Global Information Assurance Certification Paper

e-Provisioning: Business Software that makes a Case as an Enterprise Level IT Security Solution

SANS Security Essentials, GSEC Practical Assignment
Version 1.4, Option 1
Jonathan MacConnell
May 14, 2002

Comment:

Abstract

e-Provisioning systems are showing great p otential security benefits for the enterprise - sized corporation. Currently, such companies are faced with security concerns over internal security breaches and losses of small corporate assets that are difficult to track. e - Provisioning allows corporations to provision or de-provision employees, contractors and partners quickly. This saves time and money for IT staff, permits policy -based access control, and enables thorough auditing capabilities.

This paper is an introductory examination of e -Provisioning systems that will help the security or IT professional gain a broad understanding of the topic. In addition, it discusses the business case for an e -Provisioning system, reviews case studies, and examines leading providers.

1. Introduction

In the current economic environment, downsizing and layoffs have been the headline makers, and cost cutting has been the bottom -line driver. These conditions have proven fertile ground for the distribution of e -Provisioning applications that are re -pitched as the answer to key internal IT security for large enterprises. With the emergence of business - to-business services via web -based portals, this same software may be the answer to effectively manage access for an ever -increasing number of external users as well.

Recent survey responses highlighted internal security breaches as a significant threat to companies. The CSI/FBI survey has shown a significant drop in the number of companies reporting instances of internal security breaches over the last two years. In 2000, 7 1% of corporations reported an internal security breach. However, this figure dropped to 49% in 2001 and finally 38% in 2002. This reduction shows progress, but it still indicates a major problem, with an average loss of $300K annually for the 44% of respo ndents that could actually quantify these losses.

In June 2001, eWeek and Camelot IT Ltd., conducted the Camelot Network Security and Privacy Survey. They contacted 548 eWeek subscribers consisting of system administrators, IT managers/directors or CIOs/C TOs, to discuss the top threat to security.

> "… of those who reported a security breach within the last year, 57 percent said the breaches were caused by inside users accessing unauthorized resources, while 43 percent blamed accounts left open after an e mployee has left the company. Fully 21 percent of the respondents said their companies had been the victim of an attempted or successful break -in by an angry employee." [2] (Fisher)

In addition, enterprise-sized corporations are seeing significant annual losses due to their inability to track and retrieve small corporate assets such as laptops, cell phones, corporate calling cards, PDAs, etc. A recent article at FT.com cited examples of this, like a former executive selling his house with a corporate toll-free number intact, and of a UK company that paid health care benefits for 2,500 people for up to three years after they left. Another company estimated its losses of laptops to former employees as over 550K in a period of six months. This is a significant loss that is not realized by corporations or IT security professionals.

Prices on mobile assets are rapidly dropping and therefore less likely to be significant enough for companies to track. However, cell phones and PDAs are becoming more powerful and able to hold considerably more information. It is the information within these devices that causes their value to skyrocket. Most companies consider the loss of a corporate laptop as a catastrophic event, yet they are still losing other mobile devices without considering the greater implications. Adams and Heine of the Gartner group state that, "through 2004, enterprises without an IT asset management program in place to track and manage mobile devices will experience a 40 percent to 55 percent loss of IT assets..."[4]

e-Provisioning providers claim that they have the solution to both internal security breaches and corporate asset losses for large-scale enterprises. Currently, this technology is not economically available to small or medium sized businesses. However, analysts forecast that e-provisioning service providers will exist in the future to meet this need.

2. What is e-Provisioning?

According to Business Layers, a leading provider of e-Provisioning solutions, "e-Provisioning streamlines the allocation of digital resources across the enterprise. By aligning business needs with IT resources, once allocated, these resources remain digitally connected as people move throughout an organization. At the appropriate time, the resources are systematically, securely and automatically removed." [5]

In basic terms, e-Provisioning is a subset of identity and access management software. It is a directory based security management system that acts as a middleman between your current enterprise systems. For example, when a new employee is hired, a change is made in the HR system, which is then detected by the e-Provisioning system. The e-Provisioning system then begins the business processes needed to provision resources for the new employee, as summarized in Figure 1. Business Layers' eProvision Day One software utilizes roles and groups to define what resources and access an employee has rights to. Based on this information, the other systems in the enterprise will be flagged to create the appropriate account access, work order, purchase order, etc.

