Global Information Assurance Certification Paper

Security Access between Multiple, Nationwide Facilities: Processes and Policies

Mark Stepongzi
GIAC Security Essentials Certification (GSEC)
GSEC Practical Requirements (v.1.4b)
4 September 2003

ABSTRACT

Today's technology has made it relatively easy to implement physical security in a single facility or on a local campus. However, defining, implementing, managing, and publishing the policies and processes required for company employees to obtain physical security across multiple, nationwide facilities remain a challenge. The policies dealing with privacy data are included in that challenge. This vision of having a person from one facility seamlessly gain access to another controlled-access facility, without requiring multiple badges, continues to this day. Included in that vision are processes that allow persons to have access to only those areas in which they are required to be in, while having all approvals done electronically.

INTRODUCTION

One of the major issues dealing with security today is what processes and policies are needed to successfully link security systems between remote facilities. These processes must include management buy-in of the solution, user acceptance, provide approval authority that allows local management to maintain self-autonomy, and publish the policies that enforce it all. Corporate and governmental policies may enter into the decision when pertaining to companies with government contracts and federal agencies.

Another area of great concern is dealing with privacy issues. Most state governments and the federal government have laws dealing with a person's privacy data and these laws must be followed. As the federal government continues moving toward the use of Smart Card technologies the potential for a large amount of privacy data to be contained in that card mandates that policies and processes be developed which are sensitive to privacy laws.

Today's telecommunication capabilities allows for the location of company's facilities to reside anywhere in the United States. Companies have been able to negotiate excellent telecommunication rates over the past 10 years so that permanent, high-speed telecommunication lines exist between all their facilities for the purpose of transmitting messages and data.

Unlike facilities that are located in close proximity, like a campus, facilities that are separated by long distances (as depicted in the picture above) computerized access systems will likely be different. Also, each facility will have there own management personnel, security staff, and mission. Processes and policies must be established to define how the requests of employees at other facilities are generated, how they are approved or rejected, and how they are implemented. This may be no easy task since each facility will have its own unique mission that dictates the types of policies needed for the applications they support.

INFRASTRUCTURE COMPONENTS

There are several infrastructure components that must be implemented prior to creating the policies and procedures required for security access by employees at remote facilities. These infrastructures will have their own policies and processes and thus, will not be covered in this paper. What should already exist are the following:

- **An email infrastructure:** Likely email infrastructures would consist of POP3 servers, Microsoft Exchange® servers, etc.
- **An intranet infrastructure:** A likely intranet infrastructure would be a routed network over dedicated communication lines with a firewall protecting the entry point to the Internet. Perimeter security is assumed to be in place.
- **A security background check:** All personnel associated with the management and administration of the infrastructure and security systems should have an annual security background check. The class and type of security check depends upon organizational requirements.

SYSTEM SECURITY REQUIRMENTS

Before beginning the discussion on policies and processes we first will identify a number of security system requirements that are needed by each facility. These system requirements are necessary since the policies and processes for security access by employees at other facilities depend upon them.

Looking from a high-level view, the first requirement will cover the use of Smart Cards. Note that any detailed requirements will depend upon one's specialized organizational needs. In general, Smart Card basic requirements will include the following:

- Be able to quickly identify employees (e.g., colored backgrounds surrounding employees pictures or possibly the entire card stock used) as:
    - Career Employees
    - Contractors
    - Visitors
    - Temporary Access Personnel (e.g., casual, forgotten badge replacement, etc.)
- Employ the latest Anti-Tampering and Anti-Counterfeiting Technologies, which could include the use of Micro printing, Hologram, Ghosting, Optical Visual Device Embedded, and Ultra Violet Characteristics (Pee, slide 7.)

- Capable of Bio-Technical uses, such as being able to contain the information relating to a person's fingerprint (Pee, slide 7.)

- Include a physical identification (i.e., an employee's picture) for easy visual identification.

- Include the following standards (Schwarzhoff, slide 2):

    - NISTIR 6887 – 2003 Edition, Government Smart Card Interoperability Specification version 2.1 due July 15, 2003.
    - The ANSI standard when published; submission of ANSI B10 scheduled for July 30, 2003.

- Include the capability for Cyber Identification (PKI) and possibly other applications as future technology permits.

- Be able to be read by proximity readers.

When tying policies and procedures to hardware and/or logical configurations the KISS (Keep It Simple Stupid!) principle must be followed. Hardware devices should have a standard naming convention and the hardware design should be as consistent as possible for all facilities. Where possible, choose security access systems that allow the operator to create their own logical names. This allows the same naming pattern to be used among different facilities and makes it much easier for the requester to identify what locations they need access. This is of great help if the employee requesting access (the requester) is unfamiliar with the facility.

