Entrust®
Securing Digital Identities & Information

The Federal Bridge: A Foundation of Trust

The Federal Bridge: A Foundation of Trust

Entrust, Inc.

ONE HANOVER PARK

16633 Dallas Parkway, Suite 800

Addison, Texas 75001

USA

TABLE OF CONTENTS

1. INTRODUCTION

Trust has always been based upon relationships. When a customer presents a credit card, retailers accept it because they have a reliable method to verify its authenticity and validity. To do this, the retailer does not need to have a relationship with every card issuer in the world. Instead, the retailer connects to an established infrastructure that links the card issuers together and enables the retailer to verify cards issued by any company within that network.

As we move to electronic-based transactions utilizing electronic identity credentials issued by many different organizations, it is vital for a relying party to be able to verify the validity of a presented credential. It is unrealistic to expect that a single issuer of credentials will ever exist, since Government agencies, public companies and private organizations are already issuing their own credentials. To enable the recognition of these credentials by others, a network infrastructure element must be available to link together these organizations. The Federal Bridge Certificate Authority is an example of this type of infrastructure element.

Many of the public and private entities issuing electronic credentials are doing so using Public Key Infrastructure (PKI) technology. The use of PKI has enabled these organizations to maintain or improve security as they replace paper-based processes with electronic processes or replace closed communications environments with open and public networks. Both of these environments have an inherent need for strong identification of users and protection of information and resources. PKI has been implemented to address these requirements of authentication, privacy and information protection.

The US Federal Government has developed an architecture to extend trust beyond a single trust domain to address authentication, privacy and data protection needs while reducing complexity of implementation. This paper describes the Federal Bridge Certification Authority architecture, and describes how this architecture enables trust between various parties. This trust supports not only improved business efficiencies, but can also be extended to become a cornerstone element in the protection of our national cybersecurity assets.

2. DEVELOPMENT OF THE BRIDGE ARCHITECTURE

2.1 Early Architectures

As public key technology infrastructures were implemented, organizations quickly recognized that a standards-based, open architecture for authentication could easily extend to support other business needs and provide a methodology to share information and access to resources with other organizations. This recognition led many organizations to develop plans to link their public key based architectures together. These linked architectures are called trust domains, since policies within the domain define the trust relationships between the users.

The linkage of trust domains is formally known as cross-certification. Cross-certifying two trust domains includes: 1) an agreement of responsibility to follow the operating principles of the infrastructures' policies, 2) an agreement on how the infrastructures will trust each other's policies (wholly equivalent or with mapping between levels of trust), and 3) technical linkage.

As more organizations recognized the benefits of linking architectures, the simple architecture of A communicating with B was not sufficient. Instead, a mesh cross-certification architecture developed that linked organizations together in a fully connected way, as seen in figure 1 below.

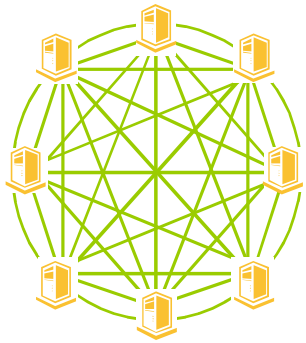

Figure 1: Mesh Cross-certification Topology

However, this topology is cumbersome to create and manage due to the policy, technical and legal elements required for each link.

2.2 Extending the Cross-Certification Architecture

The projected development of mesh cross-certification (and in some small cases, actual implementation) led many within the Federal agency community to look for better alternatives. The Federal PKI Technical Working Group, consisting of Government and industry representatives, began investigating the possibility of implementing a simpler model. They proposed a "hub-and-spoke" model of trust similar to what the financial service industry uses for processes such as check-clearing and credit card approvals. This model is shown in Figure 2 below:

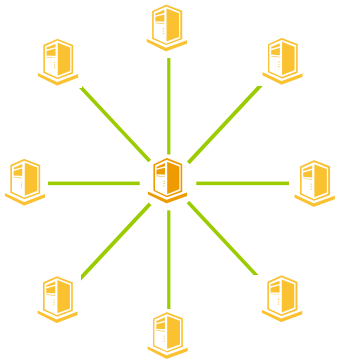

Figure 2: Bridge Cross-certification Topology

The “hub-and-spoke” architecture reduces the number of links an organization needs to interact with other trust domains. This creates immediate benefit both in initial configuration and in ongoing management. The architecture is based upon Internet Engineering Task Force standards that have developed out of the International Telecommunication Union Standards bodies. These standards also enable organizations to define restrictions to avoid “transitive trust”, the idea that if A trusts B and B trusts C then A trusts C. Transitive trust paths are not always valid, so organizations must be able to avoid these transitive trusts. The adopted standards enable the capability to avoid this problem in a very straightforward and scalable way

