

FSA Integration Partner Program
United States Department of Education
Office of Federal Student Aid



Interim Security and Privacy Architecture Report

Deliverable #124.1.1

***Task Order #124:
Security and Privacy Architecture Framework***

**Version 1.2
FINAL**

April 4, 2003

Confidential – For Official Use Only

Document Revision History

Version Number	Date	Author	Revisions Made
1.0	April 4, 2003	Hector G. Mezquida, Jesse Bowen	Initial version released
1.1	April 14, 2003	Jesse Bowen	Minor revisions; copy of project work plan added to Appendix
1.2	April 25, 2003	Jesse Bowen	Title modified – FINAL version

Table of Contents

1	Executive Summary	4
2	Introduction	5
2.1	Purpose.....	5
2.2	Project Scope	5
2.2.1	Task Order Objectives	5
2.2.2	Intended Use of the FSA Security and Privacy Architecture	6
2.3	Organization of This Document.....	7
3	Part A – Task Order Status Report	8
3.1	General Status	8
3.2	Progress to Date	8
3.2.1	Generic Security and Privacy Architecture Framework	8
3.3	Approach.....	9
3.4	Next Steps	9
4	Part B – Security Workshop Meeting Minutes.....	10
4.1	Introduction.....	10
4.2	Participants.....	10
4.3	Security Workshop Objectives	10
4.4	Security Workshop Discussion Summary	11
4.4.1	Introduction and Scope Discussion.....	11
4.4.2	Discussions about Security Architecture Topic Areas.....	13
5	Part C – Preliminary Security Business Objectives.....	18
6	Part D – Generic Security and Privacy Framework	22
6.1	Introduction.....	22
6.2	Scope.....	22
6.3	Security and Privacy Architecture Overview	23
6.3.1	Security Management	24
6.3.2	Security Processes.....	25
6.3.3	Technical Security Architecture	26
6.4	Technical Security Architecture Framework	28
6.4.1	Introduction.....	28
6.4.2	Criteria	28
6.4.3	Content.....	28
6.4.4	Identity & Access Management.....	29
6.4.5	Data & Privacy Protection	38
6.4.6	Application Services	43
6.4.7	Network & Perimeter Security.....	47
6.4.8	Monitoring Tools	51
7	Appendix	55
7.1	Diagram of Generic Security and Privacy Framework.....	55
7.2	TO 124 Project Work Plan.....	55

1 Executive Summary

This document constitutes a required interim deliverable for Federal Student Aid Task Order 124 – Security and Privacy Architecture Framework. Following an introduction to the project as a whole, this report consists of four major sections:

- Part A – Task Order Status Report – a description of the current status of TO-124, Security and Privacy Architecture Framework. This section includes an overview of the project approach and the next steps planned for the project. **(Page 8)**
- Part B – Security Workshop Meeting Minutes – a summary of discussions from the preliminary meeting held on March 6 to discuss the scope of the project and provide the business context for creating a generic security and privacy framework. **(Page 10)**
- Part C – Security Business Objectives – preliminary business objectives and security requirements identified by business subject matter experts. **(Page 18)**
- Part D – Generic Security and Privacy Framework – documentation of a conceptual, generic security and privacy framework to use as a discussion platform for developing an FSA Security and Privacy Architecture Specification. **(Page 22)**

2 Introduction

2.1 Purpose

This Interim Security and Privacy Report describes the status of TO-124: Security and Privacy Architecture Framework. This report includes an overall project status report and a summary of discussions held at the initial Security Architecture Workshop. This report also defines a draft Conceptual Framework for a Federal Student Aid (FSA) Security and Privacy Architecture.

The Conceptual Security and Privacy Framework defined in this report is an interim deliverable. This framework will form the basis for collecting and analyzing information from FSA business owners on business objectives and security requirements as input to development of the FSA Security and Privacy Architecture Specification. Final deliverables from the project will also include a Security and Privacy Architecture Implementation Strategy.

The Security & Privacy Architecture Framework project will provide several benefits to aid FSA with security design and regulatory compliance. The FSA Security and Privacy Architecture will simplify security design and deployment, and help achieve the following goals:

- Faster development of systems
- Identifying and reusing successful and proven security solutions
- Promote development of structured, systematic, and repeatable security controls
- Greater consistency of security controls across FSA systems

The Security and Privacy Architecture Framework will identify security functions that are candidates for deployment as security services. Security functions that can be deployed as architecture services available to systems across the FSA environment will:

- Decrease cost, effort, and risk associated with development of security functions
- Define technical services, components, and standards that will simplify compliance with regulatory requirements

2.2 Project Scope

2.2.1 Task Order Objectives

The ultimate aim of the Security and Privacy Architecture Framework project is to increase the effectiveness of FSA in the following critical protection areas:

- Integrity – Prevent data theft from FSA and maximize transactional accuracy.
- Confidentiality – Prevent unauthorized viewing or alteration of sensitive data.
- Availability – Prevent service disruption.
- Accountability – Provide for clean security audits.

To advance these goals, the current Task Order will create the following project deliverables:

- Conceptual Framework for Student Aid Security & Privacy Architecture.

