

Accelerate The Benefits of Smart Card Deployments with ArcotID

Blended Smart Card/ArcotID rollout delivers strong authentication and digital signing rapidly and cost effectively to the enterprise



EXECUTIVE SUMMARY

Organizations are recognizing the limits of simple passwords as user authentication mechanisms and are moving to strong multi-factor alternatives. The hardware smart card represents one option: secure and multi-functional but expensive and requiring a long deployment calendar. The ArcotID™, an innovative alternative, delivers the functionality of the smart card completely in software without requiring any new hardware or upgrades to the existing desktop.

By adopting a blended deployment plan combining ArcotID “software smart cards” and hardware smart cards, organizations can benefit from reduced deployment costs by shortening the time to transition from passwords to strong authentication and digital signing, covering all members of the extended enterprise. A blended deployment simplifies the user experience without requiring any changes to the applications that interface with either a physical smart card or an ArcotID.



STRONG AUTHENTICATION IS REPLACING SIMPLE PASSWORDS

Security experts, industry associations, and government regulatory groups recommend upgrading security from simple username/password combinations as the authentication mechanism for online applications, particularly those involving confidential information or high transaction values. Organizations are taking note of this and are moving to multi-factor, “strong” authentication solutions to allow access to resources. With strong authentication someone must have at least two of the following to be verified prior to accessing resources:

- Something physical they have such as a token or a file
- Something they know such as a PIN or a password
- Something they are (biometric information, such as fingerprints)

Strong authentication can improve secure access to applications including web portals, VPNs, and e-mail. Some solutions also enable digital signatures on documents and e-mail. Digital signatures can be used to verify the authenticity of document (who created it), verify the integrity of a document (whether it has it been modified) and verify the authenticity of approvals such as a contracts, purchase orders, financial applications, etc.

HARDWARE SMART CARDS AND THEIR CHALLENGES

To begin moving to strong authentication, some organizations have begun to deploy multi-function hardware smart cards. These credit card-sized tokens can be used for physical facilities access, to log into network resources, or to store monetary value and be used at the cafeteria cash register. Hardware smart card solutions provide increased security but present a number of deployment challenges, including:

High Cost – In addition to the per-card cost, the deployment has to take into account the cost of card readers and drivers, the cost of shipping these devices to remote users, the cost of replacing lost or broken cards.

IT Resources - Installing and configuring card readers and card drivers on existing PCs requires considerable IT planning and resources. They also require help desk resources for training and supporting end-users.

Long Deployment Window – Most large organizations budget a multi-year deployment cycle (the average is 3-5 years) to upgrade all users to strong authentication using physical smart cards. A longer deployment time postpones the benefits of strong authentication:

- Until the last user is upgraded, some users still rely on username/password combinations. This adds security risks to the organization as a whole.
- ‘Print and sign’ processes for document approvals cannot be replaced by more efficient and cost effective digital signatures until every potential signer has a smart card.

Wasted Overhead – Most large organizations have a significant number of users who don’t work in the main facility and therefore have no use for the physical access and stored value aspects of the multi-function smart card. They require only logical access to information resources and are being “over provisioned” with smart card features they don’t need.

Alternate “Back Door” Access - Organizations that deploy physical smart cards require alternate access and support methods for those who forget or lose their smart cards. Falling back to username/password is a security risk; the delay in obtaining an alternate access mechanism after loss of a smart card impacts users’ productivity.

THE ArcotID SOLUTION ADDRESSES THESE CHALLENGES

The ArcotID solution offers an equally functional “software smart card” that combines rapid deployment, ease of use, cost effectiveness, and patented security. The ArcotID is a fully featured smart card, but delivered completely in software. Applications enabled for hardware smart cards work with the ArcotID – with no change at all. ArcotID

allows organizations to exercise control over who accesses what, when, and from where - with no requirement for new hardware, readers, or drivers. Blending ArcotID into a deployment brings these benefits:

Rapid Deployment - The ArcotID can be deployed much faster than hardware smart cards. Arcot’s fully self-service web provisioning system, Arcot RegFort, allows ArcotIDs and hardware smart cards to be issued to users and downloaded to their desktops with zero administrator assistance. Existing desktops don’t have to be upgraded nor do they need any new hardware to deploy the ArcotID.

