



BoKS Access Controls for Applications

Powerful External Controls for Networked Applications

A FoxT White Paper

Application Controls

Organizations are facing a range of compelling reasons for gaining enhanced controls over their application landscapes. The control mechanisms that can be applied can be classified into internal controls and external controls.

Internal controls deal with events within the operation of the application, while external controls deal with access to, and management of, the application itself.

The nature of these controls means that a lack of proper external controls can render internal controls ineffective, since security breaches that compromise the data held by applications can involve unauthorized parties bypassing those controls.

External controls for applications include change management procedures, patch and technical management, and access control. Access control includes authentication of users and hosts and protecting data traffic between workstations and application servers.

While internal controls are by their very nature application-specific, organizations can benefit from developing a standardized approach to external controls. In today's increasingly complex and integrated IT environments, organizations are looking to implement external control programs that can be used across those environments.

BoKS Access Control for Applications provides the kind of external application controls needed today by organizations looking to secure their networks and data assets for best practice IT governance and compliance with national and international regulations. The solution can be used to protect a wide range of applications and customized using a comprehensive software development kit.

A transparent solution that does not require any modifications to applications that can be deployed on a wide variety of operating systems and hardware, BoKS Access Control for Applications has been successfully providing external application controls at a number of high-profile companies and organizations for several years.

● An Active Directory With Many Secrets

With Active Directory, Microsoft has provided administrators with a powerful directory service to organize network data and to control access to network resources from a central point. However, "powerful" by necessity also means complex, and the complexity of Active Directory has probably contributed to slowing down the rollout of Windows 2000 and 2003 servers. Initially, many organizations found simply migrating their flat NT4 domain structures into a more sophisticated Active Directory wrapping to be a significant challenge. By now, many have defined their Active Directory Forests, survived an often cumbersome deployment process, and seen their directories mature into efficient tools for centralized administration. Policies have become the levers of network management, and, as a result, Active Directory has become a repository holding extremely sensitive data.

Passwords Remain the Weakest Link in the Security Chain

Surprisingly, in most organizations, authentication is still based on passwords only, regardless of how sophisticated their use of Active Directory otherwise may be. Ideally, in a pure Windows 2000 / XP environment, Windows clients use NTLM 2 or Kerberos to protect authentication requests, which is certainly a great improvement compared to the old LM or NTLM 1 protocols. Yet, by default and for backwards compatibility, Windows clients will revert to the old, weaker protocols if required to do so by one of the nodes involved.

Although you can configure clients to refuse LM and NTLM 1 communication, this may conflict with other important services, and the gain is limited since password cracking tools such as @stake LC™ 5 (L0phtCrack™), KerbCrack and John the Ripper continue to represent serious threats. Furthermore, in modern networking environments users often depend upon being able to switch between online and offline with their laptops, which means that caching Windows domain account credentials must be allowed for practical reasons. Tools such as cacheDump enable the details about any locally cached account, which may include a recent administrator login, to be derived in a couple of minutes.

An even greater threat is posed by annoyed users, who continue to use too simple passwords or, if strict password policies are enforced, persist in using Post-It notes. They may also forget their passwords, which generates expensive help desk calls and causes downtime. Therefore, user authentication based on a single password continues to be the weakest link and an expensive one, considering the wasted time and frustration experienced by both end-users and administrators when logon fails. And, the more efficient use an organization makes of Active Directory, the more there is at stake if the weakest link is broken.

Certificate-Based Authentication

Encrypted protocols for authentication improve security. However, the use of encryption is no guarantee for accuracy unless identities can be properly mapped to a relevant authorization scheme. A bank clerk would hardly consider a seemingly valid ID as sufficient proof of a visitor's right to withdraw money from the bank. The identity of the client needs to be securely mapped to an account, and that account has to be in credit. When password cracking succeeds in spite of traffic encryption, a transaction similar to one with a negligent bank clerk takes place: you are authorized simply by proving that you exist. In the world of computers, the remedy is a digital certificate or possibly two-factor authentication. A certificate securely maps public keys to the identity of a user or a device.

Although Active Directory supports certificate-based authentication, it is not easy to find case studies reporting successful implementation of a fully PKI-enabled Active Directory without other products being involved. This may well be down to the complexity of Active Directory. Another reason is the heavy dependence upon the Microsoft Certificate Authority (CA) implied by an Active Directory-only PKI. If the CA goes down, the entire organization goes down with it.

Yet, implementation of strong authentication remains one of the most urgent next steps for Active Directory administrators concerned about security.