- Security & Privacy Architecture Framework Specification.
- FSA Security & Privacy Architecture Implementation Strategy

This work is based on the following key assumptions:

- FSA must balance business requirements, security requirements, and regulatory requirements.
- Business input to development of the FSA Security and Privacy Architecture Specification will be critical to understanding and incorporating appropriate business objectives and security goals.
- FSA has an existing IT Security and Privacy Policy framework that provides management guidelines for implementing security procedures. The current effort will need to integrate with existing FSA security and privacy policies.
- The primary focus of the current effort will be the FSA technical security architecture. However, existing FSA security policies and processes will provide strategic guidance in designing a FSA technical security and privacy architecture, and the potential impact of architecture recommendations on existing policy and procedures will be identified.
- The FSA security and privacy architecture will need to be flexible enough to respond to changes in requirements, technologies, and security threats over time.

2.2.2 Intended Use of the FSA Security and Privacy Architecture

The final FSA Security and Privacy Architecture specification will provide an important tool for the design and deployment of security measures. The architecture can be used:

- As a guide for security strategy and planning
- As a security design and deployment aid to promote structured, systematic, and repeatable development of security controls
- To communicate technical standards and decisions, both internally and externally
- As part of the FSA Solution Life Cycle to:
 - Integrate security architecture checkpoints into SLC checklists (e.g., during the vision, definition, and construction phases)
 - Describe how designers and developers can take advantage of existing security solutions or services to avoid custom builds
 - Align technical system design and configuration with FSA security policy
- To capture successful and proven security solutions for future use
- To document security architecture updates based on analysis of results from development projects and changes in system or technology requirements.

2.3 Organization of This Document

The remainder of this document consists of four major sections (Part A – Part D) that describe the status of the Security and Privacy Architecture Framework project. These sections provide the content of the deliverable “Interim Security and Privacy Report” as defined in the Task Order, and are described briefly below.

- Part A – Task Order Status Report – a description of the current status of TO-124: Security and Privacy Architecture Framework
- Part B – Security Workshop Meeting Minutes – a summary of preliminary discussions held to define the scope of the project and provide the business context for creating a generic security and privacy framework.
- Part C – Security Business Objectives – preliminary business objectives and security requirements identified by business subject matter experts.
- Part D – Generic Security and Privacy Framework – documentation of a conceptual, generic security and privacy framework to use as a discussion platform for developing an FSA Security and Privacy Architecture Specification.

3 Part A – Task Order Status Report

3.1 General Status

An Authority to Proceed was signed for TO124-Security and Privacy Architecture Framework on February 28, 2003. It covered the initial project deliverable, the Interim Security and Privacy Report. The TO124 contract was signed on March 6, 2003, covering the remaining project deliverables. Jesse Bowen and Hector Mezquida, both Integration Partner members, were immediately staffed on the project. Preliminary meetings with Ganesh Reddy, Andy Boots, and Bob Ingwalson were held to confirm the project objectives and approach. The initial project kickoff meeting and workshop was scheduled and held on March 6, 2003. The participants and minutes from the workshop meeting are summarized in Section 4 of this report.

Status meetings were set up and initiated the week of March 17 with Ganesh Reddy and Bob Ingwalson. These meetings review project status, plans, and any issues that may arise. Status meetings are announced with a meeting agenda and followed up with documentation of the meeting minutes.

Additional follow-up meetings have been held to introduce the project and its approach and to obtain perspectives from business and technical Subject Matter Experts (SMEs). Individual meetings have been conducted with Martin Renwick, Yateesh Katyal, Katie Crowley, and Chris Paladino. The Business Integration Group was briefed on the Security and Privacy Architecture project on April 1, 2003. The discussion covered project scope, objectives, and approach, and scheduling.

The Security and Privacy Architecture Framework project is on schedule to complete all project deliverables by May 30, 2003, as specified in the Task Order.

A copy of the project work plan is included in the Appendix (Section 7.1). All project tasks are on schedule as of the date of this report. Planning for the next Security Workshop has started. This workshop was originally scheduled for the week of April 11, but it will probably take place the week of April 21 to accommodate scheduling it in conjunction with a meeting of the Business Integration Group.

The following major tasks in the work plan have been accomplished:

- Project Kickoff
- Conduct initial security architecture workshop
- Develop Generic Security and Privacy Architecture Framework

3.2 Progress to Date

3.2.1 Generic Security and Privacy Architecture Framework

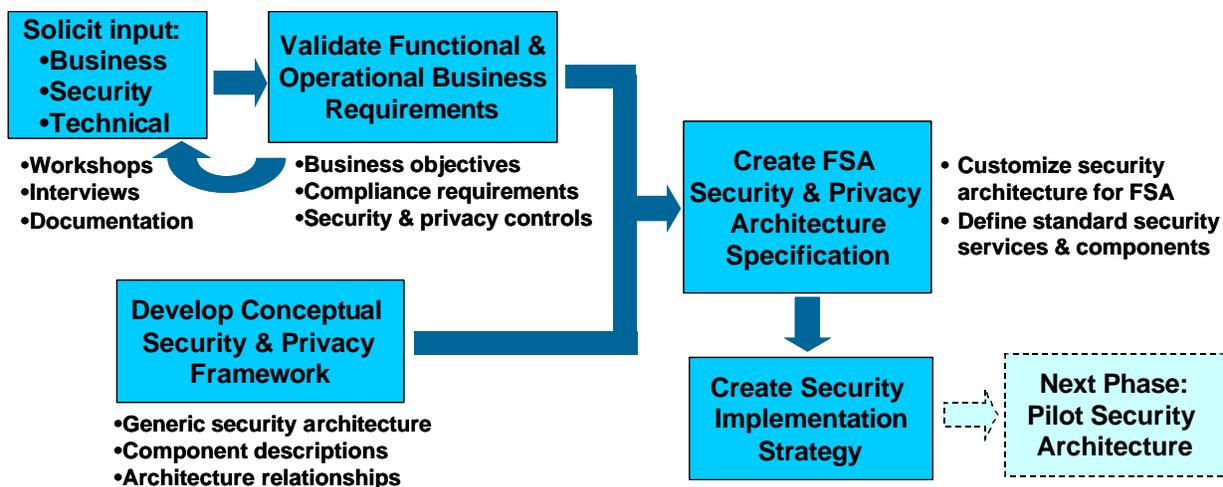
Attached in Part D of this report is a generic security and privacy architecture framework. The framework consists of topic areas covering technical security components and services, along with descriptions of functionality and relationships between components. The generic form of the framework is meant as a starting point for developing a