2.3 The Bridge Architecture Within the US Federal Government

The development of Public Key Infrastructures (PKI) within the Federal Government should not be viewed either as a monolithic structure or a single enterprise PKI. The approach being adopted for the Federal PKI is based on the concept of a bridge Certificate Authority, or “bridge CA.” The bridge CA provides trust (or certification) paths between principal Certification Authorities (PCAs) for trust domain PKIs. This approach enables large-scale government, industry, national or global PKIs to be assembled from application or enterprise-scale PKIs. (See Figure 3.) The approach is described in the Federal PKI

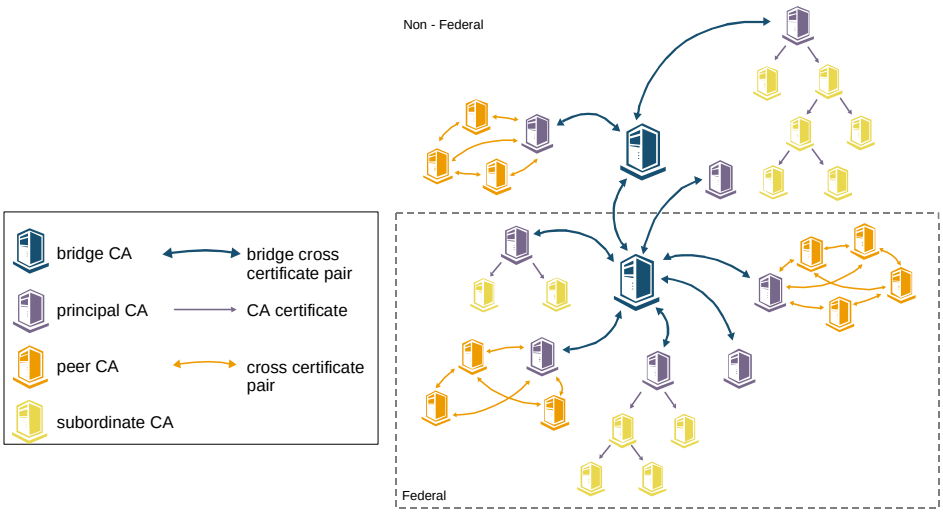

Figure 3: Federal PKI Architecture

Concept of Operations (CONOPS.) (See http://csrc.nist.gov/pki/twg/baseline/pkicon20b.PDF).

The Federal Bridge CA, operated by the General Services Administration (GSA), provides cross-certification among trust domain PKIs. Each trust domain designates a single principal certification authority (CA) to cross-certify with the Federal Bridge CA. The combination of a principal CA and its associated PKI forms the domain of trust, where the principal CA is the known point of trust for the domain.

The Federal Bridge acts as a trust conduit. It does not provide a root of trust, but instead *links together existing trust infrastructures*. One of the functions of the bridge is to map the policies of existing trust architectures. While the Bridge was originally intended to link together existing PKIs within Federal agencies, now State and national PKIs are beginning to cross-certify with the Federal Bridge as well. Organizational Bridges, such as the Higher Education Bridge, may also link to the Federal Bridge.

The process of linking an architecture to the Federal Bridge is well defined, and is managed by the Federal PKI Policy Authority (FPKIPA). The FPKIPA includes the original founding members (Departments of Defense, Justice and Treasury, NASA, GSA and the Office of Management and Budget) and the existing entities connected to the Federal Bridge (NASA, Treasury, Defense and the Department of Agriculture/National Finance Center). The FPKIPA has developed a set of documents that not only describes the cross-certification process, but also describes Federal Bridge CA policies and Product Interoperability Guidelines.

