

Identity Authentication as a Critical Growth Strategy



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

TABLE OF CONTENTS

Introduction	3
Standards Address Infrastructure Issues	3
Integrating Physical and Financial Supply Chains with Standards	4
The Case for Double Signing	4
IdenTrust: Individual Accountability	5
The IdenTrust PLOT	6
The IdenTrust Rule Set	7
Combining Security and Privacy	8
Summary	9

INTRODUCTION

No matter the size of the company, its industry or its location, e-commerce is critical to running a business. Today, e-commerce includes not only financial transactions but other types of transactions such as government contract bidding, electronically sending shipping information, and exchanging business-critical emails.

But there are glaring business risks in doing e-commerce. Having a corporate identity stolen and fraudulently used is just one danger. Without a global standard for liability, companies may inadvertently do business with unsavory parties without the opportunity for legal recourse. In addition, the time spent authenticating transactions creates costs, delays receipts and generally undermines business confidence.

Within the e-commerce landscape, identity authentication presents businesses with both challenges and opportunities.

The Economist Intelligence Unit (EIU), with sponsorship provided by IdenTrust, asked corporations from around the globe about their strategies, tactics, successes and challenges pertaining to identity authentication. The goal was to determine the role of digital identity authentication in e-commerce.

The survey results were presented by Jackie Wiles, Contributing Editor, EIU, in a web seminar. In addition, Raffi Basmadjian, Deputy Treasurer of France Telecom and Milton Santiago, Senior Vice President of Electronic Banking at Chicago-based LaSalle Bank discussed the impact of identity authentication at their organizations.

The contents of this paper were derived from that web seminar.

Major Study Findings

The major study findings include:

- Corporations need an identity authentication infrastructure to support global business growth.
- Most corporations are very concerned about reputational risk due to fraud.
- An identity authentication infrastructure must include global, multi-party acceptance.
- Those corporations not using digital certificates report that government restrictions on usage, the lack of globally accepted certificates and the inability of these certificates to interact with corporate systems are the major reasons for non-use.
- Identity authentication is a senior management rather than an IT issue.

About the EIU Global Online Survey

In January 2007, the EIU sponsored by IdenTrust surveyed 246 global corporate executives on their corporate digital authentication practices. Twenty-four percent of the respondents were from western and eastern Europe; thirty-eight percent were from the Americas and thirty-eight percent were from the Asia-Pacific region or elsewhere. About half of these executives were from companies with annual revenues greater than \$500 million (USD).

SURVEY RESULTS

Strategic Implications of Identity Authentication

Identity authentication is a two-way street: companies need to determine whether or not a counterparty in cyberspace is a trusted party and they need to be recognized as trusted parties themselves. They must identify who they are communicating with at the same time they protect their own identity. For example, transactions such as bidding for government contracts demand anonymity and privacy at the same time that any documents or parties to a transaction are authenticated. This balancing act of maintaining anonymity and privacy while verifying identities is particularly difficult when transacting business cross-border.

Companies realize the benefits of identity authentication and the role it can play in their business. The EIU study results show that many companies believe that an effective identity authentication strategy can support global business growth, eliminate redundancy, reduce manual intervention, reduce costs and better position their company to exploit market opportunities.

These companies look at identity authentication as more than a legal imperative: if they can make identity authentication a seamless part of their business process or at least make sure it doesn't stand in the way of e-commerce, they will improve their business.

Only one-fifth of the survey respondents answered 'no' when asked if more effective identity authentication would enable their business to grow more rapidly over the next three years. Surprisingly, 35 percent said they don't know the impact of effective identity authentication. Chances are that these respondents have succumbed to being paralyzed by identity authentication issues. (See figure 1.)

If identity authentication were more effective, would that enable your business to grow more rapidly over the next three years?

