



Business Case Justification For Identity Management

1000's of users benefit from cutting-edge PKI Solution

Client:	Fortune 100 Corporation (Subsidiary)
Project:	Business Case Justification for Public Key Infrastructure (PKI)
Industry:	Healthcare
Solution Focus:	National Sales Force
Technologies:	Microsoft Windows 2003 Server - Active Directory

Executive Summary

The enterprise sales force of this international pharmaceutical firm has a very mobile workforce of over 3,000 people who travel extensively. The data resident on a salesperson's laptop computer is very sensitive—so much so that the data is worth far more to the company than the laptop itself. In light of that fact, the company required the use of a technology to secure this data, so that its confidentiality can be ensured should the laptop be stolen or misplaced.

The business case methodology we employed included an extended form of cost-benefit analysis that considered factors beyond financial metrics. Other factors considered included security needs, business need, associated risks, and qualitative benefits resulting from the investment. This case study demonstrated to the client that implementation of a PKI technology is achievable, beneficial, and affordable, and is achievable in a relatively short fielding time.

Upon implementation the technology improved operations, streamlined business processes, and even reduced costs.

Business Situation

The objective was to implement the most effective level of security available in compliance with the firm's Information Asset Protection Policies.

The client required that various security protection alternatives be evaluated include bar code cards, magnetic stripe cards, PIN/password, non-PKI-enabled smart cards, and biometrics. As an example, when multiple technologies are layered using the technologies in combination (e.g., PKI, PIN/password, and biometrics), a greater degree of assurance can result. Our investigation and analysis had to include the relative costs, benefits, and potential applications of each (possible) alternative. The technologies evaluated helped build a broad range of information assurance alternatives into the business case.

Solution Description

In addition to cost, four security benefits were evaluated according to each technology: nonrepudiation, authentication, data integrity, and confidentiality. These benefits map primarily to PKI. The second section of benefits focused on the operational and business benefits, these benefits include scalability, portability, interoperability, efficiency, and data storage capacity. Although all of the alternatives evaluated provided some means of information assurance, only PKI provided the high degree of assurance required by the client in all areas.

All options to achieve the stated information assurance goals were captured. Many alternatives were considered; cost and feasibility did not preclude an alternative from consideration. These comparisons included a thorough look at the intangible benefits and increases in effectiveness that cannot be assigned a dollar value.

Finally, we compared the alternatives and recommended the appropriate solution. The preferred alternative supported the budgeting process and provided the basis for managing the results.

Technologies involved:

- Windows 2000 – (Windows 2000 Server, Windows 2000 Advanced Server and Windows 2000 Server Client Access)
- Microsoft Active Directory – (Including the introduction of a unique employee identification scheme that eliminated the use of social security numbers)
- X.05 standards based PKI technology
- Rainbow iKey Token 2032

Anticipated Business Benefits

Tangible Benefits:

- Improved Business Practices, increasing the efficiency and speed of business processes, both internally, and externally with trading partners and customers
- Simplified system and network administration through fewer passwords – which means reduced burdens on system and network users
- Single-Sign-on for Windows 2000, Exchange and Legacy Systems
- Technology to meet regulatory requirements including FDA's 21 CFR Part 11
- Ensured Data Integrity in electronic documents, making possible electronic "digital originals"
- Decreased paperwork, saving time and money
- Secure access to J&J information resources by J&J employees, partners, and customers
- Digital signature for e-mail, workflow, form signing, single sign-on, extranet access and desktop file encryption;
- Provision of an authoritative and timely, distributed, repository of information about employees, partners, customers, systems, roles and resources;
- Integration with existing and emerging J&J (and non-J&J) systems and technologies via open standards.
- Automation of network account creation, suspension and deletion process.
- Automation of the Exchange account creation, suspension and deletion process
- Improved Document and Network security, strengthening the protection of company and customer assets

Intangible Benefits:

- Increased externalization of business through outsourcing and strategic business partnerships
- Rapid granting and revoking of access rights to information on a global basis.
- Enabling the company to operate at risk appropriate to the business without impacting security of other affiliates
- Usable inside and outside the enterprise
- Helps to eliminate the use of passwords
- Interfaces with trusted 3rd parties

Conclusion

The recommended PKI solution also permitted the enterprise to take advantage of the speed and immediacy of the Internet while protecting business-critical information from interception, tampering, and unauthorized access through secure transactions. Proper management and use of public keys enable PKI to provide information assurance and an enhanced operating environment through authentication, data integrity, nonrepudiation, and confidentiality. PKI also offers significant benefits in its interoperability and scalability.