Patented Security - Patented Cryptographic Camouflage™ technology helps the ArcotID resist typical attacks, including brute force attacks. For more information on this technology, visit the Arcot web site at <http://www.arcot.com>.

Intuitive User Interface - The ArcotID adds security without adding complexity. The user experience can be configured to look exactly the same as an existing username/password screen. Alternately, the user interface can be configured to look like a familiar bank ATM window. In either case, the underlying technology delivers strong authentication for secure access.

Flexible Usage Configuration - The ArcotID can be configured to look like a smart card or a one-time-password (OTP) generating token for a variety of applications such as VPNs that only support standard passwords and OTPs. ArcotID can be optionally configured to provide on-demand roaming and strong authentication from any desktop, including from an Internet kiosk.

Attractive Price - ArcotID costs significantly less than hardware-based authentication solutions. As a software-based solution, the ArcotID has no inventory costs, shipping costs, or hardware replacement and maintenance costs.

REDUCE DEPLOYMENT TIME AND ADD VALUE

A blended deployment of hardware smart cards and ArcotIDs helps organizations adapt deployment plans to reflect the easier and less expensive rollout of ArcotIDs for groups of users who only need the functionality and features of the ArcotID.

- Organizations may recognize that many users in the extended enterprise need access only to the network data and applications, but not to facilities or to stored value cards. One Arcot customer, a pharmaceutical company, indicated that nearly 60% of constituents that needed secure access were field employees, contractors and partners who needed only network access. They didn't need other access that hardware smart cards support. ArcotID was the perfect strong authentication solution for these users.
- Other organizations that are focusing on digital signing may determine that only a small percentage of users need to secure their digital IDs (identity certificate or credential) on hardware. A large majority could use digital IDs secured by ArcotID instead.
- Most organizations will need an efficient mechanism for issuing backup credentials to users who forget/lose their physical smart cards. A 'generic' temporary physical badge and their own 'personal' ArcotID for logical access and digital signing would get users productive again with no appreciable delay or overhead.

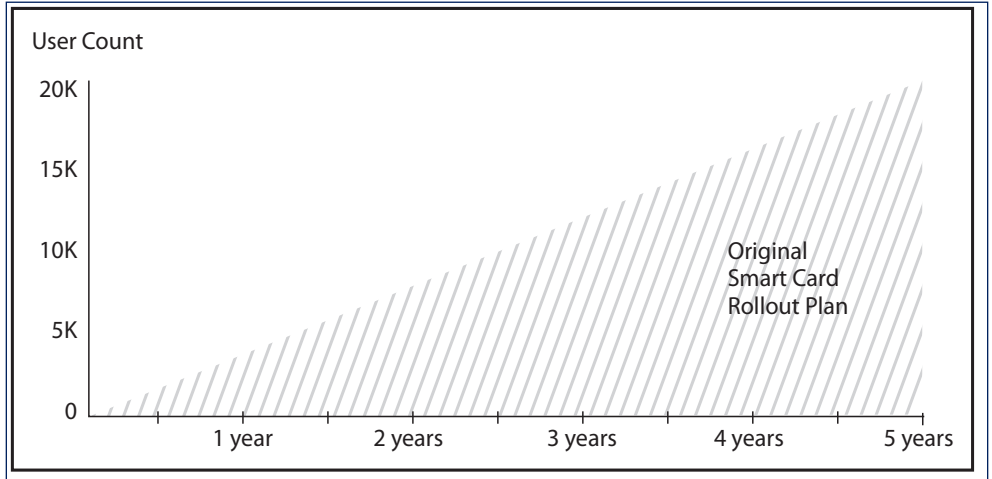


Figure 1 - Original deployment plan for hardware smart cards

SAMPLE DEPLOYMENT

Consider the complete deployment of hardware smart card solutions to the entire extended enterprise of 20,000 users. Figure 1 shows the deployment spread over a 5 year window.