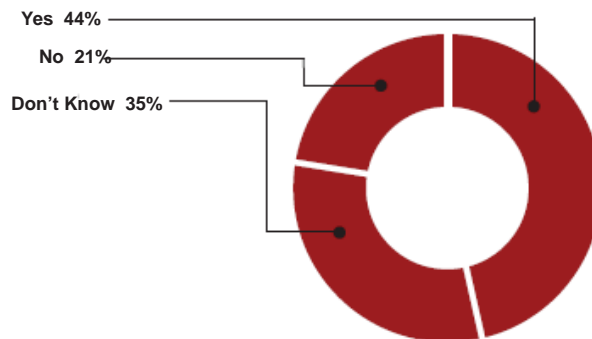


Figure 1

Source: Economist Intelligence Unit Survey

Underscoring the importance of identity authentication to business growth, most companies consider their identity authentication strategy a senior management issue. Seventy-six percent of respondents say that a senior executive, often the chief information or technology officer, is responsible for governance of identity authentication strategies.

The IdenTrust Solution: IdenTrust supports global business growth by turning the Internet into a highly secure virtual private network.

The proprietary IdenTrust rule set establishes a legally binding framework and creates an interoperable identity authentication and validation process for all transactions and documents. Unlike other identity authentication systems that rely on public law, IdenTrust identities are globally interoperable under uniform private contracts recognized in countries around the world.

▶ The Landscape Grows More Complex

It's clear from recent trends that global business will continue to become more complex and increasingly electronic. The importance of identity authentication is likely to grow as e-commerce continues to thrive. More than half of the survey respondents expect to use more suppliers and three-quarters expect to deal with more customers within the next three years. Electronic payments are also likely to rise: 31 percent of respondents say that more than 75 percent of their receivables will arrive electronically within three years.

But there are risks, which survey respondents are well aware of, that extend beyond monetary loss. Other very real risks cited by respondents include unauthorized use of proprietary or competitive information, identity theft, and reputational risk. (See figure 2.)

What are the greatest e-commerce security threats your company faces today?

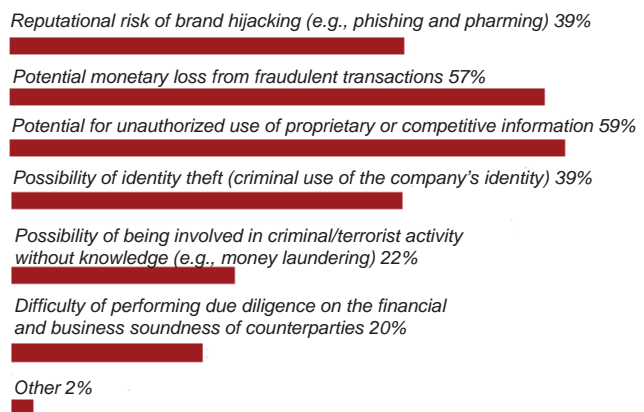


Figure 2

Source: Economist Intelligence Unit Survey

The IdenTrust Solution: To mitigate the risks of reputational, monetary and other types of risks, an identity authentication strategy must ensure the security of financial transactions as well as the company's reputation, data and other intellectual data. To simplify adoption and ensure trusted identity authentication, IdenTrust's operations are audited with the same stringency applied to financial institutions. End-to-end activity tracking for regulatory compliance is a key part of the IdenTrust value proposition.

Identity Authentication Challenges

The challenges corporations face surrounding identity authentication are two-fold: conceptually getting their hands around the problem and then implementing the selected solutions.

Conceptual Challenges

According to survey respondents, conceptual challenges surrounding identity authentication still exist. For example, since e-commerce encompasses much more than financial transactions, businesses find it difficult to begin the process of creating an identity authentication infrastructure and prioritizing their efforts and budgets. They do not want to reinvent the wheel, but rather to utilize lessons learned and proven solutions.

Implementation Challenges

Even once a business determines the appropriate identity authentication strategy, they still face implementation challenges. These challenges include knowing where to go for help and understanding the technology solutions that are available.

