GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

ActivCard: the Strong Authentication Wild Card

GIAC Security Essentials Certification
Practical Assignment version 1.4b
Option 2 – Case Study in Information Security

Prepared by: Conrad Spielman

October 22, 2002

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Abstract

A strong authentication policy is essential to reducing the vulnerability of passwords at critical entry points to an organization's network. The organization in this study established a two-factor authentication policy for remote access seven years ago, and managed a consistent implementation of challenge/response tokens and RADIUS authentication for remote access to the corporate network. Over the years, the policy has remained in force while application requirements continued to expand. Today, the two-factor authentication policy must cover new requirements, such as an upgrade of analog remote access to VPN access, system administrators crossing internal zones, customer access to applications running in a DMZ, and executive access to extranet applications like Outlook Web Access from airport kiosks. There are many issues with the current challenge/response token implementation, and the IT group has decided to look at alternatives that can meet current and future requirements.

This case study will focus on current environment issues, analysis of requirements, a review of current authentication technologies, and the selection of a solution for implementation. An important component of the analysis is the authentication matrix, which plots the organization's authentication gateways against authentication strength policy. I reviewed current technologies offered by synchronous token, smart card and biometric solution vendors. The resulting choice of a smart card solution using ActivCard authentication software and hardware was based as much upon the flexibility to meet future requirements as the ability to solve the current problem. Like adding a wild card to problematic hand in a poker, ActivCard strengthens your authentication "hand" in a number of areas, such as, remote access, web authorization, PKI certificate storage and Microsoft Windows domain authentication. I took the ActivCard solution through evaluation and pilot in order to arrive at recommendations for enterprise implementation.

Current Environment

Strong Authentication Policy

The organization in this case study has established a comprehensive security policy and conducts assessments on all new applications for adherence to this policy. The security policy stipulates that all access from or across an untrusted zone to a trusted internal zone requires two-factor authentication. Strong passwords alone are not enough for access from an untrusted zone.

Authentication, the establishment that the user's presented identity is genuine, can be conceptually divided into three factors. These factors can be theoretically classified as Knowledge, Possession and Being[1], or in more practical terms, something you know, something you have and something you are. The

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Knowledge factor includes authentication methods committed to memory, such as, a password or Personal Identification Number (PIN). The Possession factor includes some physical item that can be carried about and the theft or loss of which will be noticed, such as a token, key or smart card. The Being factor includes any physical characteristic that can be biometrically measured, such as, fingerprint, voiceprint, or iris scan. With two-factor authentication, the user must authenticate with any two of the three possible authentication factors.

Current Strong Authentication Solution

The organization currently employs a two-factor authentication solution for analog remote access, utilizing challenge/response tokens with a RADIUS authentication server. Since implementation seven years ago, the tokens have been deployed to over 4,000 staff members who travel or work from home. The user types a PIN to unlock the token. Within a minute the 8-digit challenge from the RADIUS server must be entered into the token, which produces a one-time passcode, an 8-digit string that must be returned to the RADIUS server for authentication. Either hardware or software tokens have been deployed depending upon user preference. The hardware tokens are preferred by users with more than one notebook or workstation, while the software tokens, though limited to a single notebook, are preferred by non-technical staff and executives because the interface with Windows dial-up networking eliminates keying in the eight-digit response.

Unfortunately, the current solution cannot meet the growing requirements for strong authentication. The product has been owned and marketed by five different vendors in the past eight years. Over the past two years, there have been long periods when the tokens were unavailable for purchase. The user database for the RADIUS server was recently upgraded from Paradox to SQL Server, but the vendor does not yet offer an LDAP interface. And web authorization systems like Netegrity SiteMinder do not provide built in interfaces to this authentication server, while they do offer built-in interfaces to products like RSA SecurID or ActivCard. It was clear that the organization was assuming substantial risk without a strong vendor commitment to keep the product competitive.

Besides shaky vendor support, many users had voiced dissatisfaction with the tokens. The hardware tokens were too bulky to fit in a wallet or on a key chain, and were often forgotten or misplaced on business trips. With a 6-digit PIN and 8-digits for both challenge and response, the hard token user has to enter 22 digits overall during authentication. Of course, with so many digits, authentication failures can be frequent and frustrating. With this in mind, the system requirements for a public kiosk email access project stipulated that executives would not be carrying hard-tokens, but would use Web-based certificates instead.

