



Building an Identity Management Infrastructure Today That Will Continue to Work Tomorrow

White Paper
July 2006



ABOUT THIS WHITE PAPER

This white paper describes how the lack of trustworthy Internet identities severely hinders the growth of global electronic commerce and makes the case for corporations and financial institutions to implement an identity management infrastructure that will provide trust assurance across the enterprise. This paper also demonstrates how corporations and financial institutions can create this identity infrastructure while leveraging their existing investments in security and authentication and “future proof” this infrastructure to quickly and efficiently take advantage of new market opportunities resulting from a global identity management infrastructure.

Copyright © IdenTrust, Inc. 2006. All rights reserved.

This document is the intellectual property of IdenTrust, and is protected under the laws of the United States and other countries.

TABLE OF CONTENTS

Challenges for Corporations and Financial Institutions	4
Impact of Increasing e-crime	4
Impact of Lost Business and Revenue Opportunities	5
Impact of Legislation	5
Historical Perspectives: Good in Theory, Falling Short in Practice	7
The Bottom-Up Approach with PKI	7
The Reactive Approach with Two-Factor Authentication	7
The Token Solution	8
Future Proofing: Implementing an Identity Infrastructure that is Financial Institution Issued, Backed, and Globally Interoperable	9
The Need for Both-Way Authentication	9
Financial Institutions Take Charge	9
The IdenTrust PLOT	10
Addressing a Wide Variety of Threats	10
Conclusion	11
About IdenTrust	11

The technological contest between phisher and counter-phisher is well and truly underway. It is a contest of escalation.

— David Jevans,
APWG Chairman

CHALLENGES FOR CORPORATIONS AND FINANCIAL INSTITUTIONS

Identity management continues to be a challenge for corporations and financial institutions of all shapes and sizes. For example, phishing and pharming attacks are becoming more numerous and the methods of attack more sophisticated. Forget the image of the lone hacker waging attacks from his or her dorm room; the modern fraudster is extremely technically advanced, well-funded, and incredibly adept at finding and taking advantage of security weaknesses.

Other forces are also causing corporations and financial institutions to re-think their identity management infrastructures: the impact of lost business and revenue opportunities and the never-ending pressure of new legislations.

Impact of Increasing e-crime

The increase in e-crimes using techniques such as phishing, keylogging, and Trojans is alarming. However it's not just the quantity of attacks that are increasing, but the aggressiveness and technical sophistication of the fraudsters. Says David Jevans, Chairman of the Anti-Phishing Working Group (APWG): "The technological contest between phisher and counter-phisher is well and truly underway. It is a contest of escalation."

Although phishing and pharming attacks are a concern for corporations, the majorities of attacks are waged against financial institutions and are increasingly focused on smaller institutions such as community banks and credit unions since that's where the "easy money" is. (APWG reports that the financial services industry suffers 92 percent of all attacks.)

The Bank Administration Institute (BAI) reports that fraudsters have become particularly aggressive in running phishing scams that target small and mid-sized banks. APWG data also supports this opinion: the number of unique brands hijacked increased from 92 in April, 2006 to 137 in May, 2006 – the most different brand types ever recorded by the APWG.

Projections are that phishing attacks against corporations and financial institutions will continue to increase, stunting e-commerce growth and preventing electronic services and commerce to reach critical mass. In the May, 2006 Phishing Activity Trends Report, APWG reports 20,019 unique phishing attacks, a gain of almost three thousand attacks from April and the most ever recorded by the APWG. The number of unique phishing websites detected by APWG was 11,976, an increase from April and again the highest number ever recorded by the APWG.

Money laundering is also on the rise. The Financial Crimes Enforcement Network (FinCEN) reports in the May, 2006 edition of The SAR Activity Review – By the Numbers that Suspicious Activity Reports (SAR) filed by depository institutions that identity potential money laundering increased by 37 percent from 2004 to 2005.

But since money laundering is an illegal activity which occurs outside reported economic and financial statistics, it's difficult if not impossible to quantify the economic impact of money laundering. However, the International Monetary Fund (IMF) has stated that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world's gross domestic product.

Impact of Lost Business and Revenue Opportunities

Obviously, decreasing or eliminating crimes related to identity is a goal of every corporation and financial institution. But the benefits of a comprehensive identity infrastructure encompass more than protection from criminals – the benefits also include the ability to conduct e-business globally, uncover new revenue opportunities, and improve operating efficiencies.

