Entrust®

Securing Digital Identities
& Information

Cyber Security Collaboration:
A Critical Ingredient for Worldwide Security

November 2003

Entrust®
Securing Digital Identities
& Information

Table of Contents

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc or Entrust Limited. All other company and product names are trademarks or registered trademarks of their respective owners. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

1 Introduction

During the 20th century, security was largely the responsibility of national governments, which waged conventional warfare on well-defined battlefields against a clearly identified enemy. The threats of transnational terrorism and cyber warfare overturned that calculus. Although we are still developing responses to these new threats, it is clear that business is now on the frontlines of conflict and must cooperate with government to incorporate new security measures into its governance procedures. As a result, three new global imperatives have emerged:

- No nation can rely on inward-looking, unilateral strategies to protect itself.
- With the private sector controlling the vast majority of the world's critical infrastructure systems that underpin our economy – from energy and telecommunications to financial services and healthcare – physical and economic security will depend on effective, global collaboration between government and industry.
- Since so much of our critical infrastructure and economy is dependent on information networks, cyber security has assumed a new importance. Increasingly, there is no physical or economic security without effective cyber security.

The international community and the private sector must be closely involved in the planning and deployment of new worldwide security initiatives to protect physical, human and economic assets. To initiate this process, the EastWest Institute has convened an ongoing, high-level dialogue among European, U.S. and international government officials, corporate executives, and industry experts, to establish a forum on collaborative, worldwide security. Entrust is proud to be part of that process and dialog.

2 Cyber Security

2.1 Cyber Security: The Vital Link

The establishment of worldwide security is far more complex than the application of greater physical security. The critical infrastructures (e.g., dams, power grids, pipelines, ports, financial centers, etc.) that power our economies and daily lives are now inextricably linked to powerful information systems. Damage to these systems would cause vast economic harm. Yet, the resources to protect them have not been extended on a worldwide scale to secure many of these information networks.

The reality of today's global threats is that attacks against critical infrastructures do not require physical access to targets to inflict great harm. In fact, persons bent on destruction could potentially carry out harmful economic or physical attacks from the comfort of their homes — anonymously and thousands of miles away.

According to Carnegie Mellon's CERT Coordination Center, the number of reported vulnerabilities, where software features create opportunities for malicious disruption, continues to double each year since 2000 – jumping from nearly 22,000 incidents for all of 2000 to 76,000 in the first half of 2003 alone. More alarming, industry experts contend that the actual numbers are much higher, considering that countless incidents go unreported by governments, corporations, and citizens.

The risk will only increase as businesses and governments bring more of their operations online to benefit from the increased productivity and cost efficiencies inherent in e-commerce and e-government. Unless enhanced cyber security is embraced throughout management chains and incorporated into all IT infrastructures, the true potential of the Internet and benefits to worldwide security will never be realized. Much like any physical or economic infrastructure, the security of any IT infrastructure is only as strong as its weakest link. And enhanced cyber security serves as the vital link in protecting the physical and economic elements of worldwide security.

In short, without cyber security, there is no physical or economic security.

2.2 Cyber Security: The Global Challenge

Traditionally, most organizations have focused primarily on securing the perimeters, or “borders” of their critical infrastructures through deployment of firewalls, intrusion detection, and anti-virus software. While these are important and necessary elements of protection, they are inherently limited in an environment that must enable secure access and respect the rights of citizens. As businesses and governments move online and exchange sensitive information and data with customers, partners, and employees, organizations must be able to identify with whom they are doing business and ensure that information is adequately protected. Confidently managing secure digital identities and information in a cost-effective, easy-to-use manner must serve as a critical management tool for organizations hoping to realize the productivity benefits and cost efficiencies of the Internet and technology applications.

Governments and industry worldwide must join together in an unprecedented way to actively protect the critical infrastructure and information systems that underpin our economy. Industries need to step up their security to address new cyber threats and protect their customers, suppliers, employees, and shareholders. And government must strengthen its own information systems to both protect sensitive data and establish secure information sharing. Government must lead this effort, providing the necessary incentives and leadership to encourage industries to adopt security standards and practices embraced by the world community.

Extrapolating these challenges globally will not be easy, but it will be necessary to meet the physical and economic imperatives essential for worldwide security. Three priority areas in which governments and industries must immediately work together to establish greater cyber security include:

- **Identity Management**
- **Secure E-government Services**
- **Corporate Information Security Governance**

Each of these areas is an effective pillar in addressing cyber security and when taken as a whole, will promote government and industry cooperation and adoption on a global scale.

3 Identity Management

In the past, transactions most often happened during face-to-face interaction, or between parties that knew each other well. The Internet has vastly widened the opportunities to do business with potential customers and partners in a "faceless" society. The faceless nature of these transactions has introduced new vulnerabilities and made the need for secure digital identities a requirement. Digital identities can provide the identity assurance required for system and application access and secure communication.