The following table demonstrates how user created names can be implemented to simplify access areas within a facility. The user will first create ID's for areas within the building or even access points, such as the Main Entrance Main Door. Once all the areas or points are defined, then the user will define group ID's that group areas and points for ease of use. For example, the "Std" group ID would allow no access to any location. Subsequent groups would override the default access or add on to existing permissions. The groups ultimately would define access permissions for guests, visitors, system administrators, contractors, etc. It would be a nightmare to try and administer permissions based upon the lowest level of access and add to the confusion of any visitor at a facility.

Very Simple Example of Physical Access via User Created Group Id's										
		Access areas								
		Building Access					***Computer Room Access***			
User Created Group Id's	Base Group Id	Main Door	Work Room 1xx	Work Room 2xx	Work Room 3xx	Vault	Cmptr Room A	Cmptr Room B	Cmptr Room C	LAN Access

Std	---	N	N	N	N	N	N	N	N	N
Basic1	Std	Y	Y	---	---	---	---	---	---	Y
Basic2	Std	Y	---	Y	---	---	---	---	---	Y
SysAdmin1	Std & Basic1	---	---	---	Y	---	Y	Y	---	---
Visitor-1	Std	Y	Y	---	---	---	---	---	---	---
Sys S/W	Std	Y	---	Y	---	---	Y	Y	Y	Y
Contractor	Std & Basic1	---	---	---	---	---	---	---	---	---

Once the Group Id's are defined, then they are associated with a person. For example a person named Joe could be given Visitor-1 access permission and only have this permission starting 17 June and ending 18 June. Thus Joe would have access only to the main door and the first floor workroom (1xx). Multiple permissions are possible. An example of a person with multiple permissions is for a person named Tom to have both Contractor permission plus permission to the Vault, both starting on 1 January and ending 5 January. Thus Tom would have access only to the main door, first floor workroom (1xx), the LAN, and the vault, all starting 5 July and ending 9 July. Last, a permanent employee, Jane, could have both the SysAdmin1 and Basic2 permission accesses, starting 1 January and ending 31 December. Thus Jane would have access to the main door, the second floor workroom (2xx), the third floor workroom (3xx), the LAN, and computer rooms A and B, all permissions are for the entire year. Note that it is particularly useful to limit the time of day for employees based upon their job assignment. You may not want employees wandering around the facility after normal business hours while unescorted.

PRIVACY POLICIES

When dealing with privacy issues it is highly recommended that you consult with either your organization's privacy officer or your legal department. These groups should be brought into the process during early implementation because their participation is vital to its success. If there is no policy stating that participation is mandatory then develop one as soon as possible.

As with most computer applications, the Security System should ensure that data considered private is well protected. Most standard protection mechanisms, e.g. account/passwords for authentication, encrypted data on disk and over the network, physical security for the computers and video recorders, etc., should come standard with the security system. However, usage of Smart Cards poses interesting challenges. The first important aspect of using Smart Cards is that they can be lost or stolen. If stolen, then this represents a whole host of problems. Low on the list of problems created is the basic information contained on the outside of the card; a picture of the person along with the company they work for. Of greater concern is that the card may contain, in electronic format, the person's Social Security Number, the person's fingerprint data if bio-technical

systems are used, work address, and other personal data. A policy should be created that states that all data on the card must be encrypted.

The importance of protecting privacy data cannot be stressed strongly enough. One way of protecting privacy data is for employees to participate in that protection. Identity theft is a serious crime and it is steadily growing worse each day. Policies must be established that provide annual training to all employees on the seriousness of this problem, whether or not they have Smart Cards or request access to other company facilities. This required training must include information on how to identify when ID theft may be occurring, how to protect themselves from it, and what to do if it should occur. Smart Card policies should state that employees must report immediately any of the following instances to their managers:

- When they loose a company Smart Card.
- If a Smart Card is lost, any unusual notices of access requests to other facilities, either being approved or rejected, when they did not issue a request.
- Any unusual activities of a personal nature, possibly coming from the information located on the front of the card.
- Any other unusual business activity usually associated with the company Smart Card, if the card is lost.

When issuing a Smart Card it is recommended that a policy be implemented that persons receiving the card must sign a document stating that they received the card, that it may contain information of a private nature, what that information will be used for, and their acceptance of the company's terms and conditions on usage of the card. Coordination with the company's legal department will aid in the development of the appropriate wording of this policy.