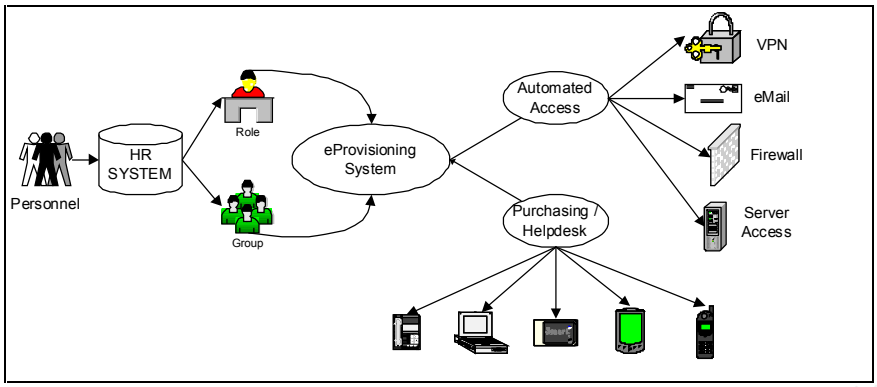

Figure 1: Simplified e-Provisioning System

This system also works in reverse, when an employee gets transferred or released from the company. The necessary change is made in the HR software, or directly in the e-Provisioning system and the change is replicated throughout the remaining enterprise systems. This also allows e-Provisioning to be used with partners, contractors, vendors and customers that are not part of the company, but that still need access to company resources on a non-permanent basis. This addresses the looming security issues being faced with the development of virtual business-to-business relationships.

2.1. The security benefits of e-Provisioning

In essence, the following issues define the security problem:

- Understanding "who needs access to what",
- Providing access to resources in a constant and widespread fashion,
- Automating the system access provisioning processes,
- Immediately de-provisioning access to resources, when they are no longer needed,
- Tracking and logging provisioning activities, the business trigger that caused them and who approved the provisioning.

e-Provisioning software addresses these security issues through a variety of methods. It provides an automated single point of control for all user access setup and corporate provisioning rules. Use of roles and groups allows consistent provisioning throughout the enterprise, independent of local anomalies. It can improve security for existing staff as their security rights are constantly monitored and aligned with their changing job and project responsibilities. Moreover, access privileges are automatically terminated when necessary, for example if staff members are released or business relationships are concluded.

Policy driven provisioning reflects corporate security guidelines, increases enforcement and is auditable. The comprehensive auditing capability is a significant benefit of an e-Provisioning system. This allows IT staff and managers to verify if there has been a true, intentional violation of security policy. How did this person get access, when, why, and by whose authority?

By providing an efficient and accurate method of de-provisioning, these systems address the potential loss of small corporate assets and the information they contain. It also reduces the chances of former employees to have access via old usernames and passwords.

2.2. General Benefits of e-Provisioning

Generally speaking, an e-Provisioning system is an easy sell to enterprise level business managers. Outside of security aspects, an e-Provisioning system has many general benefits based around the software's primary role. It is designed to have a new employee entered into the corporate IT directory and productive in a fraction of the time that current provisioning systems use. These provisioning tasks are automated when possible or streamlined and consistent when helpdesk personnel must be involved.

"Rogue Provisioning" required network administrators to manually add or change user information as IT resources are assigned, modified, or deleted. This was not only time-consuming, but error prone. An e-Provisioning solution updates the information in all relevant enterprise directories systematically. This automation of IT resource provisioning significantly improves the provisioning process, expediting the allocation and assignment of IT resources. It reduces administration time and costs involved in configuring all of the enterprise applications, services, databases, and networks. If these resources were provisioned manually, it would likely take weeks to complete the entire process. Many of these systems may even need to be re-visited after the user has discovered an error in the initial setup.

From a business perspective, managers can see a direct relation between business decisions like recruiting and the associated asset purchasing costs. IT managers can use system audits to find bottlenecks in the provisioning process and address them. Employees will spend far less time attempting to track down the resources they need to make them productive.

2.3. Business Case for e-Provisioning

It is often a challenge for IT managers to prove the business case for a new technology or investment. Business managers are infamous for not recognizing the need for information security solutions. A recent article in Information Security Magazine online clearly illustrates the increasing difficulty in making this business case.