The advent of e-business and zoned architecture has created new requirements. A strategic B2B application running in a DMZ could add tens of thousands of external customers who are required to use strong authentication. With the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

current solution, tokens are in too short supply and the RADIUS server lacks proven scalability for this application. Internally, the IT group has implemented a zoned architecture to separate development, production and corporate networks by firewalls. Unfortunately, the RADIUS server does not have built-in interfaces to the most common firewalls, i.e., Cisco PIX and Checkpoint. The IT security group is looking for a simpler solution for authenticating administrators and developers as they cross between zones.

Authentication Strength Requirements

I tried to take a wide and long approach to requirements analysis. The organization was looking for a solution that would meet a wide a set of application requirements that would last longer than any point solution. The first step was to build a tiered-authentication matrix, which would set authentication strength requirements for each network zone and system gateway. Authentication strength would be defined as 1-factor, near-2-factor, 2-factor, or 3-factor. For each gateway, both current authentication strength and desired strength would be defined.

A word must be said about what could be called near-2-factor authentication and how it differs from true 2-factor authentication. An example of near-2-factor authentication is the "software smart card", a hardened software container for a digital certificate, which can be deployed to roaming users across the Internet. The software container resists brute-force attacks on the PIN, just like a real smart card. But it is in the factor of Possession that near-2-factor authentication schemes come up short. A smart card or token has a unique, physical presence. It cannot be copied, and its loss or theft will be noticed. However, near-2-factor solutions can still play a part in an organization's authentication strategy, particularly with Internet applications where deployment of smart cards, tokens or biometric solutions is not practical.

With these distinctions in mind, I developed the tiered authentication matrix. When considering access gateways where a user's identity should be challenged, I included the usual suspects, i.e., remote access, internal firewalls between zones, workstation connections to the NOS, wireless access points and Internet applications. The incidents of September 11th widened my perspective to include physical aspects such as parking lot, building and secure room access. Although a separate physical security department manages physical access, I decided the division between physical and IT authentication systems was more political than technical, and with the new awareness of terrorism, I find that physical security has been transformed from a "minor nuisance" to "everyone's business."

The first version of the matrix only specified the 4 authentication strengths as columns. It was to be used as a guide for product evaluations, so it should not reflect solution types. But the first version of the matrix does denote both current implemented authentication strength and the desired future authentication strength requirement if there was any gap between the two. After evaluations and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

product selection, a later version of the matrix would feature an expanded number of columns that feature solutions. A sample from the matrix follows:

X = Present **O = Future**						
Resource	**Gate**	**Role**	**1-Factor**	**near-2-Factor**	**2-Factor**	**3-Factor**
Physical Access						
	Parking Lot		X			
	Building		X			
	Restricted Room		X			
	Computer Room				X	O
Remote Access						
	Analog RAS					
		Admin			X	
		Developer			X	
		User			X	
	VPN					
		Admin			X	
		Developer			X	
		User			X	
	Kiosk					
		Admin			X	
		User			X	
Wireless						
	802.11B WAP					
		Admin	X			
		User	X		O	
	Wireless PDA email					
		User	X		O	
Zones						
	Internal Firewalls					
		Admin			X	
		User			X	
	DMZ Firewalls					
		Admin			X	
		Developer			X	
	Extranet Apps -					
		Admin		X		
		User		X		
		External		X		
	Internet Usage					
		Admin			X	
		User	X			

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MS Windows						
	Workstation					
		Admin	X			
	Server					
		Admin	X			
		Developer	X			
	NT 4.0 Domain					
		Admin	X			
		Developer	X			
		User	X			
	W2K Domain					
		Admin	X		O	
		Developer	X		O	
		User	X		O	

Technology Evaluation

After the tiered authentication matrix was compiled, I evaluated the leading strong authentication solutions and selected one of those solutions to pilot.

Knowledge solutions

Passwords or PIN's - These can be defeated by dictionary look-up, brute force attack or social engineering.

Personal information - Items such as mother's maiden name, social security number or city of birth can are known by more than one person and can be easily be defeated by research.

Private answers to common questions - Often used to recover forgotten passwords, a user must register for this authentication service by supplying secret answers to common questions that will not be forgotten, e.g., the name of one's first girlfriend/boyfriend or favorite sports team. The more questions the user is challenged with, the stronger the authentication.

PassFaces - This is a relatively new type of authentication technology that involves remembering a series of pictures of human faces. For example, when users register for an authentication service of this type, they will be sequentially presented with five photo portraits of complete strangers and asked to remember something about each one. Then they will go through a training period of a few minutes where they practice picking out these faces when presented in line-ups of previously unseen photo portraits. After this training is complete, the five remembered faces would no longer be considered total strangers by the mind. The user should be able to recognize each of the five remembered photos when challenged by 5 line-ups of 25 photos at the time of authentication. This recognition has been tested to persist in the mind not only for a week, but for years.[2] The human mind develops its ability to recognize faces in infancy, an

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ability that is not fully understood. Perhaps because users don't understand how they remember faces so effectively, they don't trust using it as an authentication method. Whatever the reason, PassFaces, the only product to utilize this authentication type, has yet to gain wide acceptance for website authentication.