A global identity authentication infrastructure, for example, would enable corporations to rely on the authenticity of digital signatures for purchase orders, invoices, compliance, and other types of documents and finally automate the last part of the supply chain whether they are doing business in the same country or across borders. Financial institutions could leverage their position as a trusted third-party in the traditional off-line world and offer new, fee-based services as a trusted third-party issuer of digital certificates in the online world. Multi-national corporations with relationships with financial institutions in many parts of the world would be able to open and close accounts electronically and financial institutions would have full confidence that the digital signatures are secure and have not been compromised.

Secure identity management would also create opportunities for Reverse Factoring, a type of financing that relies on trusted third-parties. For example, purchasers can use third-parties such as financial institutions to verify the trustworthiness of suppliers, facilitating financing and e-commerce between entities not known to each other.

Impact of Legislation

In an attempt to thwart e-crimes, regulatory bodies have stepped forward to issue stronger guidelines and legislation for corporations and especially for financial institutions.

Getting the most recent media coverage is the Federal Financial Institution Examination Council's (FFIEC) *Authentication in an Internet Banking Environment* guidelines that state that single-factor authentication is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. But other legislation such as the USA PATRIOT Act, Sarbanes-Oxley Act, Single European Payment Area (SEPA), Markets in Financial Instruments Directive (MiFID), Know Your Customer (KYC), and Know Your Customer's Customer (KYCC) also weigh in favor of a multi-factor approach to security.

And other regulations are pending. For example, the Office of Management and Budget (OMB) recently required U.S. government departments and agencies to adhere to the National Institute of Standards and Technology (NIST) recommendations for protecting information with a device separate from the computer. If passed, the Bennett-Carper Data Security Act of 2006 will require financial institutions to notify customers of any type of information breach regardless of whether or not it affects customer information.

Other pending data breach legislation includes the Financial Data Protection Act, the Data Accountability and Trust Act, the Identity Theft Protection Act, and the Personal Data Privacy and Security Act. The theme is clear: protect customers from identity theft and other e-crimes by toughening up standards for corporations and financial institutions.

The federal government will continue to develop regulations aimed at protecting the online banking industry from phishing, yet this will most likely be at a pace that lags far behind that of new identity theft developments.

— Sally Hudson
IDC Analyst

ONE CHANCE, MAYBE TWO...

So just how tenuous is a financial institution's reputation? According to the Ponemon Institute's 2006 Privacy Trust Study for Retail Banking, banks are only one or two security breaches away from losing their customers. While 68 percent of customers give their bank high marks for protecting their personal information, those customers report that only two security breaches would destroy that trust. Thirty-four percent of respondents would transfer their funds after a single security breach; 45 percent after two security breaches.

Once trust is lost, consumers will transfer their accounts to a different financial institution.

Fifty-eight percent of those consumers surveyed said that a security breach would decrease their sense of trust and confidence in the organization reporting the incident. Only 8 percent of respondents did not blame the organization that reported the breach. Surprisingly, 12 percent said the incident enhanced their sense of confidence in the organization.

And if you think the answer to mitigating reputational risk is to keep mum on minor security breaches, think again. According to the Ponemon Institute, more than 82 percent of consumers believe that an organization should always report a breach, even if the lost or stolen data was encrypted or there was no criminal intent.

REPUTATION KEEPS BANKERS UP AT NIGHT

The good news is that financial services executives are beginning to take notice of the impact of reputational risk. According to the 2004 PricewaterhouseCoopers study, *Managing Risk: An Assessment of CEO Preparedness*, financial services executives now regard reputational risk as the greatest threat to an organization's market value. According to the study, 28 percent of financial services bosses felt that reputational risk was a significant threat and 13 percent felt it was one of the biggest threats they face.

When asked which was a larger threat to their financial institution: known risks such as credit risk or unknown risks including reputational risk, 57 percent were most concerned about unknown risks.

Which areas of risk represent the greatest potential threat to your organization's market value and earnings? (% of respondents rating as top area of focus; rank in brackets)

	Market Value	Earnings
Reputational risk	34% (1)	22% (6)
Credit risk	25% (2)	37% (1)
Market risk	25% (3)	31% (2)
Regulatory risk	18% (4)	25% (3)
Business/strategic risk	16% (5)	23% (4 tie)
Operational risk	14% (6)	23% (4 tie)
Business continuity risk	13% (7 tie)	13% (8 tie)
IT/technology risk	13% (7 tie)	8% (10 tie)
Treasury/liquidity planning	10% (9)	19% (6)
Governance risk	7% (10 tie)	13% (8 tie)
Sovereign/political risk	7% (10 tie)	8% (10 tie)

HISTORICAL PERSPECTIVES: GOOD IN THEORY, FALLING SHORT IN PRACTICE

While there have been well-funded and technologically advanced approaches to combat e-crimes such as PKI and tokens, none have really taken hold. Understanding why previous approaches to identity authentication have not been as successful as they could have been enables corporations and financial institutions to implement an identity infrastructure that bypasses these shortcomings.