> "Simply quantifying the need for security, or the mitigation of risk, isn't enough justification in the current economic climate. After taking the total cost for many security solutions--acquisition, employee training, administration and maintenance, and upgrade and replacement costs --the bill for adopting security solutions might seem prohibitive to the financial side of the business." [7] (Walker)

e-Provisioning providers are eager to show decision makers how quickly their solution gives a return on investment. Using the Business Layers Return on Investment

Calculator[6], the business case for e-Provisioning becomes quite apparent. Table 1 gives an example of how quickly this "security solution" proves its worth.

Table 1: e-Provisioning Return On Investment Example

Company Information Assuming a corporation of 30,000 employees with no annual employee base growth, 10% turnover and 10% moves, adds and changes (MACS).	6000 IT changes per year.
IT Provisioning Costs Average costs of IT labor with 100 IT support staff, 40% of their time spent on Moves Adds and Changes (MACS).	$339,360.00
Lost Productivity & Opportunity Costs Estimated loss of productivity costs for new employees and present employees due to lack of IT resources $3,5M. Loss of opportunity costs, what could have been done if the employees were free to work?	$8,400,000.00
Indirect costs Security breaches $300K, IT user support and fixing incorrectly configured systems $1.8M + Tangible exit costs for ($60K) = $2.1M	$2,100,000.0
Total Annual Costs & Savings Total $18M (assume the software can reduce these costs by 15%)	$2,700,000.00
E-Provisioning Costs Software cost, assuming 10 Modules to connect with other systems	$3,500,000.00
Return on Investment 3.5M Investment / 2.7M Savings Annually	16 months

The Return On Investment analysis of an e-Provisioning solution shows both direct cost savings and increased efficiencies. Fewer resources are needed to achieve more effective results. Resource tracking is also possible, providing you with complete and accurate records for interdepartmental financial reconciliation, or with vendors.

> "A substantial percentage (about 40% according to some industry studies) of your IT staff's time is taken up installing and configuring software and managing system changes related to business changes; new hires mean new computers (or freshly reconfigured ones), new assignments mean changes in user security policies, etc. Each of these changes means that not only does the IT staff have to manage the changes, but the employee is usually not productive while the system changeover is occurring." [8] (Business Layers)

At the end of employment or partnership you can immediately retrieve resources, and verify their return or service discontinuation. The added return on investment comes when you stop paying for those services immediately and guard against unnecessary expenses or loss. Security risks (and breaches) are reduced when provisioning is automated, reducing theft of company property or proprietary information.

3. Infrastructure

Each provisioning system works on a slightly different basic platform. However, they all have a system in place where the provisioning application exchanges data with enterprise directories, operating systems and applications, and legacy systems. In some cases, the IT system can communicate through existing standards, like Microsoft's ADSI and the remote access protocol for LDAP. Otherwise, the systems are connected through a secondary system called an agent. Communication from the enterprise system to the agent and the e-Provisioning system is via an XML document or comma separated ASCII file. A new standard called Active Digital Profile (ADPr) is being developed and is explained in section 3.2.

3.1. Agents

The agent acts as a translator that takes output from the legacy system and makes it understandable by the e-Provisioning system. It takes the same role going from the e-Provisioning system to the enterprise system. Access360 describes the role of the agent A the following: "Acting as trusted virtual administrators, agents translate requests and process configurations to the various systems they connect to via compressed and encrypted communication." [9]

Figure 2 shows a simplified version of how an e-Provisioning system interacts with different IT systems via agents.