The FPKIPA documents listed below can be found at the FPKIPA Web Page within the Documents section (see http://www.cio.gov/fpkipa/documents_page1.htm):

- *The Evolving Federal Public Key Infrastructure*, June 2000
- *Charter of the Federal Public Key Infrastructure Policy Authority*, May 21, 2000
- *By-Laws and Operation Procedures/Practices for the FPKIPA*, October 12, 2000
- *X.509 Certificate Policy For The Federal Bridge Certification Authority*, June 18, 2002
- *Federal Bridge Certification Authority Product Interoperability Guidelines*, September 28, 2001
- *Your Interface to Interoperate with the Federal Bridge*, May 25, 2001
- *Application for Interoperability with the Federal Bridge Certification Authority*, October 12, 2000

3. THE FEDERAL BRIDGE AND THE PRESIDENTIAL E-GOVERNMENT INITIATIVES

As stated previously, the Federal Bridge is not a root of trust, but instead provides a conduit of trust that enables applications within the Federal Government and gives State-level initiatives a method to interact with Federal initiatives, at least from an authentication perspective. The Federal Bridge supports the Presidential initiative categories (IEEE, G2G, G2B and G2C) in these ways:

- **IEEE:** The internal efficiency and effectiveness initiatives are intended to improve how the Government does business. By its nature an internal program, IEEE involves agencies interacting with other agencies or their employees. Traditionally, agencies have either operated their own trust environment or outsourced their trust environment operations. This environment is ideal for interaction with the Federal Bridge and for agencies to operate their own CA or to obtain service from a CA Service Provider such as PWC beTRUSTed or the USDA/NFC.

- **G2G:** The Government to Government initiatives link together agencies and Federal and State programs that have common needs in order to make the information flow more efficient. This environment is well suited for States and agencies to manage their own trust domains through internal operations or outsource. In both the IEEE and G2G arena, organizations with an existing trust infrastructure can leverage the Federal Bridge to extend that infrastructure to other agencies and/or to State level agencies.

- **G2B and G2C:** Due to common features, these categories can be addressed together. To date, agencies have been reluctant to broadly issue identities to millions of businesses and citizens. Issues of cost, national identity, management and registration have been significant barriers. However, the Presidential initiatives have caused agencies to rethink this view and to look for new solutions. An ideal solution would be for States to issue credentials and link to Federal programs through the Federal Bridge. Such a win-win-win scenario follows:

    i. Agencies need to register businesses and citizens to utilize their online programs. The Office of Management and Budget and the General Accounting Office want to see existing infrastructures re-used, as does GSA (since they provide the infrastructures). Therefore, these identities must carry across multiple agencies. However, Agencies are reluctant to manage these identities themselves and are looking for low cost alternatives.

    ii. Therefore, an Agency offers an online program using two digital certificate alternatives. First, users can utilize credentials issued by a State-accredited authority that meets the policy of the program and where the State CA is linked to the Federal Bridge. Secondly, users without credentials can be given the option to obtain an external certificate from a trusted third party, as long as they provide sufficient identifying information. This external certificate would be a low-end certificate since it is likely to originate from an on-line registration process. Either certificate option would work for both businesses and citizens.

    iii. As States turn on their own programs and link to the Federal Bridge, the State can leverage the users in their domain with external certificates to begin converting them to using State-sponsored certificates. At this point, no change is required in the Agency application and the Agency reduces its ongoing risks by converting the user from an Agency-sponsored external certificate to a State-sponsored certificate. While the benefit is obvious for the Agency, the user benefits by having access to State and Federal

programs and the State benefits through the potential cost savings realized from increased usage of their online programs (win-win-win).

As States roll out their credentials, the Federal Bridge becomes the trust conduit for interactions with Federal Agencies for both citizens and businesses.

4. THE BRIDGE AS A FOUNDATION FOR A NATIONAL CYBERSECURITY ARCHITECTURE

The Federal Bridge can also serve as the foundation of a National Cybersecurity Architecture to improve homeland security. The concept behind the Cybersecurity Architecture is a bridge infrastructure that interconnects each critical infrastructure service at the international, federal, state and local levels through bridges that map identity and authorization policies. A graphical representation is shown in Figure 4, Cybersecurity Architecture, below.