The high costs of this deployment plan include the previously mentioned hardware and IT costs. In addition, a lengthy deployment time leaves the enterprise less secure during the deployment window. While hardware smart cards provide secure access for those who get them, weak authentication via username/password access will persist for others until everyone receives and enables their hardware

smart card. Thus a hardware-only deployment extends the period of reduced security for the overall enterprise.

To more quickly realize the benefits of strong authentication when accessing protected resources, the organization adds ArcotIDs to the hardware deployment. The ArcotID is rolled out far more quickly than smart cards – all with no additional hardware or PC upgrades. The simpler deployment usage translates to lower training and help desk costs. As Figure 2 shows, the ArcotID deployment is completed in a few months – enabling strong authentication for online access, plus the ability to digitally sign electronic documents.

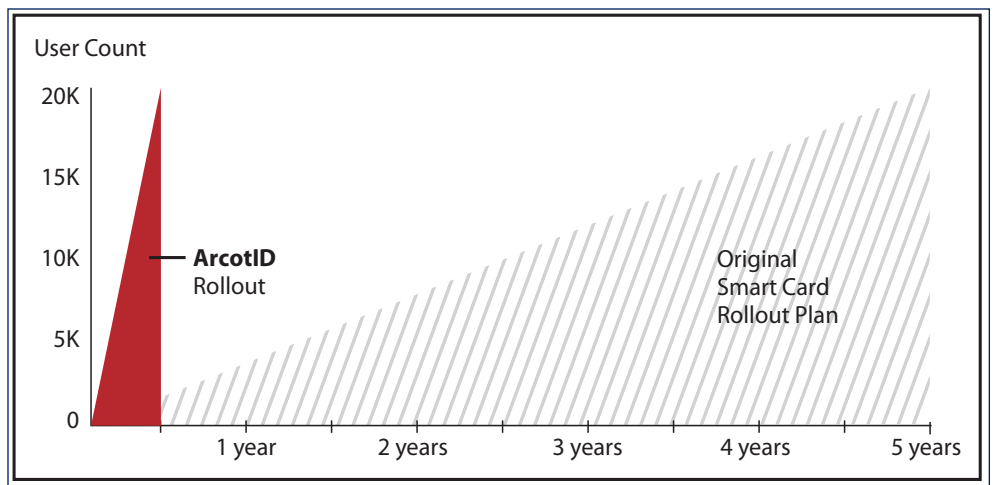


Figure 2 - Deploy Arcot ID to all users in a few months

Concurrently, smart cards are issued to those who need them – for example, users who work in a specific building or users whose digital IDs have to be held in hardware. Assuming this number is about 40% of the total population – 8K of the 20K total users – the hardware smart cards are deployed in a significantly compressed time frame.

Figure 3 represents a realistic approach to blend the ArcotID software and hardware smart card deployment – with all hardware cards issued by end of Year 3.

The blended smart card/ArcotID approach delivers several benefits:

1. All users transition from passwords to strong authentication by Month 6 instead of at the end of Year 5.
2. All users are enabled for digital signing in Month 6.
3. The organization enjoys significant cost savings from avoiding deployment of 12,000 smart card readers, drivers and cards to those who did not need that functionality.
4. The enterprise has a backup system in case users forget/lose their smart card or the computer containing their ArcotID.