Part A – Task Order Status Report

customized version that reflects the specific technical security needs of FSA. While this generic framework is drawn from industry practice and experience across a large number of organizations, it has been modified in accordance with preliminary discussions between FSA and Integration Partner personnel. The suitability of the generic framework was validated through the initial security workshop and discussions with FSA and Integration Partner subject matter experts on FSA business operations. These discussions provided assurance that the generic framework captured the technical security areas appropriate for further investigation during upcoming phases of the project focused on development of the FSA Security and Privacy Architecture.

3.3 Approach

The overall approach for this project is outlined in the diagram below:



In brief, input on FSA business objectives and security requirements will be solicited from business owners and subject matter experts. FSA security requirements will be identified and validated, then used to customize a generic security framework for FSA requirements to create an FS Security and Privacy Architecture Framework. An implementation strategy for will be developed to identify recommended approaches for deploying Security and Privacy Architecture components.

The box labeled ‘Next Phase’ represents pilot activities that will make use of the Implementation Strategy to be created by this project. However, implementation activities are out of scope for this Task Order.

3.4 Next Steps

The next steps in this project will be:

- Continue to collect input to define business objectives
- Schedule and conduct two additional security workshops to validate objectives and review preliminary design
- Begin development of the FSA Security & Privacy Architecture Specification
- Begin development of the FSA Security & Privacy Architecture Implementation Strategy

Part B – Security Workshop Meeting Minutes

4 Part B – Security Workshop Meeting Minutes

4.1 Introduction

A Project Kickoff Security Workshop meeting was conducted on March 6 to initiate the Security & Privacy Architecture Framework effort. This all-day meeting was a first step toward defining standard security services that will be available for applications and to guide future system integration or improvement efforts. The workshop included discussion of requirements and objectives for technical security components in five major domains: Identity & Access Management, Data & Privacy Protection, Application Security Services, Network & Perimeter Security, and Security Monitoring Tools.

The following sections describe the meeting objectives and summarize the results of the discussion. Preliminary meeting minutes were circulated to meeting participants and invitees for comment, and all feedback received has been incorporated.

4.2 Participants

Participants in the workshop included business and technical subject matter experts, representing several Integration Partner teams and FSA Security and IT Architecture groups. Also in attendance, to provide external industry perspectives, were Alastair MacWillson, Global Managing Partner for the Accenture Security Practice, and Michael Rasmussen, a Giga Information Group security analyst. A complete list of participants is given in the table below.

Name	Affiliation	Role
Andy Boots	FSA	Security & Privacy Champion
Jesse Bowen	Integration Partner (Accenture)	Security Architecture Team Lead, Meeting Facilitator
Shawn Caison	CSC	IT Risk Manager for FSA account
Mike Gibbons	Integration Partner (BearingPoint)	Security Support Team Lead
Bob Ingwalson	FSA	Security Analyst
Alastair MacWillson	Integration Partner (Accenture)	Accenture Security Practice Managing Partner
Hector Mezquida	Integration Partner (Accenture)	Security Architecture Team, Security Consultant
Rob O’Keefe	Integration Partner (Accenture)	Accenture Engagement Partner
Paul Peck	Integration Partner (Accenture)	Technical Architecture Team Lead
Michael Rasmussen	Giga Information Group	Security Analyst, Subject Matter Expert
Ganesh Reddy	FSA	Enterprise IT Manager
Martin Renwick	Integration Partner (Accenture)	Business Subject Matter Expert
Erik Sachwitz	Giga Information Group	Giga Account Manager
Frank Southfield	Integration Partner (ICSC)	Technical Subject Matter Expert

4.3 Security Workshop Objectives

The primary objectives of the workshop were to:

- Hold a roundtable discussion on approaches to defining the FSA enterprise security architecture
- Agree on scope and priorities for the security architecture project
- Define an initial straw-man version of the Security Architecture Framework
- Define high-level business security objectives to serve as business drivers for the FSA-specific security architecture

Part B – Security Workshop Meeting Minutes

- Identify functional and operational security requirements
- Identify existing FSA security solutions that could be leveraged to provide reusable security services
- Define security issues or considerations that will affect the FSA security architecture
- Discuss industry best practices and typical security practices

4.4 Security Workshop Discussion Summary

The tables below summarize the workshop discussion for each topic area indicated. The table generally follows the order in which the topics were covered during the meeting.