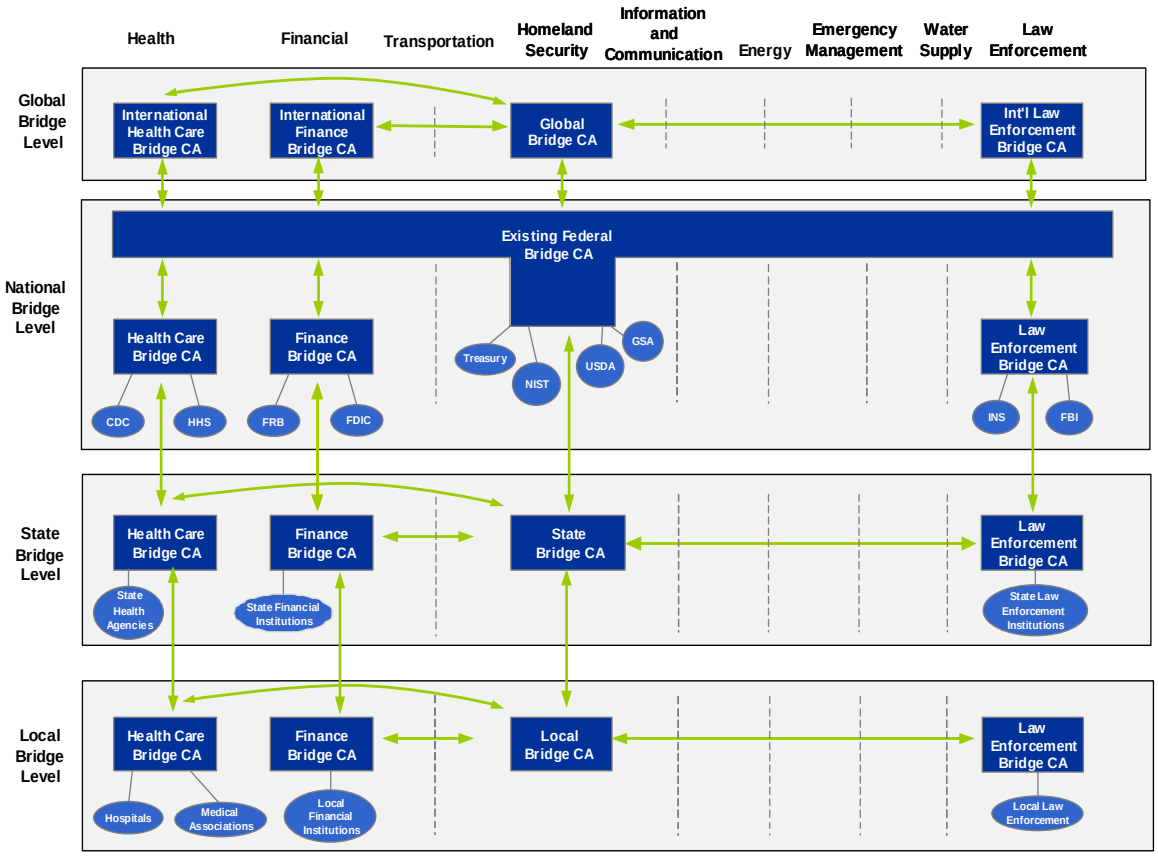

Figure 4: Cybersecurity Architecture

In this concept, each of the critical infrastructure services - health care, financial services, transportation, infrastructure and communications, energy, emergency management, water supply and law enforcement – has a bridge at each level of government. At the federal level, the bridges cross-certify with the expanded Federal Bridge CA, which provides policy mapping for international communications. This flexible structure permits a wide variety of policies to be mapped across a large number of disciplines.

Each of these bridges would be deployed to enhance the durability of the architecture. The actual servers could be configured in highly available clusters, where the members of a cluster reside at significant geographical distances from each other. If one member of the cluster failed, another member could automatically assume the responsibilities of the cluster. A different service provider could serve each cluster member, so that network outages do not affect more than one member.

5. SUMMARY

The Federal Bridge CA is a fundamental element of the trust infrastructure that provides the basis for intergovernmental and cross-governmental secure communications. The Bridge, acting as a trust conduit, extends the benefits that agencies and government organizations achieve through the use of Public Key technology to a broader set of applications and transactions. These new applications and transactions can make these government organizations more effective in their business operations. The Bridge supports the Presidential E-Government initiatives and can be leveraged by other levels of government as they expand their own E-Government programs.

This same Federal Bridge infrastructure can also serve as the basis for a strong National Cybersecurity Architecture to help protect cyber resources and to help facilitate the information sharing that is vital to addressing homeland security threats. The Federal Bridge architecture, based on open standards, can continue to grow and can provide the basic architecture for authentication for critical governmental services.

APPENDIX: ENTRUST CORPORATE OVERVIEW AND GOVERNMENT CREDENTIALS

Entrust Corporate Profile

A Secure Foundation

Entrust has been a pioneer in the Internet security marketplace since 1994 and continues to lead the market. The company develops solutions built on enhanced security services that enable government agencies, financial institutions and Global 1000 enterprises to conduct more trusted transactions over the Internet. Entrust solutions provide identification, entitlements, verification, privacy and security management capabilities that are easier for organizations to deploy, manage and use. These capabilities help to provide a secure transaction environment, enabling greater reach, speed and return for business and government operations.