According to the EIU, companies should look to existing trusted advisors for identity authentication support. Any solution provider should understand the challenges of authentication across borders and in governmental interactions. They should be committed to standards, global interoperability and multi-party acceptance. They should also explicitly guarantee to validate counterparties, protect transactions, privacy and data, and offer non-repudiation and globally enforceable legal contracts.

The EIU concluded that banks are a natural partner and advisor in authentication strategies.

The IdenTrust Solution: The IdenTrust operational environment was defined by financial institutions. The Policies (P), Legal infrastructure (L), Operational standards (O), and Technology for access (T) leverage the legacy of public trust in financial institutions as commercial intermediaries. Banks have always vouched for customers who are strangers to each other and customer identity is a core feature of all banking services. Thus, it is easier to integrate and deliver trust-related products and services with other financial institutions. This enables businesses to expand their spectrum of compliance more rapidly, maintain their privacy (they are not sharing information with an unknown third-party) and feel confident that they can trust the integration of certificate technology such as smart cards and encrypted USB drives easily.

Certificate Usage and Shortcomings

Internet-based digital certificates are used for a variety of interactions between companies and local or national government agencies. Almost half of the respondents have experience with Internet-based digital certificates. (See figure 3.)

Does your company currently employ Internet-based digital certificates for e-commerce communications or transactions?

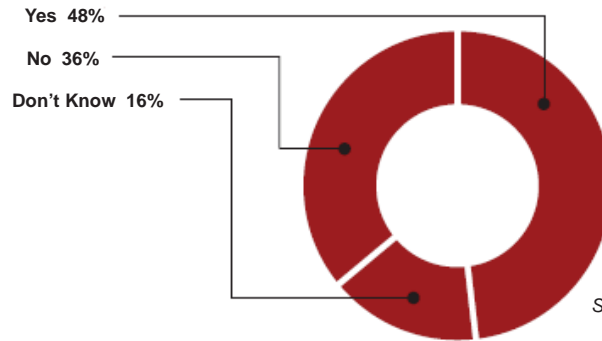


Figure 3
Source: Economist Intelligence Unit Survey

Of the survey respondents who use digital certificates, 48 percent uses these certificates for electronic corporate tax filing and 44 percent use them to file sales taxes such as value-added tax.

According to the EIU, corporations using digital certificates are largely happy with the security that these certificates provide: of the 65 percent of respondents who use banks and private providers as the certifying authority for Internet-based digital certificates, 49 percent of these users are pleased.

Unfortunately problems with Internet-based digital certificates still hamper their use. Many of these problems are related to the inability of certificates to function across borders and be globally accepted. Forty-four percent of respondents say that the biggest disadvantage is that the certificates are not globally accepted. Thirty-seven percent say that Internet hosting is not secure enough and thirty-seven percent say there is no legal infrastructure for contracts supporting digital signatures across borders. (See figure 4.)

What do you see as the biggest disadvantages with existing Internet-based digital certificates (whether you currently use them or not)?

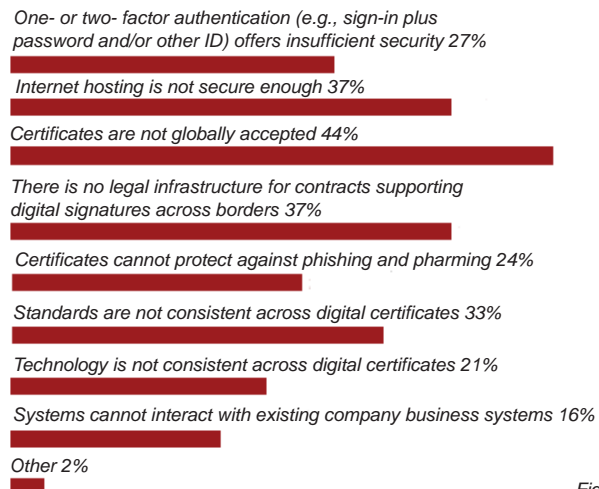


Figure 4
Source: Economist Intelligence Unit Survey

The IdenTrust Solution: IdenTrust addresses the concerns of governments, corporations and financial institutions with PLOT: policies, legal infrastructure, operational standards and technology for access. Other identity authentication providers focus only on the technological access issues rather than the full range of identity authentication challenges.

