



Pharmaceutical companies place a high value on their information assets — corporate information and research data. However, these organizations cannot afford to restrict access to corporate resources by barricading themselves inside a digital Fort Knox. To stay competitive the pharmaceutical industry depends on access and distribution of sensitive data to thousands of employees at potentially hundreds of locations worldwide.

## Business Challenge

The pharmaceutical company in this example relies on networked computer systems and central databases for storing and accessing its information asset base. A highly scalable and secure solution for employee identification and access control was required to provide 70,000 employees at 170 sites with controlled access to internal and external data. The IT team also had to provide secure access for external stakeholders such as business partners, customers, suppliers, physicians and researchers. The company was also required to be in compliance with legal standards such as GxP (GCP — Good Clinical Practices, GLP Good Laboratory Practices, and GMP — Good Manufacturing Practices) for quality control and auditability, as well as 121 CFR part 11, the FDA regulation for electronic records and electronic signatures within pharmaceutical companies.

This information access system was designed to enable the automation of a variety of business processes including:

- Drug trial information management for government
- Confidential patient information exchange
- Communication with external physician networks
- Secure procurement and customer order information

Ensuring the security of data that is accessed so widely would be challenging enough under normal circumstances. In the case of a pharmaceutical company, the problem was significantly compounded by regulatory and legislative requirements for integrity and confidentiality of electronic records.

## Benefits

- Digital certificates provide trusted identification at each end of the VPN communications tunnels
- Improved customer service

## Business Challenges

- Providing 70,000 employees and 170 sites controlled access
- Providing secure access to external stakeholders
- Regulatory and legislative requirements

## Solution

- Entrust Authority Public Key Infrastructure (PKI)
- SafeNet Luna CA3 HSM

## Solution

The company decided to issue digital certificates to employees and external partners as the basis for establishing secure online identities throughout all of their business processes. Entrust Authority Public Key Infrastructure (PKI) was selected as the software component of the solution for creating and authenticating digital identities. The company required the deployment of a 2-tier digital certificate issuance system consisting of a central Root Certificate Authority (CA) and 9 subordinate CAs corresponding to each of the company's organizational divisions. Given the important function of the digital identities, and what was at stake should these identities be

compromised, the IT team concluded that standard software-only solutions did not offer sufficient protection for the private encryption keys that would form the core of this identity infrastructure. Therefore, Hardware Security Modules (HSMs) were deployed to provide the highest levels of protection for these sensitive private signing keys – effectively the source of trust for all other IDs. The department responsible for implementing the solution was committed to a 24/7 Service Level Agreement, which required a robust HSM to guarantee up-time for the company's PKI. Specific HSM requirements also included a dual-control function to prevent super-user control.

The SafeNet Luna CA3 HSM, working in conjunction with Entrust Authority software, was selected because of its impeccable track record as a root key protection system. In addition, Luna CA3's multi-person authentication functionality guaranteed meeting the dual-control mandate by ensuring that a defined subset of individuals must be present before an administrative action can be performed with the HSM, preventing unilateral control. The Luna CA3 is a flagship product for SafeNet, leading the HSM market for root key protection systems. The product is used by over 80% of Fortune 500 companies deploying PKI digital identities. Currently, it is the only product of its kind on the market that has received certifications under both the FIPS standard as well as the worldwide-recognized Common Criteria standard.

### **Consider the Benefits**

Using A Virtual Private Network (VPN) from Check Point Technologies and a document management system from Adobe were the first applications integrated with the new digital identities. Digital certificates provide trusted identification at each end of the VPN communications tunnels set up to securely access sensitive and valuable corporate information. The digital identity infrastructure also enabled the organization to securely migrate several of its customer and partner related business applications to the Internet. An additional benefit of this streamlined process was improved customer service through more secure, reliable and efficient use of e-mail; remote access and B2B supply chain transactions with suppliers and customers.

### **Conclusion**

SafeNet, in conjunction with our software partners, delivered a comprehensive, HSM-secured digital identity system that is used to ensure secure corporate communications via authenticated VPN sessions and access to sensitive information with a secure document management system, while improving efficiency and service levels and streamlining business processes within a trusted infrastructure.