4.4.1 Introduction and Scope Discussion

TOPIC	DISCUSSION SUMMARY
<i>General Introduction</i>	
System Description & Strategic Direction	<ul style="list-style-type: none"> ▪ Overall, FSA system components have been enhanced and replaced ▪ We are moving into XML, Web Services, external integration with schools, and financial partners ▪ There is also an initiative for the design of a data strategy and the implementation of the FSA gateway ▪ Single Sign-On capabilities fit in with modernization of systems, applications, and processes
Motivation for developing a security architecture framework	<ul style="list-style-type: none"> ▪ In order to build systems that are worthy of trust, with security and privacy controls, we need a defined approach and framework to collaborate with Title IV program schools
Outcome of this framework	<ul style="list-style-type: none"> ▪ Ideally, the outcome is a broad framework that needs to be populated with security concepts, controls or services. ▪ There is a need to focus on the architecture and the process that guides the design of architecture
Office of General Counsel (OGC)	<ul style="list-style-type: none"> ▪ The office of general counsel (OGC) advocates the enforcement of Privacy Act requirements on FSA systems ▪ OGC provides review and to some degree approval of security and privacy concerns. ▪ There is a need to document and expedite this process. ▪ For this discussion OGC has two primary groups: <ol style="list-style-type: none"> 1. Privacy act attorneys – provide privacy act counsel and advisory services. 2. Business advisors to FSA –their primary concern is “how are we going to do it with the minimum amount of disruption”. There needs to be full cooperation ▪ There is a need to consider the Privacy Act early in the design process. ▪ There needs to be a checkpoint to understand Privacy Act implications and review designs with OGC to build consensus. ▪ Example of OGC guidance: <ul style="list-style-type: none"> ○ eServicing - User needs to physically click the box (e.g. Email bill, link with no capability to view bill offline).
Privacy Act	<ul style="list-style-type: none"> ▪ Business units are seeking OGC guidance and opinion on privacy matters (i.e. Privacy Act, GBL, etc). ▪ There needs to be a notice to let OGC know that we are going to share and protect information. ▪ We also need to make sure that we fulfill those obligations to protect data. ▪ A general problem is that stakeholders don’t know how to implement and interpret the regulations. ▪ There needs to be a balance between convenience and security. ▪ Computer security regulations are vague and not specific but as time progresses they become more specific (i.e. HIPPA).
Other system facts	<ul style="list-style-type: none"> ▪ The PIN system contains 30 millions individuals with credentials. ▪ Financial Partners and schools communicate on a daily basis with FSA systems. On

Part B – Security Workshop Meeting Minutes

TOPIC	DISCUSSION SUMMARY
	<p>the other hand, students have a different timeframes and frequency (i.e. once or twice a year).</p> <ul style="list-style-type: none"> ▪ Identity and Access Management is very important to protect the data. All employees and contractors have access to specific data. Role based access control needs to be incorporated into the security architecture.
An example of how to see “Security”	<ul style="list-style-type: none"> ▪ Identification and authorization/Security Infrastructure ▪ Layer of application security authorization and access control ▪ Transaction based security
Other comments and questions	<ul style="list-style-type: none"> ▪ How does Department of Ed keep track of all the channels they don’t manage? ▪ We need to try to anticipate the requirements from partner organizations. ▪ Architecture needs to be useful in order to meet security requirements.
Awareness	<ul style="list-style-type: none"> ▪ Avoid stepping on the progress of the Department of Ed enterprise architecture effort. ▪ Improve relationships with the Dept of Education. ▪ There is a need to communicate FSA security initiatives with Dept of Ed architecture and security groups
Environment	
Sites	<ul style="list-style-type: none"> ▪ VDC ▪ COD Operations
Characteristics	<ul style="list-style-type: none"> ▪ Heterogeneous environment ▪ Multiple operating centers. ▪ Multiple applications ▪ Servicing - Dec Alpha Mainframe – 20 years old
Sample Locations	<ul style="list-style-type: none"> ▪ Alabama ▪ Kentucky ▪ Texas ▪ Niagara Falls.
Private collection agencies	<ul style="list-style-type: none"> ▪ There is no control of this environment. ▪ The data in this environment is considered out of bounds. ▪ Concerns were expressed about: <ul style="list-style-type: none"> ○ What is the protection of data that comes from collection agencies to FSA? ○ How are payments protected?
Others entities and comments	<ul style="list-style-type: none"> ▪ FSA acts as an agent for Treasury ▪ Contractors ▪ Application Service Providers (i.e. JamCracker)
Scope	
General	<ul style="list-style-type: none"> ▪ The general scope for the FSA Security & Privacy Architecture, and for this workshop, is data under the direct control of FSA
Insourced vs. Outsourced Systems	<ul style="list-style-type: none"> ▪ Less control over the operational processes that these entities use. ▪ There is a need to enforce controls through contractual mechanisms (i.e. there is currently a lack of effective service level agreements (SLA)) ▪ Need to define the boundaries ▪ Contractors need to safeguard the data in order to comply with government regulations and security requirements.
User Populations and “Channels”	<p>Define requirements in the context of the 4 users groups below:</p> <ul style="list-style-type: none"> ▪ Students - borrowers ▪ Trading partners – schools, lenders ▪ Financial Partners – lenders, collection agencies ▪ FSA agents – contractors, FSA employees, lawyers, regulators, auditors
Others groups	<ul style="list-style-type: none"> ▪ Business Outsourcers ▪ ASP ▪ ECMC (hosting provider)