What is a digital identity? A digital identity is an electronic identity secured by a digital certificate. The issuance and lifecycle management of digital certificates can be provided through Public-Key Infrastructure (PKI). PKI efficiently and effectively manages digital certificates and has been proven to be highly interoperable, scalable, and manageable. PKI is a fundamental enabler of secure digital identity and provides the foundation for secure e-business and e-government transactions.

Digital identities, based on digital certificates, provide a higher level of information security. "Basic" Web security — pin and password identification — is not sufficient to meet the extensive business requirements of large organizations for comprehensive digital identity and information security. The limitations of pin and password restrict the ability of organizations to fully leverage the potential of the Internet and enterprise applications to improve productivity.

Governments have been the traditional source for identity documents. For example, in the U.S., driver's licenses have evolved into a de facto national ID, although that was never their original purpose. Other nations, such as Spain, have national ID cards that are used for both government and commercial uses. Governments also issue passports, birth certificates, or similar documents to enable travel across national borders. Government, as a trusted source of identity, has a key role to play in the Internet world in providing digital passports and driver's licenses for a new digital generation.

Enterprises also issue identity credentials, including employee badges and network access devices such as smartcards. Increasingly, enterprises are extending these credentials to partners, suppliers, and customers to facilitate tighter business integration and closer relationships. For example, financial institutions issue electronic credentials to customers to perform online cash management or banking transactions and manufacturers provide credentials to key players in their supply chains.

As with physical identity documents, an individual can hold a number of digital identities to use in various circumstances. Some recent examples of how digital identities are successfully being used:

- Governments around the world have recognized the need for digital identities and are beginning to address this issue proactively. Spain, for example, has begun issuing digital identities on smartcards as a means of enabling citizens to access government benefits such as social security, and other online government applications. The UK and other European nations are considering similar plans.

- In several of the Canadian provinces, the provincial police employ digital identities to secure internal email and remote access for officers while they are in the field. By leveraging digital identities to securely share data and simplify administrative tasks, both public safety and efficiency have been improved. The provincial police have also extended the infrastructure to municipal police so local jurisdictions can exchange information securely, access provincial databases and applications and ensure the security of their own local information repositories.

- The U.S. Criminal Information Sharing Alliance (CISA) system enables the secure sharing of criminal information by leveraging the digital identities of local, state and federal law enforcement officers. Operating along the 2,000 mile border between the United States and Mexico, border patrol agents can immediately access law enforcement data from multiple jurisdictions, thus helping them to combat drug trafficking, money laundering, and other related crimes. Digital identities strongly authenticate users to the system, thereby keeping those who are unauthorized out, while putting real-time information and communication tools in the hands of those who need them.

- In the U.S., some states such as Illinois are issuing digital identities to citizens and businesses to conduct e-government business. Through such mechanisms as the Federal Bridge Certificate Authority, these digital identities can be extended for use with Federal government applications. The Federal Bridge provides a secure bridging mechanism to authenticate identity between governments and agencies. The Federal Bridge facilitates a set of agreements to enable different government departments or corporations to recognize digital identities with a common measure of trustworthiness. This approach avoids the need for an all-encompassing, government-wide electronic identity system and connection to the bridge provides an interoperability point to all participating departments and individuals.

Digital certificates used as digital identities provide a secure foundation so businesses, individuals, and governments can benefit from efficiencies and economic growth driven by the ability to fully realize the promise of the Internet. These same digital identities can be leveraged for improved security by enabling secure access to critical data and systems, and by providing enhanced security for communication and collaborative activities.

4 E-Government

Governments, like their private industry counterparts, understand the power of the Internet to increase efficiency and enable connection with constituents, suppliers, and other governments. However, security is critical to fulfilling this promise of real-time data access, communication, and collaboration. Security enables governments to offer new online services, exchange confidential information with businesses and other government organizations, and conduct higher-value online transactions. Simultaneously, this security foundation protects government assets from internal and external attack.

Secure e-government services provide strategic and financial advantages through enabling increased constituent and supplier access to key government resources. Governments have initiated e-government projects as a way to deliver better services to their constituents and drive increased efficiency into business processes. By incorporating security into e-government projects, the benefits can be extended considerably further. This enables governments to achieve:

- Reduced transaction costs
- More efficient business processes
- Expanded reach to citizens, businesses, and other governments
- Delivery of new products and services
- Faster “time to market” – the ability to bring on new services quickly
- Greater trust in government

- Improved return on investment and decreased cost of ownership
- Better local conditions for economic growth

Governments around the world have realized how security and digital IDs accelerate the benefits derived from e-government. Five of the top six e-governments globally, as ranked by Accenture, are deploying digital identities as a foundation for their e-government strategies.

Canada is also an excellent example of secure e-government. As measured by Accenture, Canada leads the world in the rollout of e-government programs. Canada has a well-developed security solution known as Secure Channel, which uses PKI technology on a countrywide scale to accommodate all taxpayers, businesses, and levels of government. Many applications are being deployed using Secure Channel, all leveraging an efficient common infrastructure for security.

