the device based certificates to deliver a truly comprehensive level of trust.

IdenTrust would like set up meetings with appropriate device suppliers and the Bank to discuss this opportunity jointly, review its benefits, and gain agreement to move forward with a pilot. While the market is not demanding this yet, compliance and the increasing awareness by consumers of the vulnerabilities of pin and password for Internet based activities will move the market in this direction. The Bank, in conjunction with IdenTrust and other member banks can lead this market.

It is definitely IdenTrust's goal to make device SSL (secure socket level) certificates, used in conjunction with bank issued IdenTrust Trust Network certificates, a commodity that will differentiate a device supplier when utilized in conjunction with the banks doing the deployment. Meetings are being set up to explore this further and to determine how to assist in bringing EMV standard machines to the US market. Both MasterCard and Visa have expressed an interest in participating in anything that will help to get the EMV standard deployed in the US market, so they can be counted on to help the market make this transition too.

Benefits to the Bank

Utilizing digital certificates as validated customer credentials both in and outside the United States brings strong bottom line benefits to the Bank. Issuing certificates once per customer, and reviewing those credentials on a bank determined schedule, eliminates the need for every product group to perform the vetting and validation exercise. Identity vetting is an enterprise level activity, thus standardizing the process and reducing the opportunity for a fraudster to exploit different methodologies used by different bank departments. This credential card also creates a totally new revenue stream for the Bank. As more activities require identity authentication, the Bank is positioned to charge the party desiring the validation. While initially this may primarily be a service to various governments and agencies, over time, as digital credential use becomes widespread, merchants, schools and non-profits will also require this level of authentication. By deploying the identity credential card at the early end of market growth, The Bank will gain competitive advantage with an innovative solution. The continued expansion in market awareness globally and the fact that the Bank card will be interoperable around the world, makes this card an appealing product both in and outside the US.

Summary

Activities are underway around the globe utilizing digital identity certificates and signatures. While initial focus has been around the business to business transactions and governments with their agencies, increasingly, countries are deploying consumer based programs. This is born out in the programs underway in most of the European countries, Latin America and Asia. Every one of them has to determine how to issue identities and manage them on an ongoing basis. In conjunction with this, these countries are also expanding efforts to address the money laundering programs they have put in place. Most are inadequate to address the expansion of laundering that is resulting from increased deployment of Internet Protocol based networks. Networks that have traditionally been proprietary are moving to the Internet to save costs.

The Bank has a unique opportunity in this environment to supply digital identity certificates and signatures that they issue to their customers based on global KYC standards that countries around the world have accepted. Providing this capability supplies convenience and trust to consumers, governments and corporations. Additionally, it reduces the risk of money laundering through providing transaction tracking tied to a particular identity. This gives the bank a much more comprehensive view to activities, tying them together in a new way to spot trends of suspicious activity. A partnership with IdenTrust and the EMV (PayPass in the US) brings together not only the device manufacturers, but also Visa and MasterCard in an effort to crack down on this fraud.

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.

Corporate Headquarters

IdenTrust, Inc.
55 Hawthorne Street, Suite 400
San Francisco, CA 94105
Telephone: 1.866.IdenTrust (433.6878)
Fax: 1.415.486.2901
www.IdenTrust.com

International Office

288 Bishopsgate, 3rd Floor
London, England EC2M 4QP
Telephone: +44(20)3008.8330
Fax: +44(20) 3008.8331