Part B – Security Workshop Meeting Minutes

TOPIC	DISCUSSION SUMMARY
Different ways to approach technology	Technology Views: <ul style="list-style-type: none"> ▪ Infrastructure view ▪ Data view ▪ Applications view ▪ Business process view
Biggest Security Risk	<ul style="list-style-type: none"> ▪ EDNET
Other Comments	<ul style="list-style-type: none"> ▪ Financial Partners are not only lenders but are also loan servicers ▪ Common Student ID (CID) – identify project background information and dependencies

4.4.2 Discussions about Security Architecture Topic Areas

TOPIC	DISCUSSION SUMMARY
IDENTITY & ACCESS MANAGEMENT	
<i>Identification & Authorization</i>	Can also be viewed as enrolment and single sign-up
Trust	<ul style="list-style-type: none"> ▪ Placing trust in other organizations to do the verification of an individual ▪ Schools are concerned about giving information about their employees. ▪ We are assuming that credentials are not being shared by school individuals. ▪ Identity proofing – partner school helps with the verification of student identity. ▪ Validation of Student ID is performed with SSN system. ▪ Authentication of System to System interactions (transactions, batch processing) ? ▪ Financial Partners – what is the process to access information between them?
Institution enrollment process control	<ul style="list-style-type: none"> ▪ The president of the institution signs a form. ▪ After signature is obtained, institution is able to participate on the student gateway. ▪ School – financial aid administrator’s access? ▪ Transaction – (i.e. SAML, Web Services) –possibility of accepting credentials from another institution.
Student	<ul style="list-style-type: none"> ▪ Are able to do personalization of their portal ▪ Validation of student information doesn’t occur until they submit the transaction and the application is approved (Comment from Yateesh Katyal: The 2nd bullet is incorrect. Student identities are verified as part of the application processing function; the application is not complete until it passes the SSA verification, VA (if applicable), INS check (if applicable), Selective Service (if applicable), NSLDS, and other matches. Also, FSA does not "approve" applications; it simply processes them to generate an expected family contribution (EFC) that is noted on the Student Aid Report (SAR) sent to students/parents and Institutional Student Information Record (ISIR) sent to schools.) School takes a sample of the population to validate credentials ▪ Business Perspective: <ul style="list-style-type: none"> ○ Access data ○ Enter data – students sign-up. There is no need for validation. ○ Submit application for financial aid – there is a need for identification. PIN comes into play.
<i>Authentication and Single Sign-On</i>	

Part B – Security Workshop Meeting Minutes

TOPIC	DISCUSSION SUMMARY
“Single Sign-Up”	<ul style="list-style-type: none"> ▪ Single Sign-Up for all the groups? ▪ Portals provide the opportunity to authenticate users one time and pass credentials to other applications. ▪ What are the systems (or entities) that feed data to FSA systems?
Tiered Access	<ul style="list-style-type: none"> ▪ Students – Tier 1 ▪ Everyone else - Tier 2 access ▪ Servicers (Access to <i>n</i> number of schools, a subset of the total number, and subject to modification)
FFEL Community	<ul style="list-style-type: none"> ▪ Business focus for two main reasons: <ol style="list-style-type: none"> 1. Subsidized and held by federal government - Direct loan 2. Guaranteed and issued by a financial institution (Citibank, Sallie Mae) ▪ If the student has not graduated, there is no single view of how much a student has already in financial aid.
<i>Authorization & Access Control</i>	
Access Control comments	<ul style="list-style-type: none"> ▪ Front end relies on the PIN site for the authentication credential ▪ Students: End-user interacts with only one system that is connected to the back end. ▪ School getting batch information. ▪ Schools and financial partners areas will not merge into a portal like for the students. ▪ There is a need for a horizontal view of the school portal. ▪ Role based access control is an important solution that permits granular access. ▪ Is the broader picture complete and validated? ▪ Current regulations are getting executives’ attention ▪ There needs to be more attention to governance responsibility for information security. ▪ Architecture Guidance should drive procedures. ▪ Framework should be discussed with the business units.
<i>Data Repositories</i>	
Comments	<ul style="list-style-type: none"> ▪ There has to be a link between centralized function and all the entities. ▪ There is a need for directory services and integration with FSA applications. ▪ Audit logging of applications; individual access to records ▪ Revocation of credentials (i.e. RACF suspended IDs)
<i>Administration & Provisioning</i>	
Requirements	<ul style="list-style-type: none"> ▪ Centralized administration functions ▪ Manage account parameters, e.g., <ul style="list-style-type: none"> ○ Credential aging (such as forcing password expiration) ○ Enforce password policies ○ Efficiently terminate accounts