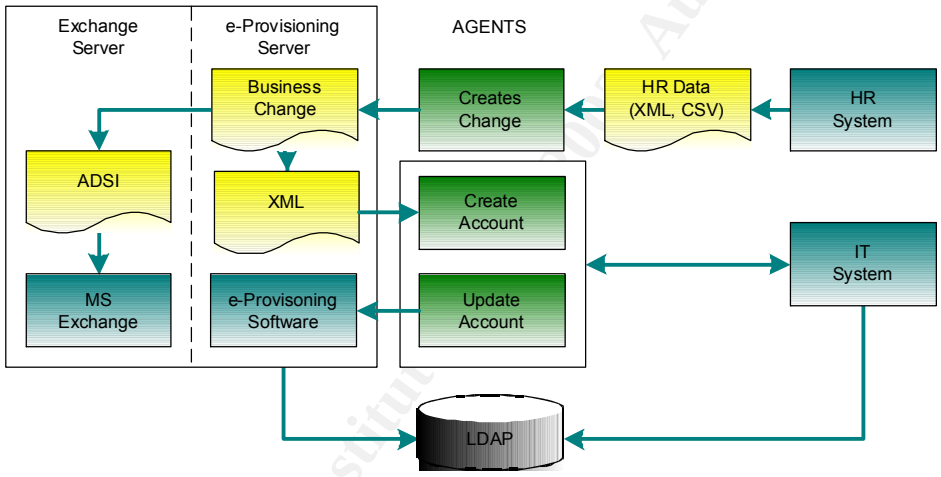

Figure 2: Simplified e-Provisioning Infrastructure

Business Layers calls these agents "eProvision Modules" (ePMs), while Waveset Lighthouse uses the term "gateways". These agents may be on the server that is hosting the e-Provisioning system, they may be on a stand-alone server, or they may reside on the server that is hosting the legacy system.

Currently, these agents are available from most e-Provisioning providers to many common security applications and enterprise systems. Business Layers, Waveset, and Access360 offer agents for their systems to Checkpoint Firewalls, SAP HR systems, RSA

Secure ID, LDAP, iPlanet, etc. If an agent does not exist, all providers have the capacity to develop custom agents.

3.2. Active Digital Profile Standard

Active Digital Profile (ADPr) is a proposed XML based open standard that is being developed for a method to communicate e-Provisioning information between two systems. ADPr is a framework for describing the structure and content of e-Provisioning information in an XML Document. The information can then be easily used by any application that makes use of XML, to provision resources or services. Business Layers writes that, "The Active Digital Profile Initiative will standardize interfaces and methodologies used to provision digital resources that span devices, applications and services within the enterprise and between enterprises." [10]

XML is a text-based markup language that is quickly becoming the standard for data interchange on the Web. As with HTML, you identify data using markup tags. But unlike HTML, XML tags tell you what the data means, rather than how to display it. Where an HTML tag says something like "display this data in *italics*", an XML tag acts like a field name in your program. It puts a label on a piece of data that identifies it as a specific field.

In the same way that you define the field names for a data structure, you are free to use any XML tags that make sense for a given application. Naturally, though, for multiple applications to use the same XML data, they have to agree on the tag names they intend to use.

The Active Digital Profile standard can be looked at as an agreement on the tags being used to define the e-Provisioning data and how to map them to the data used by their applications. It contains authentication, authorization, and administration information that is used to identify the sender to the receiver. It also contains context information that defines the scope of the actions being requested.

Business Layers introduced the initial draft of the ADPr specification. The members of adpr-spec.org are maintaining the specification. They will submit the final draft of the specification to OASIS at the appropriate time. The details of the specification are available at http://www.adpr-spec.com/profile/spec.htm .

4. Secure Communications

The connections between an e-Provisioning system and the remote agent use authentication schemes and encryption to keep information exchange secure. This section is an overview of what e-Provisioning providers are doing to ensure system security, but does not go into a detailed analysis of potential security weaknesses.

4.1. Secure Socket Layer (SSL)

Business Layers uses XML over HTTPS , 128-bit Secure Socket Layer (SSL) encryption between their e-Provision Day One product and the associated agents. Data is not passed

in clear text, but is passed over encrypted using https with the key generated when Microsoft IIS is initiated. Access360 also uses https SSL to securely transfer data.

eProvision Day One sends the ePM server a random generated run-time key (combination of machine sending request and Day One internal database key). When eProvision Day One activates an ePM it is activating it with the eProvision Day One run-time key. This run-time key changes all the time even if running the same procedure. eProvision Day One checks the request against this key.

SSL is a protocol developed by Netscape for transmitting private documents over the Internet. SSL uses a public key to encrypt data as it is transferred. Many Web sites use the protocol to obtain confidential user information, such as credit card numbers and can be recognized by the URL starting with https: instead of http:. More information on SSL can be found at http://developer.netscape.com/docs/manuals/security/sslin/contents.htm .

4.2. CHAP & Triple DES

Waveset Lighthouse authenticates using Challenge-Handshake-Authentication-Protocol, and triple DES encryption with a 168-bit session level key and a full PKCS5 cell padding.