Possession solutions

One-time Passcode Tokens

The one-time passcode token dynamically generates a numeric passcode that is sent from a client, to a firewall, VPN gateway or web server, which forwards the passcode to an authentication server. If the passcode matches that which the server expects from that specific token, the server accepts the authentication request. If the passcodes do not match, the request is rejected. There are three types of one-time passcode tokens, time-synchronous, event-synchronous and asynchronous (challenge/response.)

The time-synchronous token, typified by RSA SecurID, uses an internal clock to generate an unpredictable digit string, which changes every minute. The RSA ACE authentication server uses the same clock and string generation algorithm. The user must also enter a PIN as a second factor, which along with the digit string becomes the passcode. Even if a valid passcode was sniffed by a hacker across the network and was resubmitted within the five-minute window, it would be rejected, because the server will not accept the same passcode twice. To protect the user's PIN, it is imperative that the passcode be sent across an untrusted network over an SSL connection.

Event-synchronous tokens use a counter to generate the digit string. Each time the user performs an event, like pushing a button on the token, the counter is incremented. The server keeps track of a similar counter for each user. Otherwise, the time and event-synchronous tokens are similar. Both types face similar vulnerability to rejected authentication attempts if the token and server get out of synch. With time-synchronous rejection, the clocks could be out of synch by more than 5 minutes. With event-synchronous, the user could be playing with the token and accidentally increment the counter too many ticks in front of the counter on the server.

The challenge/response or asynchronous token, typified by PassGo Defender, differs from a synchronous token in that the RADIUS authentication server issues a challenge digit string to the user. The user unlocks the token with a PIN and then enters the challenge. The token produces a response string, which the user submits as the one-time passcode. The advantage in this approach is that the PIN is not submitted across the network so the passcode response does not need to be encrypted. The disadvantage is that the user needs to type both the challenge and the response correctly, twice as many digits, which leads to more errors.

One-time passcode token technology is relatively stable and has been widely implemented for strong authentication solutions for the past ten years. RSA SecurID is by far the market leader with more than 8 million worldwide users.[3]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

But these tokens can only perform one function, that of producing one-time passcodes. I was looking not just to improve on the present challenge/response token solution, but to pilot a solution that would provide strong authentication with Network Operating System login and digital certificate storage.

Smart Cards

With a chip that houses a processor and storage, smart cards provide a platform for secure, portable storage of a user's digital certificate and private key. The card is inserted in a smart card reader and unlocked with a PIN, clearly providing a 2-factor authentication advantage over storing the certificate on the PC hard disk. Once unlocked, the certificate can be used for encryption or authentication. Smart card solution vendors like ActivCard have added other authentication options, such as Windows NT 4.0 login and one-time passcode generation. These additions, plus the fact that a smart card can be used for building access, make smart cards the most flexible strong authentication option.

There are some major drawbacks with smart cards. Hardware smart card readers must be installed at the workstation. Provisioning and managing multiple applications on each card is more demanding than token administration. Of course, this means a smart card solution will be more costly to implement and manage.

Some experts would debate whether the smart card should also function as a corporate photo ID card. Andrew Phillips states, “Although such usage of smart cards has benefits, if the card carries information about the holder, the company or both, an opportunist who finds a lost ID card could use this information. For maximum security, cards should carry only the text offering a cash reward for returning lost cards to a P.O. box address.”[4] But in this scenario, a user must carry both a photo ID card and a smart card, and they would be more likely to leave the smart card in a reader when they leave the building. The best compromise would be to include a photo and a unique corporate design, but no clue as to company name or address on the card.

USB smart keys

The USB smart key plugs into the PC USB port and functions like the combination of a smart card and a smart card reader. The advantage over a smart card is that no hardware needs to be installed. The disadvantage is that the USB port may be located in the back of the PC, which makes frequent insertion and removal awkward. Also, the USB key cannot do double duty as a building access card.

Soft-Tokens and Soft-Smart-Cards

The software-only solution that comes closest to meeting the full status of Possession is the software token that can only be installed by floppy disk, and must be uninstalled by the same-keyed floppy disk before moving it to another machine. Of course, this floppy disk copy protection scheme is cumbersome to administer in-house, and far too awkward for Internet applications. It also has the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

limitation in that it resides on the hard disk. Therefore, if the notebook PC is lost or stolen, so goes the software token, whereas a hard token or smart card should be carried separately from the notebook.