Denmark, ranked number four by Accenture, has recognized the value of a government-wide approach to e-government service delivery. The country is finalizing a nationwide, service-oriented IT architecture to facilitate secure e-government delivery of services and to stimulate data sharing between public and private entities. As part of this architecture, the Danish government plans to issue digital identities to all citizens. These digital IDs will be used with agencies such as Central Customs and the Tax Administration. Digital IDs will also improve the efficiency of internal, government-to-government and government-to-business communication and collaboration while protecting vital government resources.

The China Financial Certification Authority (CFCA) is an example of government and private bodies jointly leveraging a system of digital identities. The CFCA is a joint venture body of 13 leading commercial banks of China under the direct leadership of the People's Bank of China, China's central bank. The CFCA utilizes digital identities to facilitate the secure delivery of services to almost 180,000 direct users.

5 Information Security Governance

The challenge facing government and industry is to collaborate in new ways to protect our economies and our critical infrastructure. Much like it did for Y2K, government can leverage shared expertise and muscle to increase local, national and global security in tandem with enterprises. This can only work, however, if the private sector and government work on a global scale to establish trusted and long-term partnerships.

On the business front, management must take the lead in developing and implementing credible and effective cyber security programs for the enterprise. Cyber security is not just a technical issue that can be addressed by the CIO. It is a corporate governance issue that must be addressed by CEOs and Boards of Directors. There is broad consensus on the actions necessary to remedy the problem. What is lacking is a corporate governance framework that allows for effective execution.

Until executive management systematically incorporates cyber security into its everyday business practices, it will make halting progress toward securing its business financials and its information systems. Only by treating cyber security as a governance issue and defining specific tasks that employees at all levels of an organization can discharge, will the private sector create the implementation framework necessary for results. In doing so, business will not only advance customer satisfaction and create new market opportunities, but also provide enormous contributions to the physical and economic security of citizens, businesses and governments throughout the world.

Government must encourage this process, not by passing technical mandates, but by setting an example and inviting collaboration. Like business, government must insist that cyber security be treated as an executive management issue that involves risk assessment, remediation and reporting. By insisting that cyber security be treated as an organizational priority and funding it accordingly, government can spur the private sector toward action.

Recently, an Information Security Governance Task Force convened by the Business Software Alliance released a management framework that the private sector can implement to address the growing need for cyber security and respond to existing regulatory requirements. The Task Force, co-chaired by Entrust Chairman, President and CEO Bill Conner and Internet Security Systems, Inc. (ISS) President and CEO Thomas Noonan, was created to elevate information security governance issues to the higher management level within companies and organizations. The framework, presented in a white paper entitled, "Information Security Governance: Toward a Framework for Action". The paper can be downloaded from: www.bsa.org/security/ITgovtaskforce.pdf .

6 A Call to Action

The security challenges of the 21st century require international cooperation and collaboration on an unprecedented scale, including the promotion of strong cyber security measures to protect government and corporate IT systems, and ultimately, the world economy.

To address cyber security, both governments and industry must take proactive measures to secure their systems. This security also provides significant economic benefit through enabling extended integration between customers or citizens, partners and employees, and increased return on investment. Conversely, the failure to protect critical cyber systems also poses huge economic risk.

Governments and industries throughout the world must take the following actions:

1. Work cooperatively with government and industry to facilitate the issuance of **digital certificates** that can be leveraged for e-government and e-business applications, as well as to secure information and improve worldwide security.

2. Encourage the growth of strong and stable **e-government** with strong security policies and practices. This will both protect the valuable data and communication necessary for worldwide security, while reducing the cost of government and lowering costs for businesses interacting with the government.

3. Support standards for **identity management** through groups such as the Liberty Alliance, which will promote and enable both e-government and e-business and create the environment of trust that is critical for success. Continue to strengthen government security practices for e-government and security systems through policies and programs.

4. Initiate development and implementation by management of credible and effective **cyber security programs for the enterprise**. Cyber security is not just a technical issue that can be addressed by the CIO; it is a business and corporate governance issue that must be addressed by CEOs and boards of directors. Insist that cyber security be treated as an **organizational priority** and fund it accordingly.

5. Facilitate and adopt **information security governance** guidelines and frameworks such as the one from the Business Software Alliance. The government can assist this progress by implementing contract incentives for corporations with strong security programs. The Y2K example supports the effectiveness of this approach.

6. Promote success stories around security best practices as a way of promoting brand and trust, as well as raising awareness across industries and governments on the importance of effective security solutions.

7. Promote and support forums like the EastWest Institute to share best practices and raise the profile of effective security as essential for worldwide security and economic growth.

7 About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world leader in securing digital identities and information, enabling businesses and governments to transform the way they conduct online transactions and manage relationships with customers, partners, and employees. Entrust's solutions promote a proactive approach to security that provides accountability and privacy to online transactions and information. Over 1,200 enterprises and government agencies in more than 50 countries use Entrust's portfolio of security software solutions that integrate into the broad range of applications organizations use today to leverage the Internet and enterprise networks. For more information, please visit **http://www.entrust.com**