SMART CARD POLICIES & PROCESSES

When developing policies and processes to govern the issuance and usage of Smart Cards a cross-functional management committee, comprised of all stakeholders, should be formed. This provides a mechanism for ensuring that adequate representation of all stakeholder viewpoints, resolution of disputes, and coordination of roles and responsibilities is accomplished. It also acts as a forum that allows all stakeholders a voice in what policies and processes are developed for use of Smart Cards and any applications the card may contain. There is only a finite amount of data the card can hold and not every application may be able to be implemented. The management committee will also facilitate the resolution of issues that may arise between stakeholders.

The guiding principle for the management committee should be based upon the Information Technology Governance process. This process simply states that the governance committee will be comprised of all the stakeholders for the

infrastructure or architecture being managed. Information Technology management will share decision making responsibilities with the other stakeholders. All stakeholders will share in the accountability for the success or failure of the infrastructure or architecture.

The management committee will oversee all technical and policy aspects of the Smart Card. The committee will decide what Smart Card standards will be used, what information will reside on the outside and contained within the card, and all policies starting from when the card is issued to when the card is returned. The committee will also be responsible for the processes governing the card's usage.

Policies and processes for managing Smart Card technology must document the processes for card administration and distribution from start to finish. These policies and processes should include items such as:

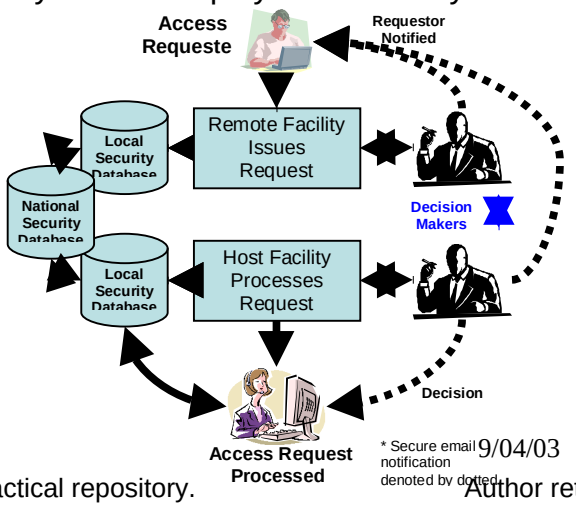
- Issuance of replacement/temporary cards due to cards becoming lost, damaged, or forgotten.
- Cards not surrendered upon termination or retirement.
- Accurately verify the identity of the recipient.
- Personal information that must be collected and stored securely.
- Personal information that must be securely maintained, synchronized among various applications, and is able to be updated with newer information.
- Infrastructure costs must be considered.

Organizations should consider how Smart Cards are to be managed. Whether a management committee is formed or not, they must determine a mechanism to coordinate the changes such a card technology will bring to the companies' business processes.

FACILITY MANAGER APPROVAL PROCESS

With the design of the system and supporting processes needed to manage the security system now defined, we will focus our attention in describing the processes and policies for this system to operationally work.

The overall approval process for allowing anyone not employed at a facility is for the facility managers or their designee to either approve or deny physical access to their facilities. No policy should state that a request for physical access from other facilities be automatically approved. Because facility managers are responsible for everything that happens in their facilities they have final approval authority for



determining who may have physical and logical access to their facility. The diagram to the right depicts what a high-level approval process might look like for physical access.

The previous diagram depicts the basic process flow where by requests are generated by the requester, approved by both facility managers, and followed by the decisions being sent electronically. With most companies reducing staffing levels these days it is important to reduce the number of people involved in the approval process. Thus procedures must be in place and agreed to by facility management that electronic requests are acceptable. Also, there will likely be insufficient staff to accompany company employees from other facilities during the times they are at the guest facility. This makes it very important that policies be in place that governs their visits.

The facility manager's approval process will likely be close to the following process: A fellow employee from another facility sends a request for access to a facility they plan on visiting. The request will include the access dates, times, and areas to be accessed. All requests and notifications are done via secure email. The approving authority decides whether to grant or reject the request and then notifies the requester of their decision. Requests approved are marked as "approved" and when the requester travels to that facility; their badge will operate at all the access points that were approved for. The requester will not have to sign a sign-in log nor wear a temporary/visitors badge. Normal security logs will contain information on areas the requester accesses and would be used if any audit is required. Smart cards would be used since they would contain Bio-Technical (e.g., digital finger prints) information required for use at any finger print scanner locations.

Requests rejected will have the request marked as denied along with the requester being notified. If the requester did show up at that facility after being rejected, then all requests for access attempts would be denied and logged. They should then contact facility management to discuss their access needs to that facility.

Some requests may have the request modified and in this case the requester is notified of the decision along with what access was approved. The requester would then have access only to areas approved by facility management. If access to other areas is necessary, then they would have to discuss the need for access with them upon arriving.

