



Government Agency Takes Control of Access Management for Sensitive Applications

The agency can now be sure that all communication with sensitive applications is encrypted and that access is allowed only with the use of a smart card from FoxT.

CASE STUDY

A high profile government agency in Scandinavia faced a problem when it wanted to implement a system solution: the new infrastructure lacked security, as did the open systems it ran on.

Moving to the new system was deemed too unsafe unless an appropriate solution could be found to address the security issues. The agency had a long list of requirements of the security solution, key among which were:

- Easy administration
- Secure single sign-on
- Strong authentication
- Data encryption

The government agency's environment included more than 20,000 users, network-hosted mainframes, Unix servers running different brands of the operating system, and PCs running Novell and Microsoft. The agency also wanted to use a Web-based application that required certificate login. This diverse environment presented the agency with a challenge when it came to finding a security solution that could meet its needs.

Only One Contender

In the end, only one company came close to providing a viable offering, and the agency chose the FoxT ApplicationControl solution.

Following the successful implementation of FoxT solutions, employees in the organization now have to log on only once to their workstation using a smart card. At the same time the user logs on to the PC, he or she is automatically logged on to the network in a secure manner. To work with applications secured by FoxT ApplicationControl, the user simply clicks the application icon to get direct access - there is no need to log on again. The user is identified directly by means of the smart card that he or she inserts into a card reader at the workstation. When the user removes the smart card, the PC is automatically locked.

The move has made life much easier for administrators, who can now provide users with access to a number of different applications from a single point. They can now also deploy a security policy governing parameters such as password length and content and number of login attempts. Administrators have full control over all access routes and can be confident that users removed from the system lose all access to the protected resources.



About FoxT

FoxT protects corporate assets with an enterprise access management solution that centrally enforces granular access entitlements, in real-time, across operating systems and business applications on any networked device. The ability to proactively administer, authenticate, authorize, and audit access across diverse platforms, down to the file and device level, enables organizations to greatly reduce compliance and audit costs, streamline IT security administration, and protect corporate value by mitigating the risk of insider fraud. Headquartered in Mountain View, California, FoxT serves Global 1000 customers in 32 countries. For more information - www.foxt.com or email sales@foxt.com.

Providing Identity and Access Management

FoxT ApplicationControl provides easy-to-use identity and access management including centralized system administration and security policy management for administrators and security and usability enhancements for users, such as single sign-on to workstations and file encryption services.

The solution enables organizations to distribute public key credentials (such as signature and file encryption keys) to users' workstations and stores them in a credential store (smart card, virtual card or Extended Smart Card). Users also benefit from single sign-on to network resources, such as MS Active Directory and Novell NDS. Unattended workstations are secured with a locking function triggered by inactivity or removal of the smart card.

Providing Secure Single Sign-On

FoxT ApplicationControl provides users with single sign-on (SSO) to, and protected communication with, selected applications, making the operations environment more user friendly and secure and helping organizations decrease helpdesk calls related to lost passwords.

Dovetailing with the existing security infrastructure, FoxT ApplicationControl enables administrators to centrally enforce strong password policies, log activities, and instantly block users from accessing all applications.

FoxT ApplicationControl is a non-intrusive solution and usually requires no changes to the legacy client or server, and no configuration changes to legacy clients. The FoxT ApplicationControl toolkit-based approach also makes for easy customization to meet environment-specific challenges.

Moving Forward with Confidence

The agency can now be sure that all communication with sensitive applications is encrypted and that access is allowed only with the use of a smart card. The government agency has already begun implementing the next step to further enhance its identity and access infrastructure using FoxT Technology's functionality for "Extended" Smart Cards. This technique involves using a smart card to lock a "virtual card", a digital repository of certificates, private keys and other credentials that is issued and managed by FoxT ApplicationControl.

This approach offers two crucial benefits. First the limited storage space on the physical smart card is no longer an issue since unlimited stock of credentials can be stored in the virtual card. The second benefit relates to smart card and certificate management. If users lose their smart cards, they can still access their important credential information in the virtual card using a replacement smart card. This avoids users having to re-enter login information for applications and minimizes the number of new certificates that need to be issued if users lose smart cards. Additionally, if users forget their smart card at home, they can be issued a temporary smart card so they can work normally while still being subject to the same stringent levels of authentication and authorization.