Part B – Security Workshop Meeting Minutes

TOPIC	DISCUSSION SUMMARY
ENCRYPTION	
General Comments	<ul style="list-style-type: none"> ▪ Confidentiality solution needs to be mapped to the communication channels we use. ▪ Applications moving to the Internet. ▪ What is adequate protection for data transmitted over the Internet? ▪ Need to tie safeguards to data classification model. ▪ An ATM encryption policy was developed for COD ▪ There is no formal definition of a data class. Data integration group is supposed to be working on this. ▪ There is sensitive information that is important for fiscal integrity ▪ Hard-Drive data backup data. How is it stored? ▪ Data of tapes in transit is unencrypted ▪ An FSA challenge is the control of environments that are outsourced (I.e. the network). ▪ PC's – no permanent cookies allowed ▪ What about people that do school reviews with NSDL data? ▪ Is the responsibility of the school to safeguard FSA data? This is outside of the scope of this task order. ▪ FSA feels able to enforce the encryption of the communication link. In other words, FSA should be able to enforce the standard for transactions/exchanges. ▪ What happens to the data when a school closes? ▪ Some schools are using EDI and refuse to migrate to the SAIG solution. ▪ There is a need for a security architecture and strategy for FSA. ▪ General topic may be better described as “Data Protection”, since not all solutions use encryption
<i>Communications Encryption</i>	
SSL	<ul style="list-style-type: none"> ▪ SSL is an available technology that we should deploy ▪ SSL is already being used for browser-based applications ▪ FTP over an SSL connection is used in the bTrade system
<i>Data Encryption</i>	
Data Types	<ul style="list-style-type: none"> ▪ The following are FSA data types: <ul style="list-style-type: none"> ○ Personal private – students’ information, needs for protection of communication and storage medium. ○ Financial data in association with an individual. I.e. FSA handles “Metadata” about finances, shared with Treasury Department ○ Information about FSA security – configuration data, security procedures, risk assessments, vulnerabilities, etc. ○ Eligibility data for institutions. ○ Information about services ○ Public information
Data Encrypted:	<ul style="list-style-type: none"> ▪ Secret data ▪ Password files
<i>Message Integrity</i>	
	<ul style="list-style-type: none"> ▪ Is it a requirement for communications inside or outside of the organization? ▪ It calls into question a lot of our business processes ▪ Financial Transactions – disbursements – checks and balances ▪ Code – no coding standards to incorporate security ▪ What is the chain of systems that exchange messages? ▪ Connect direct – application for transmitting data to treasury ▪ Overall, it is left to the application to check the integrity of the

Part B – Security Workshop Meeting Minutes

TOPIC	DISCUSSION SUMMARY
	message.
<i>Non-repudiation</i>	
	<ul style="list-style-type: none"> ▪ Non-repudiation is currently procedural, based on underlying bilateral agreements (i.e. Signing promissory notes). ▪ I.e. EzAudit – application that enables schools to submit audits. ▪ This area is going to be influenced by regulatory matters.
<i>Secure Messaging</i>	
	<ul style="list-style-type: none"> ▪ Secure SMTP it is virtually impossible in FSA current environment. ▪ I.e. Message to the website, take into consideration Privacy Act. ▪ There is a requirement for secure messaging, but there are scalability issues. ▪ Web Mail approach methodology: <ul style="list-style-type: none"> ○ Link/login to system ○ Privacy Act ▪ Requirement to protect Privacy Act data from inadequate disclosure ▪ There is a need to define pro’s and con’s; requirements, choices and context.
NETWORK & PERIMETER	
<i>Traffic Filtering and Content Control</i>	
	<ul style="list-style-type: none"> ▪ Checkpoint Firewalls ▪ Policy – “connection between FSA and open networks must be protected by firewalls”. ▪ No requirements on implementations. ▪ Policy - “all unnecessary services should be turned off” ▪ Email system outsourced to the Department of Ed ▪ Firewall Architecture has the following characteristics <ul style="list-style-type: none"> ○ Load Balancing ○ Availability ○ Resilience ▪ Redundant firewalls and isolation of networks “VLAN” in the VDC ▪ FSA is unable to insource application hosting
Contracts	<ul style="list-style-type: none"> ▪ There is a need to integrate security and regulatory requirements into contracts ▪ Integrate SLA’s, performance metrics, and penalties into contracts ▪ There is a need for better integration of technical and security requirements into the contract vehicle (I.e. checklist for hosting providers) ▪ Define classes of services? ▪ Feasibility to add additional services to on-going hosting contracts
MONITORING TOOLS	
<i>Centralized Logging</i>	
	<ul style="list-style-type: none"> ▪ No requirement for logging DBA, but there is a need to log environment changes ▪ What are the department’s incident response requirements? ▪ What is an adequate level of logging? ▪ Logs for forensic analysis should be stored separately. ▪ Independent of provider this needs to be incorporated into the SLA’s.
<i>Patch & Configuration Management</i>	
	<ul style="list-style-type: none"> ▪ CSC performs two internal assessments per year. IG performs four. ▪ Patches should be done within hours ▪ There is a need to track alerts and its applicability to the system. ▪ Assess severity and criticality of applications ▪ Incorporate Patch management into the SLA’s ▪ Define business process for patching vulnerabilities. (Identify, test, deploy, monitor, etc).

Part B – Security Workshop Meeting Minutes

TOPIC	DISCUSSION SUMMARY
<i>Intrusion Prevention</i>	
	<ul style="list-style-type: none"> ▪ Akamai network would serve as intrusion prevention mechanism. ▪ Web activity monitoring
APPLICATION SERVICES	
	<ul style="list-style-type: none"> ▪ Legacy: retrofit vs. Sunset ▪ Three approaches to application security <ul style="list-style-type: none"> ○ Don't integrate ○ Wrap to use common functions ○ Integrate ▪ What is the effort? ▪ Classify based on business value ▪ Options to use adapters ▪ Embedded security functions are used for access control in data bases ▪ Set standards (e.g. session management, coding standards) ▪ What are we going to do with business systems that are not being retired? <ul style="list-style-type: none"> ○ Let them be ○ Front end the application ○ Not allow new applications to embed security functions ▪ Proxy, adapters, Middleware layer (e.g. MQSeries) ▪ Define process and policy to integrate common functions ▪ Certification and Accreditation: <ul style="list-style-type: none"> ○ There are two general support systems ○ SAIG ○ VDC ▪ Integrate application level vulnerability assessments in the development phase of the SDLC
<i>Web Services</i>	
	<ul style="list-style-type: none"> ▪ How to address? ▪ There will be a commitment to use when technology matures to leverage security services ▪ Internal vs. External ▪ Currently at a conceptual level

Part C – Preliminary Security Business Objectives

5 Part C – Preliminary Security Business Objectives

The table below summarizes business objectives and requirements related to security that have been identified to date. These requirements were gathered during security workshops and from individual meetings with business owners and subject matter experts. This list represents a preliminary set of business objectives that will drive security requirements for the FSA Security and Privacy Architecture. It will be supplemented and refined during development of the FSA Security and Privacy with additional input from FSA business owners and subject matter experts.