CHAP sends an encryption key from a server acting as an authentication agent to the client program. This enables the username and password to be transmitted in an encrypted form and not in clear text. A detailed description of CHAP can be found in RFC1994 at http://community.roxen.com/developers/idocs/rfc/rfc1994.html. "Cheating Chap", a white paper on potential weaknesses of CHAP claims that it is not the right protocol for authentication over IP based networks. It can be found at http://stealth.7350.org/chap.pdf

Triple DES is a strong encryption scheme that encrypts data three times with DES encryption before sending it. There have been theoretical, but impractical weaknesses proposed for this method of encryption. More information on Triple DES can be found at or http://www.rsasecurity.com/rsalabs/faq/3-2-6.html.

4.3. General Security Issues

e-Provisioning providers point to internal security breaches of other corporate systems as a primary reason for an enterprise to consider this kind of a system. What is not mentioned is that the system in and of itself is a potential security risk that must be addressed.

Your security system is only as good as your weakest link. e-Provisioning providers openly train new administrators on their predominantly Windows based systems. As with most software, it is likely to have vulnerabilities when deployed 'out of the box'. Moreover, because it is the central administrative authority, access to this system likely means an entrance point to all systems throughout your enterprise. A wise security professional will recognize that any 'out of the box' system will need to be tested for vulnerabilities in a given environment and hardened appropriately.

5. e-Provisioning Providers

Currently, the major players in the e-Provisioning market are Business Layers eProvision Day One, Waveset Lighthouse, and Access360 enRole. Business Layers is currently recognized as the industry leader, but most analysts feel that this market and these products are still in their infancy. It is outside of the scope of this paper to do an in-depth comparison of each of these products. However Access360 does provide a good paper on selecting a provisioning solution. "The Provisioning Solution: Evaluator's Checklist" can be found at http://www.access360.com in their pressroom.

5.1. Business Layers eProvision Day One

Business Layers (www.businesslayers.com), is a leading provider of provisioning solutions. Their main product, eProvision Day One, enables a secured and systematic process for allocating digital resources to employees, contractors and business partners, ensuring that these resources are allocated and de-allocated quickly and efficiently.

Business Layers was the first company to define and address the provisioning market, and the first to define a provisioning standard. They have an alliance program that provides the framework to deliver the most comprehensive e-Provisioning technology solutions to Business Layers' customers. This alliance includes high profile security providers such as Checkpoint, RSA, and Netegrity. Current clients include Chevron, Syracuse University, and Ernst & Young.

5.2. Waveset Lighthouse

Waveset Technologies, Inc. (www.waveset.com), headquartered in Austin, Texas is a provider of identity management software that enables the secure control of business initiatives across enterprise, intranet and extranet environments. Their central product is called Lighthouse: Access Management Automation solution. As with other products, it offers Automated User Provisioning, Delegated Administration, and Audit and Reporting. However, it also offers account self-service and web single sign-on Management. Waveset also has a strong technology alliance with companies such as RSA, SUN, and Oracle. Clients include GMAC Financial Services, BNSF Railway, the State of Texas, and VISA USA.

5.3. Access360 enRole

Access360 (www.access360.com), headquartered in Irvine, California provides the company's flagship offerings, enRole and Access360.net. As with other products it ensures that the right people have access to the right resources, while maintaining corporate policies, individual privacy and security. Access360 has also developed a strong alliance with BioNetrix, Entrust, Netegrity, RSA, and Verisign. Customers include national and global corporations such as BP p.l.c., E*TRADE, OppenheimerFunds, Overseas Union Bank and Sony Electronics.

6. Case Studies

e-Provisioning is finding a wide audience with IT and Business managers in a variety of industries. Three examples of organizations that have selected an e-Provisioning system to help manage IT assets and user access are presented below.

6.1. Chevron

Chevron Information Technology Co. is deploying provisioning software/role based network access control for up to 31,000 users in 40 countries. They plan to deploy Business Layers' eProvision Day One software to create a centralized control to manage IT assets and user access to networks for employees and vendors.

Chevron expects it to solve recurring problems for the company. A key feature that Chevron is interested in is the ability to "de-provision" an employee when they leave the company.

6.2. Syracuse University & Widener University

Syracuse University is using Business Layers' e-Provision Day One system to set up 18,000 students that pass through each year. The main focus was to reduce costs and improve the efficiency and security by automating the back-end processes of managing students' access to digital resources.