Put Your Eggs in More Than One Basket

BoKS Access Control for Desktops and Microsoft Active Directory combined provide network and security administrators with a flexible solution in which each technology is utilized for its special strengths in a complementary fashion. With BoKS Access Control for Desktops providing strong authentication services, protecting your Active Directory assets, and providing a smooth path for PKI rollout, Active Directory is used for what it does best: directory services.

BoKS Access Control for Desktops for Authentication

Improving the quality of your authentication schemes is an obvious next step. But it can be a difficult and a very expensive one along a rocky road. BoKS Access Control for Desktops helps by removing some ugly bumps, allowing you to achieve major improvements with small steps.

Ideally, the costs involved in establishing the identity of a user should match the estimated value of knowing that identity. Of course it would not make sense to invest in advanced techniques to secure logon to a system that only

“Security risks multiply as a company integrates its systems. The challenge is to meet the differing security needs of enterprise resource planning, supply chain management, and customer relationship management systems.”

Gartner, November 2003

holds information that is publicly available anyway. The fact is however that many organizations commonly use plain passwords to protect information whose value and confidential nature merit strong authentication. The substantial efforts required from the very start when implementing such solutions are often deemed disproportionate to the value they bring, a view reinforced by the lack of flexibility inherent in many such solutions. Administrators should be able to provide strong authentication for accounts that need strong protection while allowing less complex and less costly alternatives for others.

With available authentication techniques, there is a relation between costs and deployment pains on the one hand and confidentiality on the other. Below, the red graph illustrates the path towards stronger authentication with standard tools, token and smart cards. Added confidentiality typically costs, and each additional step on the ladder costs even more.

BoKS Access Control for Desktops introduces a flexible set of options going from passwords only over virtual cards and tokens to smart cards or extended smart cards, which makes initial efforts easier to handle as illustrated by the green graph above. At the same time, it offers a manageable way to improve the quality of your Active Directory authentication without having to make your Active Directory login itself certificate-based.

Imagine you could add a new strong authentication option to the ones listed above. If users were to continue to use the least expensive method, plain passwords, but these passwords would consist of extremely long, randomized character strings and would also be changed very frequently.

There is only one problem: No human user would be prepared to type nonsense passwords of, for example, 16 characters, let alone change them several times a day. However, BoKS Access Control for Desktops willingly takes on the task, enabling you to enforce the most detailed password policies. It even handles your password changes for you. And your users don't even have to know their gobbledygook Windows passwords since BoKS Access Control for Desktops takes care of the Active Directory login procedure as well.

Flexible PKI-Based Credential Store Protection

Naturally, BoKS Access Control for Desktops means costs as well. However the ease of use and simplified roll-out compensates and makes PKI-enabling your organization a realistic perspective. From day one, it provides your users with a secure container using PKI techniques in which your secrets are safely maintained, even your Active Directory passwords. The interaction with Active Directory for password updates and automatic password synchronization is handled in the background without any user interaction.

The BoKS Access Control for Desktops security server can be configured to initiate frequent password changes to be propagated to your Active Directory,

“We don’t manage specific compliance efforts at the corporate level. Business managers are responsible for identifying and addressing risks. We only ask them to inform us about control issues they’ve identified. But we don’t track their actions... we rely on audit tests to confirm we’re ok.”

Global Risk Manager, Top 25 Financial Institution

making unauthorized access to your Active Directory as unlikely as if you had secured Active Directory itself with a much more expensive alternative for strong authentication.

Flexible Rollout of Certificate-Based Authentication

If you were to require smart cards for Windows logon using Active Directory alone, you would have to take one very big step the first day.

With BoKS Access Control for Desktops, you can phase in strong authentication step-by-step without changing user credentials.

A BoKS Manager security server or one of its Replica servers handles user logon requests. BoKS Desktop resides on each client machine and provides strong authentication and access to user credentials. It also provides single sign-on to Microsoft Active Directory (or Novell NDS).

Logon Modes

The solution can be set up to take over initial Windows logon. This configuration is referred to as Integrated Logon mode. In this mode, the user logs on to his or her machine using BoKS Desktop, which automatically and transparently handles the Windows domain logon in the background. The user's Active Directory password can be synchronized with BoKS Desktop credentials in different ways to ensure seamless integration with Active Directory. The logon sequence is as follows:

- The user authenticates to BoKS Desktop using one of the available logon methods.
- The BoKS Desktop communicates with BoKS Manager, which authenticates the user.
- If the authentication succeeds, the user's credentials are downloaded, and the user is authenticated to Active Directory.