	Students	Trading Partners (Schools)	Financial Partners
Identity & Access Management			
<i>Identification & Registration</i> (Initial identification and enrollment of users, including creation of security credentials)	Currently performed by the application and/or the PIN site. Define three registration processes: 1) No identification or registration required (appropriate for initial contact or initial expression of interest) 2) self-registration, for personalization and access to partially completed applications (e.g., Student’s Portal) 3) full registration for PIN required to submit application (e.g., FOTW)	Involved in enrollment process; Validate system administrator credentials only; other credentials accepted if vouched for by system administrator	Validate system admin credentials only; then accept credentials from partners (transitive trust); other credentials accepted if vouched for by system admin
<i>Authentication</i> (Validating user credentials when access to a system is requested)	Requirements are: 1) No authentication needed when requesting information or viewing public pages; 2) Authentication using self-defined username and password when viewing partially completed applications or for personalization. Functions; 3) Authentication with individual PIN to submit an application or view information about submitted applications or their processing.	Required; assumption is that only one individual uses an ID, but realistically more than one person may use a single account	Yes; assumption is that only one individual uses an ID, but realistically more than one person may use a single account EDNET for employees & agents.
<i>Authorization & Access Control</i> (Assign and enforce privileges for specific data and resources based on authenticated identity of user)	Students/parents should have access only to own data	Required; users should have access only to data of that institution; distinction between FFEL community and Direct Loan organizations.)	May have access to multiple schools; need to allow for changing access to add or delete schools from access list.

Part C – Preliminary Security Business Objectives

	Students	Trading Partners (Schools)	Financial Partners
Directory Services (Storage and management of user information, security credentials, and other security data)	TBD	TBD	TBD
Administration & Provisioning (Provision and manage user and system accounts)	Administrative functions are required for management of user accounts	Yes, administrative functions are required: 1) ability to report on users (and their affiliations) who have access to each system 2) ability to remove users who should no longer have access	Yes, administrative functions are required: 1) ability to report on users (and their affiliations) who have access to each system 2) ability to remove users who should no longer have access

Data & Privacy Protection	
Communications Encryption (Protect confidentiality and integrity of communications channels with encryption techniques)	For use of Point-to-Point circuits; a current standard is to use FTP over SSL connection (for bTrade file transfer) One solution is to use hardware encryption as deployed for the ATM network for COD. Tied to data classification; don't have a formal one now, but operationally: 1) Personal/private (individual info., Privacy Act info., very sensitive) 2) Financial data about individuals 3) Financial integrity data; data dealing with transactions, payments, etc. 4) Operational data (not as sensitive, dealing with less sensitive data about operations of FSA, schools, financial partners) 5) Public, non-sensitive data
Data Encryption (Protect confidentiality and integrity of data stored in databases with encryption)	No general requirement for encryption of data at rest (e.g., stored in databases, on workstation drives or laptop drives), even for most sensitive data. Exception is that encryption is required for credential data, like passwords or encryption keys, and other types of security data that must be protected. No requirement for encryption of hard drives, or for protection of backup media. Scope is electronic data only; not required for telecommunications, FAX, etc. Financial data would be a candidate for higher levels of protection, but not handled differently now (e.g., no encryption in databases).
Message Integrity (Prevent unauthorized modification of transmitted data and/or detect modification attempts)	Now at application level; generally uses business rules and other logical checks rather than message hashing or other encryption-based integrity controls; some protection provided by encryption during transmission, but does not apply after decryption or while stored.
Non-repudiation (Provide evidence that will prevent repudiation of authorship or content of a transaction)	All current methods are procedural, e.g., based on a set of transactions such as that between student, schools, and FSA: a student applies for aid and provides identifying information; FSA processes the application and sends aid to schools; schools provide aid to students; non-repudiation of loan obligations based on fact that the individual who "signed" for the loan with a PIN is the same person who attended school and received academic credit. Financial obligations have been upheld in court based on this relationship even when no physical promissory note could be produced. There may be future regulatory requirements that will mandate more explicit non-repudiation controls.