Entrust pioneered public-key infrastructure (PKI) and was the first to integrate Privilege Management Infrastructure (PMI) technologies with PKI. Entrust extends this capability across multiple applications and platforms, for a variety of wired and wireless devices, and with other innovations.

The company's marquee client roster boasts more than 1,200 customers, including US Dept. of State, US Dept. of Energy, US Dept of Justice, the State of Illinois, NASA, JPMorgan Chase, the U.S. Coast Guard, the UK and U.S. postal services, Lloyd's TSB, Merrill Lynch, the Government of Canada, and many more. No other Internet security enabler is better equipped to provide solutions built on the enhanced security services required for governments and businesses to move transactions online and deliver efficient and convenient e-government, e-procurement and e-commerce services.

Enhanced Security Services

Entrust is leading the next critical phase in the Internet's evolution, bringing trust and security to governments and businesses. Entrust solutions built on enhanced security services help to provide the following capabilities:

- **Identification:** Allows senders and receivers to have more confidence in who they are dealing with in the electronic world. Strong identification is achieved through digital identities, which are similar to an "electronic passport."

- **Entitlements:** Enables organizations to grant customers, employees and business partners various levels of access to applications and data, based on a person's identity and role.

- **Verification:** Provides an auditable record that helps to bind each party digitally to a transaction, so that it is more difficult for a party to repudiate their participation. Verification can take the form of digital signatures and digital receipts, which are now recognized in legislation in the U.S. and many European countries.

- **Privacy**: Helps protect information while in transit and storage throughout the life of a transaction. Importantly, the other vital component of privacy includes the policies that govern an organization's use and disclosure of information.

Entrust's Security Management is the infrastructure that enables organizations to effectively and efficiently manage identification, entitlements, verification and privacy in a way that reduces the burden of administration for the administrators and end users. Entrust's award-winning security management is comprised of three key features as follows.

- **Modular deployment** can help deliver quicker return on investment, allowing organizations to deploy an initial capability and add functionality as needed.

- **Transparent security management** helps reduce downtime and cut training and help-desk support costs, allowing end users and administrators to focus on their work, instead of the security.

- **Broad platform and application support** to work with multiple IT environments and industry standards now, and in the future.

The application of these capabilities to governments, financial institutions and other enterprises enable these organizations to conduct more trusted transactions over the Internet facilitating deeper, tighter integration with citizens, businesses, suppliers and employees.

Company Facts

- U.S. based corporation
  - Headquartered in Dallas, TX
  - Major presence in Virginia, California, New York
- 10 years experience in security software and services
- 700+ employees
- 10 offices worldwide

First Mover in Internet Security

- PKI (1994)
- PMI - Portal Access (1997)
- Wireless (1999)
- Enhanced Internet Security (2001)

- Entrust has over 90 patents and patents pending
- Entrust has 50% worldwide PKI Software market share - *Gartner Oct., 2001*
- Entrust ranked #2 globally for all encryption technology - *Gartner Oct., 2001*
- Entrust ranked #2 globally in authentication - *IDC Oct., 2001*

Awards and Recognitions

Entrust is recognized as a market leader through a number of industry awards, such as:

- The 2002 Information Security Magazine Excellence Award for best **"Soft Form Factor Authentication Solution"**.

- In 2001, for the third time in five years, Network Magazine named Entrust's software **"Product of the Year"** in the **"Authentication and Access Control"** category, and Network Computing awarded Entrust its **"Well-Connected Award"**.

- For the second consecutive year, Entrust received the **"CrossRoads Award"** in 2001 for the most comprehensive information security product for personalization and access management for global ebusiness portals.

- In addition, Entrust was awarded the 2001 **"Advanced Card Award"** and the 2000 CRMPower **"Golden Award"** for most customer-centric company of the year.

Seizing the Opportunity

Entrust is moving aggressively to capitalize on its leadership in delivering integrated solutions built on enhanced security services with identification, entitlements, verification, privacy and security management capabilities. The company has focused on leading adopters in government and other key vertical markets in more than 40 countries worldwide.

The company is also establishing relationships with system integrators and system consultants to expand its market coverage and service capabilities. Importantly, Entrust is working with hardware and software original equipment manufacturers (OEMs) to package solutions for enhanced security services for government, and multinational Global 1000 organizations and other enterprises.