Widener University in Pennsylvania was one of the first organizations to see the potential of an e-Provisioning system in the educational arena. Widener went from manually creating 2000 new computer accounts to automating this task with Business Layers' e-Provision Day One. This solution helped them virtually eliminate the need to create custom scripts to transfer data from the administration system. In addition, it reduced the number of human errors, which they spent weeks fixing, by 97%.

6.3. Burlington Northern Santa Fe Railway

Burlington Northern Santa Fe Railway uses Waveset's Lighthouse product to help them manage over 40,000 users identities and access rights. It took only 45 days to deploy this solution to hundreds of locations throughout North America. It acts as the central access control for MS Windows NT & Exchange Servers, IBM mainframes, mainframe based transport control system, and an IBM AIX system. BNSF feels comfortable that they could easily add 10,000 more external users to the system without radically changing the system that they have in place.

7. Summary and Conclusions

e-Provisioning is an emerging technology that has raised some interest in the security community. The fact that the number of internal security breaches and losses of assets is so high signifies the need for e-Provisioning to be accepted as an access management tool. This, coupled with the fact that an e-Provisioning system will save time for both new employees and IT staff, should make this attractive to business managers. In addition, the Return On Investment of an e-Provisioning solution can be quite rapid.

e-Provisioning applications are in their infancy. The future could see a more mature offering for enterprises and a service provider structure for small to medium sized businesses. It lends itself to ever-growing global corporations, and virtual business-to-business partnerships.

Therefore, by providing an efficient and accurate method of provisioning and de-provisioning, these systems address the potential losses that large corporations see every day. e-Provisioning systems may be the beginning of the end for the horror stories about ex-employees logging back into corporate systems or walking away with a PDA.

Acknowledgements
Marlin Pohlman, Schlumberger Network and Infrastructure Soluti ons
Seth Deutsch, Business Layers

References

1. Computer Security Institute."2002 Computer Crime and Security Survey", April 7, 2002 http://www.gocsi.com/press/20020407.html

2. Fisher, Dennis. “Mi ssing the Threats Under Their Noses”, eWeek, June 25, 2001. http://www.eweek.com/article/0,3658,s=701&a=8033,00.asp

3.Bird, Jane. “Ghost workers who haunt the bottom line”, FT.com, April 2 2002 http://news.ft.com/ft/gx.cgi/ftc?pagename=View&c=Article&cid=FT3EFWYZJZC

4. Adams. Patricia and Heine, Jack. “Is It Worth Tracking Mobile Assets Less Than $1,000?”, Gartner Group, 8 March 2001

5. “Frequently Asked Questions” , Business Layers, 2002 http://www.businesslayers.com/faq.asp

6. “eProvision Return -On-Investment Calculator”, Business Layers, 2002 http://www.businesslayers.com/roi.asp

7. Walker, Don. “The ROI of Information Security”, Security Management Magazine Online, August 2001 http://www.scmagazine.com/scmagazine/sc -online/2001/article/033/article.html

8. “eProvisioning and Security Management An Automated Approach to Managing Enterprise Resources”, Business Layers, 2001 http://www.businesslayers.com/eProvisioning_and_Security_Management.pdf

9. “Solutions, Agents”, Access360, 1999 -2002 http://www.access360.com/solutions.asp?section=solutions&sub section=agents&id=33

10. “ADPr: The Active Digital Profile”, Business Layers, 2001 http://www.adpr -spec.com/

11. Bray, Tim, Frankston, Charles, and Malhotra, Ashok, editors. “Document Content Description for XM L”, World Wide Web Consortium, July 31, 1998 http://www.w3.org/TR/NOTE -dcd

12. “Introduction to SSL”, Netscape Communications Corporation, 1998 http://developer.netscape.com/docs/manuals/security/sslin/contents.htm .

13. Simpson, William. "Request for Comments: 1994, PPP Challenge Handshake Authentication Protocol", Computer Systems Consulting Services, August 1996 http://community.roxen.com/developers/idocs/rfc/rfc1994.html

13. Krahmer, Sebastian. "Cheating CHAP", February 2, 2002 http://stealth.7350.org/chap.pdf

14. "Cryptography FAQ, What is triple -DES?", RSA Laborator ies, 2002 http://www.rsasecurity.com/rsalabs/faq/3 -2-6.html

15. "The Provisioning Solution: Evaluator's Checklist", Version2.1, Acess360, 2002 http://www.access360.com/pressroom.asp?section=pressroom&subsection=access360whitepapers&id=103