The Bottom-Up Approach with PKI

One of the first and most promising technologies to address identity management is Public Key Infrastructure (PKI). PKI has been around since the mid-1970s and has been used successfully in large-scale implementations such as by the U.S. Department of Defense (DoD). One of PKI's strengths is that it can also be used to authenticate digital signatures, making them legally binding. However, one reason PKI hasn't become more ubiquitous is because few business applications require identity authentication with digital certificates and signatures.

While a robust technology, PKI implementations have historically resulted in fragmented, siloed security and identity management that did not easily support interoperability. To bring true value to government agencies, corporations, and financial institutions, a PKI-based infrastructure must have interoperability both with other systems and with other countries' government mandated schemes. Additionally, it must be able to rely upon the policies and procedures used for issuance of the certificates.

The Reactive Approach With Two-Factor Authentication

As e-crimes such as phishing, pharming, and money laundering proliferated, corporations and financial institutions looked to decrease their risk of attack. In their haste to install security measures quickly, many implemented solutions such as passwords coupled with another type of identification.

But corporations and financial institutions have discovered that these solutions fall short. For example, a password coupled with individualized graphical images does not protect against man-in-the-middle attacks because fraudulent sites can be inserted into the workflow through techniques such as phishing, thus compromising the data being transferred. To protect against man-in-the-middle attacks, the user must be authenticated to the site as well as the site being authenticated to the user.

For example, a recent man-in-the-middle attack involving a large, multi-national financial institution highlights the shortcomings of one time passwords, a type of two-factor authentication. In this attack, the criminals spoofed the token key hardware used by the bank's customers to generate one-time passwords, tricking the customers into entering their passwords into website forms that the criminals then used to enter the real website.

In a more low-tech approach, thieves can easily steal PINs by looking over a victim's shoulder and the victim is unaware of the theft until a crime is committed.

To protect against man-in-the-middle attacks, the user must be authenticated to the site as well as the site being authenticated to the user.



The Token Solution

While analysts and security experts agree that the most secure approach to identity authentication is to provide users with a device that belongs solely to them – such as a smart card or a token – the arguments against these devices include that users will not want to use a device, that devices are expensive, and that devices can be easily lost or misplaced.

However, those arguments are no longer valid. Devices such as iPods and other gadgets that make use of USB ports are common and can easily serve double-duty as security devices. The only missing link is an easy, inexpensive way to educate users and transition them to using more secure devices such as tokens, USB devices, or smart cards.

Although this paper focuses on the business-to-business need for identity management, most corporations and financial institutions are also concerned about the impact of identity authentication on their consumer customers. And while study after study confirms that consumers are nervous about Internet fraud and identity theft, consumers also understand that the financial institution bears the liability should they suffer monetary losses due to identity theft. Financial institutions offer little incentive for customers to sign up for digital certificates and signatures since few applications demand them for authentication. The case for trust is not being made strongly enough! Financial institutions are skittish about enforcing device-based security without being able to show customers value-added services and benefits in return.

However, lack of interest in devices is not the case with commercial customers who are beginning to demand these devices for business applications such as global account management. Entities involved in supply chain commercial transactions are liable for greater losses and are more eager to implement the utmost in security, even if that means managing hardware devices. The good news for financial institutions is that as more and more corporate employees become comfortable with tokens and smart cards, that acceptance will filter down into their consumer habits as well.

IdenTrust was created to enable one trusted entity to issue certificates through trusted financial institutions.

FUTURE PROOFING: IMPLEMENTING AN IDENTITY INFRASTRUCTURE THAT IS FINANCIAL INSTITUTION ISSUED, BACKED, AND GLOBALLY INTEROPERABLE

As discussed earlier in this paper, most identity authentication solutions only provide a piece of a comprehensive approach to identity security. For example, corporations and financial institutions have already implemented an array of security measures to address everything from physical access to single sign on and provisioning. They now need to focus specifically on identity authentication.

To have the flexibility to respond to each new type of fraud and resulting regulation, a comprehensive approach to trust needs to offer a spectrum of products that provide varying degrees of trust. It's nearly impossible to predict identity authentication needs in five years, one year, or even next month.