Biometric (Being) solutions

In an evaluation of biometric technology for Congress, as mandated by the USA Patriot Act of 2001, The National Institute of Standards and Technology (NIST) came to four preliminary conclusions:

- Iris scans rely on proprietary technology that makes evaluation of their accuracy difficult.
- Fingerprints work pretty well, but accuracy needs to be better for wide scale use.
- Facial recognition technologies aren't mature yet.
- No biometric technology works well enough to be relied on by itself.[5]

This sums up the general perspective of IT in regards to biometrics for general user authentication. There is a lot of hope and promise, but very few cases of enterprise deployment. Possibly the first use of biometrics we will see widely deployed is as a second authentication factor that could replace PIN's. Fingerprint scanning and smart cards could be complementary technologies. Privacy advocates are concerned about central storage and network transmission of fingerprint template data. Storing the fingerprint template locally on a smart card and authenticating the live fingerprint locally quell these privacy concerns. A fingerprint reader and smart card reader can easily be combined into the same small desktop unit. With this synergy in mind, ActivCard recently purchased Ankari, a biometric authentication vendor, and is working on combined suite of applications and devices.

Product Selection

I selected ActivCard for a pilot because it provided a flexible platform for implementing many of the technical solutions described above. While most smart card vendors have focused on the smart card as a payment platform, ActivCard's client authentication software and RADIUS server have established them as a leader in the smart card authentication space. In fact, the Department of Defense has selected ActivCard as one of the major vendors involved in a mega-project to issue smart cards to 4.3 million persons in all branches of the armed services.[6] Using ActivCard technology would enable the following 2-factor authentication solutions in our organization:

- One-time passcode authentication for VPN, dialup, firewalls, and wireless access points.
- Strong authentication for Windows NT 4.0 and 2000 domain login

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Secure container for PKI certificates

These could be implemented using the following products

- ActivPack 4.4 - a RADIUS server that provide Authentication, Authorization and Accounting. It works with one-time passcodes generated from any ActivCard smart card, token, or USB smart key.
- ActivCard Gold 2.01 - a Windows client application that manages the smart card's PIN and authentication applications.
- ActivCard 16K crypto-flex smart cards OEM'd from Schlumberger
- ActivCard smart card readers (PCMCIA and USB) OEM'd from SCM
- ActivCard synchronous tokens
- ActivCard USB smart keys
- ActivCard Simple Sign On Pilot - an add-on to ActivCard Gold which allows seamless interface with the Nortel Contivity VPN client

Pilot & Implementation

The objectives of the pilot were to present the following solutions on a single smart card:

- Remote Access strong authentication using Nortel Contivity VPN
- Entrust Certificate strong authentication
- Windows Domain strong authentication

Preparation: Installing ActivCard Gold client and ActivPack server

In preparation for the pilot, the ActivPack server and ActivCard Gold client needs to be installed and configured. These instructions are not comprehensive (for that, check the vendor manuals), but, rather, focus on key configuration points that are essential to a secure configuration.

ActivPack 4.4 setup tips:

- Install on Windows 2000 server on Intel-based server with appropriate configuration for production duty, e.g., RAID-5 disk array, dual processors, redundant power supplies and fans. Partition the drive during Windows 2000 setup for an operating system partition and an application partition. Change the letter of the application partition from D: to E:.
- Apply the latest tested service packs and Microsoft security patches. Remove IIS, and any unnecessary services. Apply a security policy template that has been hardened as much as possible.
- Install ActivPack 4.4 from CD or the latest version supplied by the vendor.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

    - Change the installation destination from the default to a folder on the E: drive.
    - Select all three components: the Administration Console, the Server Configuration utility and the CreateDB utility
- Run the ActivPack Server Configuration utility
    - Change the ActivPack shared secret, user ID and password from the default to meet security policy. The shared secret is used for encrypting communication between the ActivPack server and any administration consoles on other workstations. Besides protecting login to the console, the user ID and password are used to create the database encryption key.
    - Change the DSN ODBC user ID and password and make note of them. You will need to create this account on your SQL Server (or other ODBC compatible) database.
- Move the databases from MS Access to a more robust platform like MS SQL Server by using the ActivPack Create Databases utility.
- Run the ActivPack Administration Console
    - Within the console, add an authentication server and a gate. The first server will be the one you have just installed.
    - Change the RADIUS shared secret from the default and make note of it and the RADIUS port (default 1812). You will use the shared secret and port when configuring the Nortel VPN server.
- In order to use One-time Passcode authentication, Windows authentication and Entrust certificate authentication all on the same card, an **undocumented tweak** is required because of different password strength requirements on these platforms.
    - On the ActivPack server, edit the following file: E:\ActivCard\ActivPack\Admin\DefaultGold.spl
    - Change the following line:

      PINLengthMax: 8

      to

      PINLengthMax: 25
- Install ActivCard Gold on the ActivPack server. This is required in order to install a smart card reader on the server USB port, which will be used for initializing the first user smart cards.
    - Choose custom install
    - Change default install folder to E: drive.
    - Turn off all options except for the ActivReader USB Connection, the

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ActivCard Gold Base Services and the Documentation.

- After the install is finished, plug the USB card reader into the server USB port.
- Reboot.

<u>ActivCard Gold setup on a notebook</u>

The objective is to install ActivCard Gold to support a USB or PCMCIA smart card reader, with Windows network login, Entrust certificate container and one-time passcode enabled.

- Choose custom setup
- Select only the following features:
    - Network Login:
        - Dial-Up Client
        - Windows Network Login
    - Digital Certificates
        - Microsoft CAPI Support
        - Entrust Client Support
    - Smart Card Reader Drivers
        - ActivReader USB Connection
    - ActivCard Gold Base Services
        - ActivCard Gold Base Services
        - Quick Fill
    - ActivCard Gold Documentation
- Finish the install.
- Insert the smart card reader in the PCMCIA slot.
- Reboot.

Remote Access Strong Authentication

The objective is to use the ActivPack RADIUS server to authenticate remote access via Nortel Contivity VPN with ActivCard Gold generating the synchronous passcode. The Nortel Contivity VPN switch needs to be configured with a new RADIUS server and a new user group.

<u>Configure the Nortel Contivity switch</u>

- Upon accessing the web-based administration for the Contivity switch, click on the left-hand navigation menu to select “Servers”, “RADIUS Auth”. Make sure you toggle CHAP authentication and fill in the primary IP address, port number and RADIUS shared secret. These values should be the same as configured in ActivPack.
- In order to verify these settings, scroll down to the bottom of the page and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

click “RADIUS Diagnostic Report”. A secondary web page will pop up that verifies the settings are correct and the link to the ActivPack RADIUS server is functional.

- Select “Profiles”, “Groups” from the navigation menu. Add a new group.
- Once the new group is added, click the Edit button beside its name.
- Scroll down until you see the IPSec section, then click the Configure button.
- Scroll down to the Authentication section. Check the “User Name and Password” option. Type in the Group ID and Group Password. This same group and password will be used in configuring the Nortel client.
- Save the configuration.

Create User and Smart Card on ActivPack Server

Each user needs to be created on the ActivPack server, and a unique smart card needs to be initialized so that it only works for authenticating that user.

- Run the ActivPack Administration Console from the server or from any remote workstation on which the console has been installed.
- If necessary add new group.
- Set the Initialization Parameters for the group. This includes
    - Maximum number of failed authentication attempts before the card locks up
    - Initial PIN code value.
- Then add a new user.
- Once the user is added, select the user's icon.
- Insert a new or erased smart card in the reader.
- Click the token initialize button. The smart card's unique serial number should appear in the token SN text box.
- Click Initialize ActivCard Gold button. The card will be initialized for this user to be authenticated by ActivPack.
- Note the initial PIN value for communication to the user. Label the card with the user's name and/or user ID, but, of course, do not put the initial PIN on the label.

Nortel Contivity VPN Client configuration

- Install the Nortel Contivity Client, accepting all installation defaults.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