Entrust in the Government Sector

Cornerstone of E-Government

Entrust has over 10 years experience providing security services to the United States government and governments around the world. Our portfolio of enhanced security services has enabled **over 330 government customers worldwide** to conduct trusted communications and transactions with their employees, suppliers, citizens and businesses. As a result our government customers have been able to extend new services to constituents via the Web, improve cross-government collaboration, and lower costs by replacing paper-based processes. A brief overview of Entrust's credentials in the government sector follows.

U.S. Government Customers

- Top Federal Agencies including U.S. Departments of: Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Labor, Justice, State, Transportation, Treasury, Veterans Affairs, NASA, Social Security Administration.
- Majority of states with strategic E-Government initiatives including: Illinois, Wyoming, California, New York, Florida, Virginia, Tennessee, Washington, Missouri, Massachusetts, Nebraska, North Dakota, Kentucky, Kansas, Alabama, Ohio.
- Key technology partner of U.S. Security agencies including: National Institute of Standards and Technology (NIST) and National Security Agency (NSA).

Governments Around the World

- Cornerstone of security infrastructure for Government of Canada, extending to multiple provinces.
- European Governments including UK, France, Italy, Norway, Denmark, Ireland, and Spain.
- Asia/Pacific Governments including Thailand, China, Hong Kong, Singapore, and South Korea.

Technical Expertise

- Entrust was the first company to receive a FIPS 140-1 certificate and continues to maintain this certification for its broad portfolio.
- Entrust is an author, visionary and driver on more than 30 industry standards boards and forums.
- Entrust is a co-founder of the PKI Forum, a vendor neutral, not-for-profit organization whose primary mandate is to increase PKI awareness and address multi-vendor interoperability.
- Entrust is a key contributor to both the Business and Technical Working Groups of the Federal PKI Steering Committee, which was commissioned to facilitate a lead advisory role to guide Federal agencies, executive agencies, and the Government Information Technology Services (GITS) Board on matters germane to the PKI infrastructure, interoperability, business functions, technology, law, and policy.

Foundation of the Federal Bridge

The United States Federal Bridge Certification Authority (FBCA) was established to serve as a link between U.S. agencies for interoperable, secure E-Government transactions using digital identities. FBCA provides the capability to align the diverse policies and procedures of various departments and agencies, enabling each department or agency to set their own policies and procedures relative to their secure communication requirements.

Entrust's enhanced security solutions serve as a core element of the Federal Bridge, and demonstrate interoperability with all major Bridge vendors. Many agencies including the DoD, USDA, NASA, DoE, FDIC, and states such as Illinois are currently using or plan to utilize the Federal Bridge.

The Federal Bridge enables Government and non-Government organizations to conduct secure communications, collaboration and transactions over the Internet, streamline internal processes, enable E-Government, improve service delivery to citizens and agency trading partners, and to deter and protect against the threats of cyber terrorism.

Government Accredited Certification and Validation Laboratories

Entrust CygnaCom is a wholly owned subsidiary of Entrust, Inc, which specializes in providing professional computer security services and cryptographic solutions to one of the world's largest information technology markets, the United States Government and Governments abroad. In addition, Entrust CygnaCom provides professional services to customers in the financial and health-care industries. With a staff of highly qualified engineers, it has the depth and experience to offer clients a complete package of security risk assessment and consultation services. Labs perform compliance testing to verify that product design, implementation and documentation meet certain security requirements recognized by the U.S. Government.

- Entrust CygnaCom won the U.S. Government's "Hammer Award" for the successful implementation of the FTS2001 electronic bid process that provided paperless solutions for vendors to submit complex proposals electronically, saving taxpayers approximately $1.5 million a year, and 52,000 staff hours.

- Entrust CygnaCom operates two laboratories: The Security Evaluation Lab (SEL) and the Cryptographic Evaluation and Assessment Lab (CEAL) dedicated to providing fair, objective, and cost-effective assessments of all products submitted for certification and validation.

- Entrust CygnaCom’s lab facilities were among the first to be accredited by the U.S. Department of Commerce, the National Institute of Standards and Technology (NIST), and the National Voluntary Laboratory Accreditation Program (NVLAP) for information technology security testing against the federal cryptographic criteria (Common Criteria (ISO/IEC 15408).

- Over 50 highly skilled computer security, PKI and PMI consultants with expertise in PKI, cryptographic technologies, security engineering, systems integration and development, the FIPS 140-1 Standard, the Trusted Computer Systems Evaluation Criteria (TCSEC), and the Common Criteria (CC).

For more information on Entrust’s solutions for government please visit www.entrust.com/government/index.htm.