Alternatively, BoKS Desktop can be used to protect specific credentials only. This configuration is referred to as On Demand Logon mode. In this mode, the user logs on using the normal Windows logon functionality and authenticates to BoKS Desktop only when access to given credentials is required. For example, if BoKS Access Control for Desktops is used to distribute keys for signing, with On Demand Logon a user will be prompted to authenticate to BoKS Desktop as soon as he or she wants to sign an email.

Logon Methods

BoKS Desktop can easily be configured and reconfigured to operate with stronger authentication methods as needed, from regular passwords to strong

“We spent the last 18 months implementing HIPAA across the organization. Now we’re starting over again with SOX. More (regimes) will follow as we look at industry trends.”

SOX Program Leader at a leading health care provider

authentication using tokens or smart cards. Regardless of logon method, one and the same Credential Store is used. In other words, the container holding the user certificates and the certificates themselves remains unchanged, but the method used to open the container may vary.

Regular Passwords

Passwords are used to cryptographically protect virtual cards. Administrators can configure BoKS Desktop to enforce different types of password policies.

RSA SecurID Token Passcodes

Using RSA SecurID tokens, the password strength of the user's virtual card is improved. This method provides two-factor authentication by requiring a random, one-time passcode in addition to the user's normal password. The information is sent to BoKS Manager, which then uses an RSA ACE/Server for passcode authentication. BoKS Access Control for Desktops comes complete with support for RSA SecurID tokens with no need for extra client-side software. A working RSA ACE/Server is required for SecurID authentication.

PIN codes

Passwords used to open smart cards are usually referred to as PIN codes. Besides opening smart cards with PIN codes, BoKS Desktop can be used to enter PUK codes for unlocking blocked smart cards and for PIN code changes. PIN codes are the entry mechanism for Extended Smart Cards, since the smart card component has to be opened in order to unlock the virtual card.

Credential Stores

Credentials that are associated with a user must be stored in a secure and protected way. FoxT Technologies offers several different storage solutions built on hardware and software protection methods and devices. Using BoKS Manager, credential data is automatically synchronized. It is possible to select the degree of credential roaming allowed by allowing or disallowing client-side caching of credentials.

Smart Cards

A smart card is a physical device kept in the user's possession that contains a hardware chip that can store user credentials. In order to use a smart card, a reader has to be installed on the client machine. Smart cards are very secure cryptographic containers because a PIN code must be entered to gain access to the credentials and data. After a predefined number of failed PIN attempts, the smart card locks up. This feature makes smart cards immune to cryptographic attacks.

USB Tokens

USB tokens are a relatively new class of cryptographic devices. Technically, a

USB token is a combination of a smart card and a smart card reader in a common USB device. The advantage is that no reader installation is needed in order to roam between computers. A USB token works just as any smart card in conjunction with BoKS Desktop.

Virtual Cards

A virtual card is a symmetrically encrypted file that contains user credentials. As the name indicates, a virtual card duplicates the functionality of a smart card. This means that the virtual card contains separate storage areas for keys, certificates, and parameters. A virtual card can be used to store the same kind of information as a smart card, but does not have the memory constraints of the hardware-based smart card solution.

Extended Smart Cards

When a key pair from a smart card is used to encrypt a virtual card, you get an Extended Smart Card. As a result, the virtual card becomes a transparent extension of the smart card, combining the best qualities from both storage methods. The user experience is the same as with a normal smart card, but the space and management problems are resolved. All data parameters and new certificates can be placed in the Extension Virtual Card (the virtual card portion of the Extended Smart Card) for automatic data backup and storage.

Managing Lost Smart Cards and Key Recovery

If a user loses the smart card portion of the Extended Smart Card, the administrator can remove the smart card protection mechanism and assign a new logon method, for instance a normal password. The user can use the password to access the virtual card, where the user's credentials are stored, and can continue to use the credentials in this way until a replacement smart card is available.

Extended Smart Cards Protect Traveling Users

A user who loses his or her smart card while traveling may not be able to log on online to automatically download a new virtual card. Administrators can prepare for this event by leaving the virtual card password protection mechanism activated when creating the Extended Smart Card. The password is not provided to the user. If the user loses the smart card, he or she calls the administrator and obtains the password for the virtual card. This procedure allows the administrator to constrain the use of password authentication to emergency cases only.