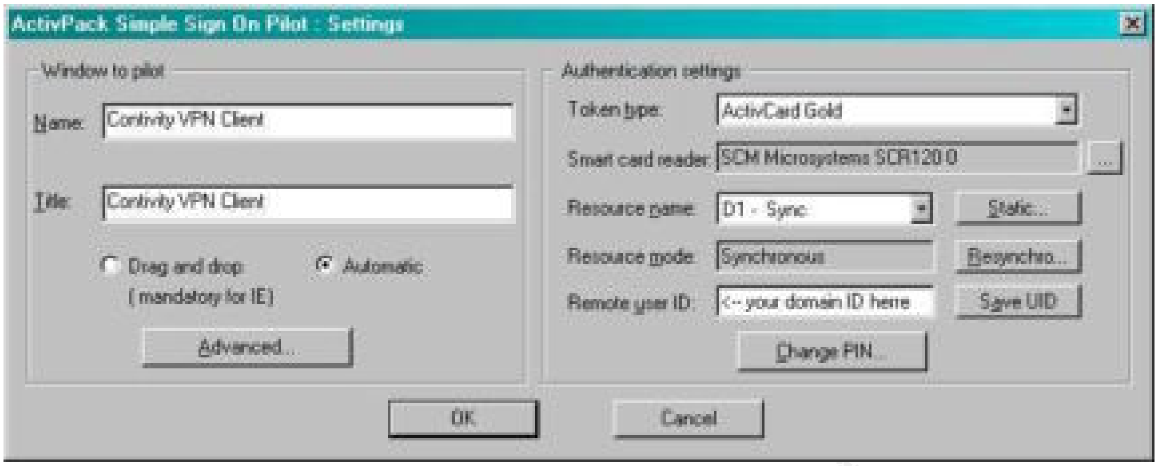
- Run the Connection Wizard.
- Create a name “ActivPack VPN” and description for the profile.
- Choose Hardware or Software Token Card as the authentication type for this connection.
- Choose the “Response Only Token Card” as the type of card, which means we will be using synchronous rather than challenge/response mode. ActivCard supports either mode, but synchronous is faster.
- In the Token Group Information dialog box, enter the ActivPack user ID that was assigned to the smart card. For Token Group ID and password, enter the group name and password created for the group on the Nortel Contivity switch.
- For Destination, enter the hostname or IP Address of the Contivity switch.
- For Dial-up Connection, select “No, I do not want to dial first.”
- Click Finish to complete the wizard.
- Important: Create a shortcut for this Contivity client configuration. Use this shortcut whenever you need to launch this configuration with the ActivCard Simple Sign-On client. This will prevent accidentally launching the Contivity client in any other mode with the ActivCard Simple Sign-On client.

ActivPack Simple Sign On

The ActivCard Simple Sign On Pilot (SSO Pilot) simplifies two-factor authentication by transparently sending the synchronous one-time password to the RADIUS server. The user only needs to enter the local smart card PIN for authentication. The SSO Pilot takes care of the rest.

- Install the software from the Clients folder on the ActivPack Server.
- Select install for All Users (HKEY_LOCAL_MACHINE).
- From the Start | Programs menu, choose ActivCard | ActivPack Client | ActivPack Simple Sign On Pilot.
- Notice a new key icon has appeared in your systray.
- Right click on the key icon and select Settings.
- Click Add…

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.


ActivPack Simple Sign On Pilot : Settings

Window to pilot

Name: Contivity VPN Client

Title: Contivity VPN Client

○ Drag and drop (mandatory for IE) ● Automatic

Authentication settings

Token type: ActivCard Gold

Smart card reader: SCM Microsystems SCR120 0

Resource name: D1 - Sync

Resource mode: Synchronous

Remote user ID: <-- your domain ID here

- Enter "Contivity VPN Client" in both the Name and Title fields.
- Token type is "ActivCard Gold".
- The Smart card reader should automatically select the reader you have installed.
- Resource name is "D1 – Sync".
- Resource mode is "Synchronous".
- Remote user ID is your ActivPack user ID.
- Click Advanced…
- Info to check is "User Name".
- Before challenge is "Challenge:".
- Without token is unchecked.
- Script is "<PWD><ENTER>".
- Click OK, OK, Close.

<u>Using the Contivity client with SSO Pilot</u>

- Establish a connection to your ISP.
- Insert your smart card in reader.
- Run the ActivPack VPN shortcut for the Contivity client, which you previously saved to your desktop.
- When prompted, enter your smart card PIN.
- The Contivity client will flash on and off as SSO Pilot transparently fills in your synchronous password, which is passed to the VPN switch and authenticated by the ActivPack RADIUS server.
- Your VPN session is active when the Contivity icon appears in your systray.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Entrust Certificate Strong Authentication

The objective is to load the Entrust profile to the smart card instead of the PC hard disk. The advantage is that the profile becomes portable for those using multiple workstations. It also provides strong authentication, because you must have the card and know the PIN.

Before beginning, it's **important** to note that the password you assign to your Entrust profile during the registration (or recovery) process will become the PIN on your smart card. Once the Entrust profile is loaded to the smart card, if you change the PIN, the Entrust profile will be inaccessible, until you also change the profile password. This means that the password strength rules for the Entrust profile must intersect with allowable values for a PIN. If your Entrust password rules require a minimum of 8 characters, with at least one uppercase and one lowercase character, you cannot have an 8 digit PIN on your smart card.