For example, IdenTrust policies govern 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. In addition, IdenTrust uses open standards-based technology in a unique, proprietary manner to ensure even higher levels of security. IdenTrust identities also encrypt and control the process flows, ensuring that no one can intercept or redirect the transaction or document, eliminating both phishing and man-in-the-middle attacks.

The Ideal Identity Trust Infrastructure

When corporations were asked to describe an ideal identity trust infrastructure, the top responses were that digital signatures and credentials should be legally binding around the world (43 percent), be able to guarantee multi-party, multi-bank transactions across borders (40 percent) and provide a seamless user experience (30 percent). (See figure 5).

What would be the greatest business benefits of using the ideal identity trust infrastructure?

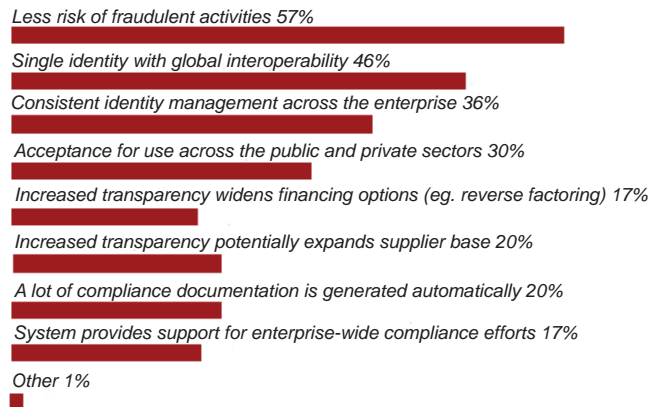


Figure 5

Source: Economist Intelligence Unit Survey

The IdenTrust Solution: A unique benefit of the IdenTrust approach is that a single identity can be used across multiple institutions and multiple applications running in multiple environments. That same identity is legally binding in more than 175 countries around the world. Only the total combination of the PLOT components provides a comprehensive solution to risk management in digital transactions.

SUMMARY

Although they understand the critical nature of identity authentication, many corporations are frustrated by the lack of global authentication standards that are legal binding and handled in the same way in multiple environments. Without this, they are limited in the business they can transact cross-border. Keeping corporate management up at night are issues such as the threat of reputational risk, accountability down to the individual, the headache of managing multiple identities with the parties they do business with, and the lack of standard identity authentication. Without solutions, these issues will continue to impede the growth of their business.

The survey respondents' ideal identity authentication infrastructure includes global operability, a globally accepted legal framework, and an easy-to-use interface, all of which are provided by IdenTrust.

//
We need standardized digital identity management. //

//
It's not easy to find a solution which is accepted around the world. Technology is not the problem. Standards are the problem since they are local or national in nature. //

Case Study: France Telecom: The Search for Standards

A large multinational corporation, France Telecom has a geographic presence in 94 countries and operates in more than 200 countries, explains Raffi Basmadjian, Deputy Treasurer. As a result of these global operations, the company's centralized group treasury department must transact business with a wide variety of financial institutions in different countries. Many of these institutions are smaller, local banks. It's critical that France Telecom be able to communicate with these institutions securely using globally accepted digital identity management, says Basmadjian.

To solve its identity authentication challenges, France Telecom developed an identity management platform based on the SWIFT network. Although the network allows for secured messaging between France Telecom and the banks, it does not provide digital identification of the individuals initiating and receiving the transactions.

"We need a legally binding method that allows us to work with small local banks yet provide the same type of digital certificates and identity structure as the large institutions since it's very difficult for us to manage 94 different types of digital identities," he says. "We need standardized digital identity management."