Extended Smart Cards Provide Stability and Flexibility

Extended Smart Cards make it possible to use different authentication methods in a seamless way. Users can be provided with different authentication solutions over time, but their important credentials always stay the same. It is

also possible to have users with full-featured non-extended smart cards coexisting in a network with Extended Smart Card users. This makes it possible to migrate between smart card solutions at your convenience without massive hardware deployments.

Benefits of Extended Smart Cards

To appreciate the benefits of Extended Smart Cards, it is helpful to understand the strengths and weaknesses of smart cards and virtual cards. Extended Smart Cards combine desired properties from both smart cards and virtual cards:

- **Smart card storage limitation problems are solved.** New data is stored in the Extension Virtual Card rather than on the smart card.
- **Support for read-only smart cards.** In cases in which users are prevented from making changes to the smart card, such as identity cards issued by authorities, it is impossible to store parameters and additional keys on the smart card. Instead, these credentials can be stored on the Extension Virtual Card.
- **Support for devices without storage capacity.** Even devices such as mobile telephones and certain USB tokens that cannot do much more than provide an RSA key pair and encryption capabilities can serve as protection devices for Extension Virtual Cards.
- **Protection of smart card investment.** The functionality of existing hardware can be extended over time without replacing all of the smart cards.
- **Quick driver development.** Because less is required of the smart card, development of new smart card drivers is simplified. Some existing PKCS #11 modules may even be used off-the-shelf.
- **Support for multiple smart card devices** with the same level of system functionality. Since the smart card functionality is extended, it is possible for an organization to mix different smart card types and manage them in a uniform way.
- **Reduced administration.** If the smart card is the sole way of accessing a system and the sole bearer of the user's credentials, it causes administrative overhead when the user loses the smart card.

However, if the smart card is used only as a key to the Extension Virtual Card, it is possible to replace the smart card without losing any credential information. A new smart card can simply be assigned to the Extension Virtual Card, which allows the user to continue to access systems in the enterprise and user credentials stored in the virtual card.

- **Improved virtual card encryption protection.** An Extended Smart Card is much harder to attack cryptographically than a password-protected virtual card.

Frequent Password Updates to Protect Active Directory

Once clients are enabled with strong authentication using BoKS Access Control for Desktops, the password synchronization features of BoKS Manager can be used to secure Microsoft Active Directory accounts. The weakest link becomes radically strengthened when organizations change passwords frequently and use long, randomized character combinations.

BoKS Desktop can be configured to update the password of its Windows account whenever it has been changed server-side. BoKS Manager can randomize passwords and initiate scheduled password updates in Active Directory.

Thus, users will be authenticated using the flexible scheme for logon methods offered by BoKS Access Control for Desktops while their matching Active Directory identities are updated with long passwords that remain a secret between BoKS Manager and Active Directory. There is no need for users even to know their Windows passwords, since authentication to Windows is handled in the background by BoKS Desktop. Password policies that would be absolutely impossible to implement if normal users were to comply with them suddenly become an efficient tool to protect your Active Directory accounts.

So why not activate smart card requirements directly in Active Directory?

Admittedly, from a technical point of view and if you ultimately use smart cards only, some of the benefits organizations achieve using BoKS Access Control for Desktops could also be achieved in a Microsoft-only environment, issuing certificates using the Microsoft CA and deploying through Active Directory. However, network administrators in organizations using BoKS Access Control for Desktops maintain they had good reasons to go with FoxT :

- BoKS Access Control for Desktops offers tremendous flexibility both during the deployment phase and subsequently in operation, which makes PKI rollout a realistic and manageable task. Without BoKS Access Control for Desktops, it simply would not have been possible.
- Extended Smart Cards alone make the investment in BoKS Access Control for Desktops worthwhile and profitable, since smart card administration otherwise remains a constant maintenance headache and administration cost.
- The ability to switch easily from online to offline mode is a requirement in organizations where many users are mobile with their laptops. Credential caching in Windows is an unacceptable security threat.
- BoKS Manager is an extremely stable, reliable, and scalable security server with its own built-in CA. It has a proven track record, having been in use at some of the world's largest banks and manufacturing companies for more than a decade. If the BoKS Manager server goes down, one of its Replicas can be promoted easily to Master, taking over the role of the main server.
- If security is an issue, putting your eggs in more than one basket is a smart move.



FoxT
883 North Shoreline Blvd.
Building D, Suite 210
Mountain View, California 94043
www.foxt.com
650.687.6300

Copyright © FoxT. All rights reserved.
The document is provided for informational purposes only and the contents herein are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior permission.

FoxT logo is a trademark of FoxT, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.