Even though ActivCard will allow you to have a PIN with upper and lowercase characters, it's a good practice to keep PIN's numeric, because some points of authentication may only have a 10-keypad. For instance, ActivCard sells the ActivReader, which looks like a token with a 10-keypad and a sleeve for a smart card. Slide in the smart card, and the ActivReader becomes a standalone token for synchronous RADIUS authentication. But use of this token requires a numeric PIN.

With this in mind, the ActivCard administrator and the Entrust administrator must come to an agreement on Entrust password strength rules for the group that will be loading their profiles on smart cards. I would advise setting the Entrust rule to allow all-numeric passwords with a minimum of 8 digits, but some organizations may require increasing the length to 10.

The procedure to load the Entrust profile to the smart card is:

- Make sure you included Entrust digital certificate as one of the options during the custom install of ActivCard Gold that was described earlier in this paper. You can run ActivCard Gold Utilities to check.
- Also make sure you followed the undocumented tweak to change the PINLengthMax parameter to 25 in the DefaultGold.spl file on the ActivPack server during initial configuration.
- Use Entrust Automated Registration Authority (Auto/RA) to create or recover your profile.
- When the Entrust create/recover wizard asks, "Where would you like to store your Entrust profile?" select the "Store profile on smart card" option. You still need to specify a folder on the hard drive, because some support files will be written to that location.
- Enter a name for the profile, usually your name or user ID.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The wizard will prompt you to create a password. Hopefully, the advice above was followed and you can enter an all-numeric PIN and pass all the password strength tests.

Windows Domain Strong Authentication

The objective is to add Windows NT 4.0 or Windows 2000 domain 2-factor authentication using the same smart card that is already configured for remote access and Entrust.

Adding Windows NT Domain Login to the card

- Insert your smart card in the reader.
- Double click on the ActivCard Gold icon in the systray. The icon looks like a blue smart card in a reader.
- The ActivCard Gold Utilities will launch.
- If prompted, enter your PIN.
- Right click on the Network Login folder
- Click Add > Windows NT Login…
- Enter your NT user ID and domain name.
- Select Lock workstation for card removal behavior. For total smart card security, check the “Only unlock with smart card” option.
- Click the “Password is user defined (static password)” radio button.
- Enter your current NT domain password. If you use special (non-printable) characters in your password, click the Advanced… button to enter them.

Adding Windows 2000 Domain Login to the smart card

To take full advantage of Windows 2000 smart card authentication, you must use certificates rather than passwords for login. Unfortunately, Microsoft only recognizes user certificates issued from a Microsoft PKI Certificate Authority (CA). This means a certificate issued by an Entrust, Baltimore or RSA Keon CA will not be recognized by the Windows 2000 smart card authentication. ActivCard Gold just functions as a container for the Microsoft certificate, leaving authentication to the Kerberos logon protocol. Procedures for implementing a Microsoft PKI and Windows 2000 smart card authentication is outside the scope of this paper, but is well documented in the *Windows 2000 Server Resource Kit.* [7]

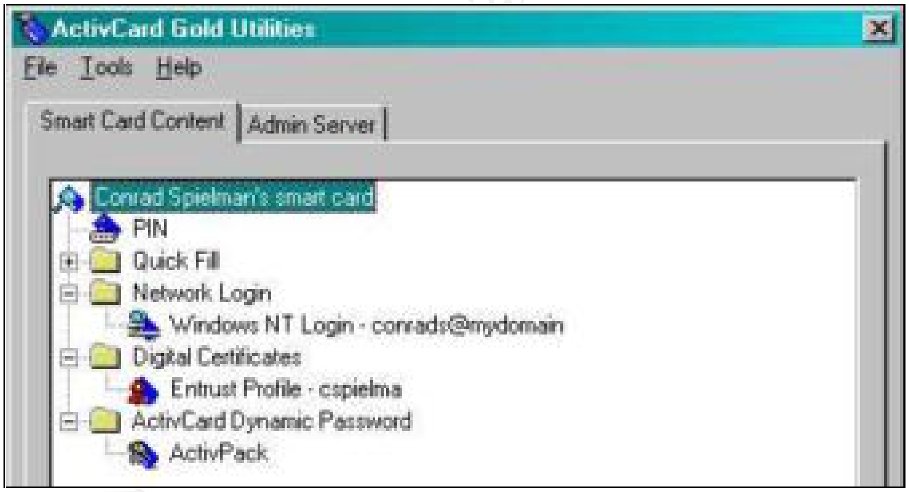
Pilot Results

Let’s look at a typical scenario that demonstrates all three types of strong authentication with the use of one smart card. I am ready to leave for work in the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

morning and turn on the radio. There's an accident on the freeway again, and traffic is backed up for miles. I set up my notebook with a wireless card in one slot and sit down at the kitchen table with a cup of tea. After the warning banner, Windows 2000 prompts me for my password. I slip my smart card into the card reader in the other PCMCIA slot. The prompt changes from "Password" to "PIN". I enter my 8-digit PIN on the keyboard, and ActivCard logs me into my notebook with cached NT domain credentials.