It is recommended that a standard facility access request form be developed for each facility. This will list the access points and access groups for each facility so the requester can select the access needed. This form will also aid the facility manager's decision on whether or not to grant the requested access. The policy that governs this form must mandate that all requests must use this request form. No access will be granted using any other form or from general email requests.

Each company will have their own unique form; the basic information should include the following:

- Person's name
- Business Address
- Business Phone Number
- Company representing
- Reason for the visit
- Employee they are visiting or sponsoring them
- Dates of visit
- Requested hours of access; starting and ending times
- Access permissions requested (facility dependent)

PUBLICATION OF POLICIES AND PROCESURES

It is extremely important and necessary that all policies and procedures be published. Without them published, then they would not be effective or enforceable. These publications must highly visible so users cannot state they have not seen them or were not aware they existed. It is highly encouraged that the legal department and possibly the company's employee relations departments be involved in the creation of the publications.

These policies and processes must be published so that all employees are aware of them. A message during the login process stating the company's privacy policy is, why the information is collected, and who may have access to this information is absolutely necessary. Also during in the message the email policies will be displayed. Once this message is displayed the user will not be allowed to go to the next login screen until they agree with the terms and conditions of the policies presented to them. This process is repeated every time they login into the computer system.

In addition, management support is critical since to all these policies and procedures. Their support is the "authority stamp"-signifying acceptance and must be publicized and vocalized at every opportunity.

CONCLUSIONS

Although a number of areas were covered where policies and procedures are need, there are six major points that this paper deals with. They are:

1. Processes and policies are necessary at all levels of security.
2. Smart Card management requires processes and policies for their life cycle management and usage.
3. Management must buy into all processes and policies published. They must show their support for them by following them themselves.

4. Management will retain approval authority for any access to their facility. This must be clearly stated in all the processes and policies published relating to employees requesting facility access.
5. Processes and policies must be publicized so there is consistency among the facilities and employees are fully aware of what is expected of them.
6. Privacy information must be protected.

LIST OF REFERENCES

Pee, Sonya. "The GSA Nationwide Credential Project." 28 May 2003. http://estrategy.gov/smartgov/information/jack%20finberg%20censured/sld007.htm

Schwarzhoff, Teresa. "GSC Update: Smart Card Manager's Meeting." 22 May 2003. http://estrategy.gov/smartgov/information/teresa%20schwarzhoff/sld001.htm

Smart Card Alliance. "Secure Personal Identification Systems: Policy, Process and Technology Choices for a Privacy-Sensitive Solution." February 2002. http://estrategy.gov/smartgov/information/secure_id_white_paper_feb02_dc.htm

General Services Administration. "Smart Card Policy and Administrative Guidelines." 20 October 2000. http://estrategy.gov/documents/101800_policy_handbook.PDF

Atoyebi, Vanessa. "Status: DHS Smartcard Initiative." 28 May 2003. http://estrategy.gov/smartgov/information/joe%20broghamer/index.htm

Schwarzhoff, Teresa; Dray, Jim; Wack, John; Dalci, Eric; Goldfine, Alan; & Lorga, Michaela. "Government Smart Card Interoperability Specification." 16 July 2003. http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

Smart Card Alliance. "Privacy and Secure Identification Systems: The Role of Smart Cards as a Privacy-Enabling Technology." February 2003. http://www.smartcardalliance.org/pdf/alliance_activities/Privacy_White_Paper_Feb03.pdf

Smart Card Alliance. "Using Smart Cards for Secure Physical Access." July 2003. http://www.smartcardalliance.org/pdf/alliance_activities/Physical_Access_Whitepaper.pdf

Federal Financial Institutions Examination Council. "Financial Services Modernization Act: Gramm-Leach-Bliley Summary of Provisions; Title V – Privacy." http://www.ffiec.gov/exam/InfoBase/documents/02-con-g-l-b_summary_of_provisions-010416.pdf

US Department of Justice; § 552a. "Records maintained on individuals: The Privacy Act of 1974; 5 U.S.C. § 552A As Amended." 1 June 2001. http://www.usdoj.gov/04foia/privstat.htm

Bedeli, Robert. "Privacy Act Guidance – Update." 24 May 1985. http://www.dod.mil/privacy/pdfdocs/PrivActGuidncUpdate_05241985.pdf

US Office of Management and Budget. “Appendix I to OMB Circular No. A-130 Federal Agency Responsibilities for Maintaining Records About Individuals.” http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html

Rutgers, The State University of New Jersey. “Social Engineering.” http://rusecure.rutgers.edu/secguide/soceng.html

Identity Theft Resource Center. “Workplace Id Theft.” http://www.idtheftcenter.org/workplace.shtml

ACKNOWLEDGEMENTS

Microsoft Exchange® is a registered trademark of the Microsoft Corporation.