A WIN-WIN SOLUTION: SECURITY SOLUTION MAPPED TO USER NEEDS

Organizations have recognized that they must migrate away from username/passwords and enable strong authentication for all their users in the extended enterprise – employees,

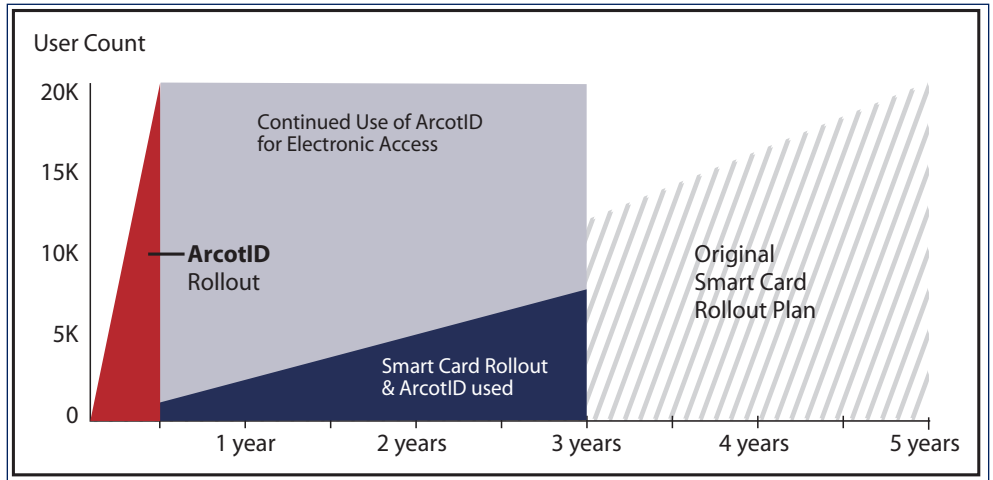


Figure 3 - Simultaneously deploy smart cards to the 8K users who really need them over 3+ years

partners, contractors and customers. The questions facing these organizations are:

- What authentication scheme do I use?
- How long will this deployment take?
- How much will this deployment cost?
- What are the security implications during the deployment?
- Are backup mechanisms required with the new authentication scheme?
- Do the backup mechanisms impact security? Do they impact user productivity?
- Do all my users need the same authentication scheme?
- Can all my applications be supported with the proposed authentication scheme?

A multi-factor authentication scheme based on smart cards addresses most of these questions. A deployment plan that blends both ArcotID (software smart cards) and hardware smart cards helps meet organizational security goals more quickly and cost effectively than hardware alone. These advantages include a faster deployment, reduced hardware expenditures, leveraging of existing investments, and expansion of strong authentication to additional applications today and in the future. To learn more visit www.arcot.com or call 408-969-6100.

ABOUT ARCOT SYSTEMS

Arcot is a leading provider of strong two-factor authentication and digital signature solutions. Arcot's software offerings are compliant with industry standards including 3-D Secure, IdenTrust, and SAFE. Over 10,000 banks and other enterprises use Arcot to protect the identities of millions of employees, partners, and consumers worldwide. Organizations also work with Arcot to comply with regulations or legislation such as FFIEC, Sarbanes-Oxley, and HIPAA.

Arcot Systems, Inc. | www.arcot.com

Corporate HQ | 455 West Maude Avenue | Sunnyvale, CA 94085-3517 USA | (408) 969-6100

Arcot International | Trinity Court-A | Wokingham Road | Bracknell, Berkshire | RG42 1PL UK | +44 01344 668 280

Arcot Deutschland GmbH | Schulweg 7 | D-82343 Pöcking | Munich, Germany | +49 8157 997793

Arcot, the Arcot logo, ArcotID, Arcot KeyFort, Arcot RegFort, Arcot RiskFort, Arcot SignFort, Arcot TransFort, Arcot TrustFort, Arcot WebFort, Arcot Universal SAFE Signing Interface, and Arcot Universal Client, are trademarks or registered trademarks of Arcot Systems, Inc. in the United States and other countries. Other trademarks are the property of their respective owners.

Copyright © 2006 Arcot Systems, Inc. All rights reserved.

Part Number: SB101-1006-05