I need to check my email at work and browse the traffic report, so I launch the Nortel Contivity shortcut called "ActivPack VPN" on my desktop. I'm prompted for my PIN again. The wireless card seems to be working fine with my wireless DSL router and DSL modem, because within ten seconds the VPN connection is active, without having to type in the one-time passcode. (SSO Pilot did it for me.) During startup, the Entrust login window opens automatically, but I ignore it. I launch Microsoft Outlook and peruse my inbox. The status from last night's intrusion detection scans catches my eye, so I double-click on it. As usual, it's S/MIME encrypted, so the Entrust login window pops up again. I enter my PIN, take a sip of tea while the email is decrypted using my private key from the smart card. There are some serious issues I need to address about last night's scans. I can see it's going to be a rough day, but at least strong authentication with my smart card has worked without a hitch.



Conrad Spielman's smart card
- PIN
- Quick Fill
- Network Login
  - Windows NT Login - conrads@mydomain
- Digital Certificates
  - Entrust Profile - cspielma
- ActivCard Dynamic Password
  - ActivPack

The scenario above sounds too ideal to be true, but in fact, my daily experience has been much like that now that most of the configuration kinks have been worked out. Also, I am aware that the Windows NT domain authentication, even though it is 2-factor, is a show of strength that can be circumvented. I can still login to Windows with my 1-factor password and avoid using the smart card. But as part of the pilot, we wanted the users to get the feel for the convenience and security of Windows login with a smart card in preparation for an Active Directory implementation next year.

One of the challenges of certificate management on ActivCard Gold is the size of the Entrust Profile. Entrust does not allow one to download just the private key

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and the certificate to the card. Instead, one must download the Entrust profile, which includes additional code that facilitates Entrust's user-friendly applications. The Entrust profile will not co-exist on the same card with any certificates from other PKI vendors. So if you use Entrust for secure email, but also want to use Microsoft certificates to login to Windows 2000, you will have to choose one or the other.

Another challenge is the speed of smart card access. Users familiar with file and email encryption using an Entrust profile on the hard disk will be dismayed by the additional time Entrust Express or Entrust ICE require to read from the smart card chip. The average delay is about 45 seconds, which quickly becomes frustrating for any user who encrypts or decrypts just a few files per day. Since other PKI vendors only load the private key and certificate to the smart card, this read access delay should be less evident than with Entrust.

With the current rollout to 50 pilot users, users are informed of the drawbacks of moving their Entrust profile from the hard disk to the smart card. The choice is then left to the user. It is also possible to recover the Entrust profile back to the hard disk at a later date if the user is impacted by the smart card read access delay.

Conclusions

The objective of this project was to analyze requirements, evaluate strong authentication products, and deliver a pilot implementation. The primary requirements were strong authentication, flexible implementations, and stable technology. ActivCard smart card authentication solution was the best match for this organization's requirements.

This pilot proved that with ActivCard Gold and ActivPack, a user could possess a single smart card that delivered:

- Remote Access strong authentication
- Entrust strong authentication
- Windows strong authentication

That looks like three of a kind, and in this game that is not a bad hand.

List of References

[1] "The Challenge of User Authentication," Ankari White Paper, Ankari, Inc., http://www.biowebserver.com/downloads/PaperUserAuthentication.pdf

[2] "The Science Behind Passfaces", Document Revision 2, September 2001, Real User Corporation, http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] "Press Release: RSA Security is a leader in wireless user authentication market", http://www.rsasecurity.com/worldwide/pr/uk/010322.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[4] Phillip, Andrew, “Planning for smart cards”, January 29, 2002 http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2843255,00.html

[5] Jackson, William, ”NIST identifies good and bad points of biometrics”, Government Computer News, 08/26/02; Vol. 21 No. 25, http://www.gcn.com/21_25/security/19773-1.html

[6] Weisman, Robyn, “U.S. Orders Over 4 Million Digital ID Cards”, NewsFactor Network, October 26, 2001, http://www.newsfactor.com/perl/story/14429.html

[7] Microsoft Windows 2000 Server Distributed Systems Guide, Microsoft Press, 2000, 767 – 772.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.