Need Both Way Authentication

While it is promising that the first steps have been taken in the U.S. to comply with guidelines such as those from the FFIEC and other legislation, most of those steps have been to authenticate the user to the site, not the site to the user. Corporations and financial institutions must do both, and, they must then sign both the data and the container in which it is transported.

In Europe, both SEPA and MiFID will require identity authentication for securing each leg of a cross-border transaction. All of these approaches benefit from the Know Your Customer approach that financial institutions have plus the liability limitations that are inherent in bank-owned schemes such as SWIFT, MasterCard and Visa. Lastly, global schemes require global interoperability.

Financial Institutions Take Charge

In the late 1990s a group of large, global financial institutions decided it was time to address the problems inherent in a global, electronically connected environment such as the Internet. These institutions understood the benefits of creating a globally interoperable identity authentication infrastructure that was based upon financial institution regulations (the most stringent, comprehensive and global in the world governing financial transactions) and practices. To create this infrastructure, these institutions designed a community of trusted participants and relying parties. They also capitalized on the role that financial institutions have always played in trusted commerce.

IdenTrust was created to enable one trusted entity – in this case IdenTrust – to issue certificates through trusted financial institutions that act as certificate authorities and in turn issue certificates on behalf of other financial institutions or directly to customers.

It is the combination of all of these capabilities - policies, legal framework, operations, and technology (PLOT) -- that makes IdenTrust the most comprehensive solution available.

The IdenTrust PLOT

Core to IdenTrust is “PLOT:” policies, legal infrastructure, operations, and technology upon which members rely. When IdenTrust was created, the members recognized the need for policies, procedures and guidelines that would be able to work across multiple institutions and borders. The resulting rule set has stood the test of time, governments, and multiple banks.

But for identity authentication to really provide the trusted environment customers require for doing business, the legal framework had to be acceptable both domestically and cross border. IdenTrust member banks work with their governments to obtain legal acceptance, thus facilitating cross border interoperability.

For an individual bank to deploy this infrastructure, the institution must incur a great deal of expense. To eliminate this barrier, IdenTrust launched a hosted service which is yearly audited to outsource the products, services, and customer support required for certificate issuance and validation.

Lastly, to simplify banks’ deployment with customers, IdenTrust has certified a number of USB Tokens, Smart Cards and software-based methods for authentication of the certificates. This means that “out of the box” these products work with the IdenTrust solutions.

It is the combination of all of these capabilities – policies, legal framework, operations, and technology (PLOT) -- that makes IdenTrust the most comprehensive solution available. Competitors provide one or more of these pieces, but only IdenTrust provides them all and can deploy them from a single internal application through global communities. PLOT is the only way to insure complete protection against the entire spectrum of fraud attacks.

Addressing a Wide Variety of Threats

Membership in the IdenTrust network provides financial institutions access to a comprehensive suite of products and services. The network is designed to accommodate additional features and functions provided through trusted partners that support expanded regulations as well combat against new types of e-crime.

For example, membership in the IdenTrust network protects against insidious man-in-the-middle attacks that can bypass standard two-factor authentication by validating IdenTrust certificates against a real time updated list that indicates whether or not the certificate has expired or been revoked.

IdenTrust is regulated in the same way that financial institutions are and is subject to the governmental standards and regulations within the geographic regions where financial institutions are members. As a result, IdenTrust can act as relying parties for the transfer and authentication of identities across the global Internet.

By implementing a security infrastructure that can support a complete set of operational, logistical, network, and technical capabilities, financial institutions can provide identity assurance to other government and corporate entities as well and minimize the cost of deploying multiple infrastructures that must then be integrated and coordinated.

CONCLUSION

Without a globally interoperable approach to identity authentication, crimes such as identity theft and money laundering will continue and global e-business will never fulfill its promises. New, innovative, and technically sophisticated technologies will also continue to be delivered to prevent and control these crimes and help apprehend these criminals. Scaling the Internet to deliver true e-commerce will not be possible without addressing identity authentication.

Legislation is continually being enacted to keep up with new crime threats. For now, the FFIEC guidelines remain just that – guidelines – but there is little doubt that multi-factor authentication will eventually become law. While SEPA and MiFID are also still being finalized, financial institutions across Europe are allocating resources to focus on implementation of these two directives. These directives will evolve into legislation and regulation and be supplemented by additional requirements to respond to a dynamic market.

What's needed is a phased approach to identity authentication that will work today and be able to be expanded and strengthened as needed rather than implementing a solution that works for a time but then must be retrofitted to protect against more sophisticated attacks.

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