The answer will be to add digital certificates and identity management to identify each user individually on top of the secure SWIFT network using the IdenTrust Trust Infrastructure.

According to the EIU survey results, many corporations recognize the need for identity authentication, but often these organizations are unsure of how to start the process and how to prioritize what is most important for securing their unique business. They must also address the issue of the identity management initiatives becoming relegated to IT as opposed to being viewed as a top-level strategic initiative requiring executive management support and sponsorship.

"At France Telecom, a security policy provides the framework for what we need to do to protect our assets," explains Basmadjian.

Although they have a clear idea of what they need to protect the company, it has been difficult to find an identity authentication solution that meets France Telecom's requirements. "There are very good certificates available in the market, but the trouble starts when you have to secure a company over a large geographic area as we do," says Basmadjian. "It's not easy to find a solution which is accepted around the world. Technology is not the problem. Standards are the problem since they are local or national in nature."

France Telecom, through its partnership with BNP Paribas, has found a globally interoperable solution with IdenTrust. France Telecom will use the IdenTrust identity authentication solution to significantly reduce operational costs as well as mitigate the risks of doing business in an electronic world.

“If we don’t have a commercially reasonable, user-friendly identity solution that requires very little IT support, we will lose that sale.”

“As a financial provider to corporate practitioners, our identity is sacred. If our identity is compromised, our trust is lost.”

Case Study: LaSalle Bank: Keeping Financial Arteries Clear

LaSalle Bank’s customer base consists of a broad spectrum of corporate clients: both large, multinational corporations as well as small and mid-sized businesses (SMB). The challenge in supporting SMBs, explains Milton Santiago, Senior Vice President of Electronic Banking, is that these organizations lack the IT resources or expertise to support a complex identity authentication infrastructure that would provide them with the levels of security that they need.

LaSalle Bank provides what Santiago calls “financial arteries” to these smaller customers that enable them to manage funds with the utmost security. “These systems are how our customers know and trust our bank,” explains Santiago. “Any blockage in these financial arteries means a blockage in how they manage their funds and exposes them to financial risk.”

“If we don’t have a commercially reasonable, user-friendly identity solution that requires very little IT support, we will lose that sale,” he adds. “Having an identity strategy that is simple to implement is critical for all of us to stay in business.”

Santiago believes that an ideal identity trust infrastructure should enable e-commerce transactions as seamlessly as credit card transactions. “Credit cards are accepted anywhere in the world and come with a high level of trust,” he explains.

The industry still needs education, says Santiago, calling “knowledge our strongest weakness.” He says that organizations of all sizes are largely unprepared with a sound identity management solution. “We have been working on educating the industry about the important of implementing an identity management solution,” he adds.

LaSalle Bank’s commercial-strength identity management solution identifies the banks’ customers, technology providers and its partner banks. The bank takes a consultative approach to helping these entities resolve their identity management challenges and working with any identity authentication schemes already in place.

“Take the time to educate customers,” advises Santiago. “Technology is not the limiting factor; I have never seen technology limitations. But education and common-sense business practices can be more important than the technology itself.”

Santiago uses the example of employees accessing their personal email accounts while at work as a security threat that is often overlooked. “This is where identities are compromised and your brand is exposed, but most people don’t think about email,” he warns.

Even as a financial institution, the risk of monetary losses is just one danger. “Reputational risk really concerns us,” says Santiago. “As a financial provider to corporate practitioners, our identity is sacred. If our identity is compromised, our trust is lost. We spend a lot of time and resources ensuring that our identity is not compromised.”

Santiago likens identity theft to catching the common cold. “When you get a cold you’re often not even sure when or how you got it. It’s the same with identity theft. We need to make sure our customers are immune to these types of threats in order to secure our customers’ trust.”

He also recommends not waiting for governmental regulations to push organizations toward global identity authentication, saying that governments tend to be slow to react. “Base your identity authentication on your business strategy rather than waiting for government regulations to catch up. Be proactive rather than a follower,” Santiago advises.

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, 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
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