Part C – Preliminary Security Business Objectives

<p>Secure messaging (Protect confidentiality and integrity of email messages and file transfers)</p>	<p>Not used now. Feeling is that current email encryption solutions are not suitable for communication with external parties because of overhead and management burden (client software, encryption key management, etc.) Might consider alternate, <i>ad hoc</i> approaches, such as JIT key management (ZixMail, Authentica), or “webmail” systems. One approach to this item may be to describe current options, define pros and cons, and provide advice about recommended solutions, avoiding prescriptive direction. Already use some solutions for file transfer, like FTP over SSL.</p>
<p>Network & Perimeter</p>	
<p>Traffic Filtering (Inspect network traffic based on factors such as source and destination addresses or existence of valid sessions; block unauthorized or harmful network traffic)</p>	<p>Need load balancing and high availability. Need redundant firewalls. Need isolation of network segments Connections to open networks must be protected by firewalls. No specific implementation requirements; service providers are expected to meet requirements. Architecture should provide requirements or standards that would apply to service providers, even if specific solutions or implementation details are not included.</p>
<p>Content Control (Inspect traffic and block malicious content such as viruses, worms, Trojan horses, or other unacceptable content)</p>	<p>There is no content filtering within FSA environment; Dept. Ed. is the service provider for FSA email.</p>
<p>Intrusion Monitoring (Detect attempted attacks on networks, operating systems, and servers; alert operations personnel to initiate appropriate incident response)</p>	<p>Monitoring requirements will depend on class of services.</p>
<p>Intrusion Prevention (Detect and block attempted attacks on host operating systems and applications)</p>	<p>Includes host intrusion detection; may include web activity. Will be the responsibility of the service provider. What about contracting with provider such as Akamai who could do this?</p>
<p>Remote Access (Provide secure VPN and dial-up services)</p>	<p>Need to build requirements into SLAs. Can provide checklists for hosting providers, and to evaluate hosting providers. (This applies to the other network topics as well).</p>
<p>Monitoring Tools</p>	
<p>Auditing and Logging (Recording, storing, and reporting user and system activity and access privileges.)</p>	<p>No requirements for logging database access, but need to log environment changes (change management?) Need to address log storage and define requirements for separation of systems, and for controls to protect logs.</p>
<p>Analysis and Correlation (Consolidating and processing audit data, log data, and other security information to detect patterns that indicate potential security incidents)</p>	<p>No requirements now.</p>
<p>Vulnerability Assessment (Tools to inspect networks, host systems, and applications for potential security weaknesses)</p>	<p>Need to specify the number of times per year the vulnerability assessment is performed. Should assessments be conducted independently of provider? Some will allow this, some won't. Should be part of the SLA, and FSA should have the ability to perform these assessments themselves.</p>
<p>Forensics Tools (Tools to inspect systems and security information to gather evidence about suspected security breaches)</p>	<p>No specific requirements currently</p>

Part C – Preliminary Security Business Objectives

<p><i>Patch & Configuration Management</i> (Tools to detect or deploy system patches, updates, or fixes; tools to maintain the integrity of host or application software)</p>	<p>Need response time requirements. The SLA should address version and patch control, but a reasonable life-cycle process needs to be provided for (i.e., identification, analysis, testing, deployment, and monitoring).</p>
<p>Application Services</p>	
<p><i>Embedded Security Functions</i> (Security functions deployed within applications, including authentication, access control, auditing, account administration)</p>	<p>Functions deployed within the application, and strategy for defining security requirements, will vary with the type of system. Types of systems: 1) Legacy systems that will be retired soon, or for which it would be prohibitive to retrofit – will not use new security functions provided as services. 2) Legacy systems that can be wrapped or proxied – use interface, API, etc., to integrate legacy system and enable it to use external security services. 3) New systems – architecture standards should require that new systems will use the security services provided in the new FSA architecture.</p> <p>Decisions need to be based on business value, and the availability of integration options (pre-built vs. custom adapters) Need policy and process for classifying systems and making decisions about migration strategy.</p>
<p><i>Security Integration</i> (Interfaces or APIs used to integrate applications with external security services)</p>	<p>See above.</p>
<p><i>Web Services Security</i> (Security standards and functions for protecting web services transactions)</p>	<p>Address by discussing, and describing future, anticipated uses. Not yet a mature set of standards, and little commercial technology is available yet, but it will become more important, and has the potential to provide important security services, such as transactional and end-to-end accountability. Another issue is with external partners; i.e., which schools will have web services developed enough to take advantage of FSA systems? Will also depend on interest of the business.</p>
<p><i>Transactional Security</i> (End-to-end authentication, access control, and auditing for system and user entities in multi-tier architectures)</p>	<p>No specific requirements yet identified</p>

6 Part D – Generic Security and Privacy Framework

6.1 Introduction

This section describes a generic security and privacy framework. The purpose of this framework is to provide a conceptual basis to guide development of an FSA Security and Privacy Architecture. The overall framework covers organizational and process elements of information security, in addition to security technology. However, the primary focus of the detailed framework is the technical architecture layer of information security. The generic framework describes major technical security components, their uses, and their interrelationships.

The overall security and privacy framework is organized into three major layers:

- Security Management
- Security Processes
- Technical Security Architecture

The major domains that make up each of these layers will be defined, but only to provide context for understanding the integration between technology components and their supporting processes and management structures. Each domain within the Security Technology layer will then be described in greater detail.

6.2 Scope

The generic security and privacy architecture framework described below is intended as a succinct compilation of major security and privacy functions. The framework is intended for use as a design aid and check for comprehensiveness during development of an organization-specific security architecture. It offers a starting point for understanding and designing an architectural view of secure solutions. This framework identifies security functions and components that can serve as building blocks for security solutions, and how those components fit together. Along with security governance structures, security policies, and supporting processes, this framework should allow description of a detailed security architecture that meets the specific requirements of an organization.

The framework is designed to be broad enough, yet flexible enough, to provide descriptions of technical security measures in common use among most commercial, government, and private organizations. However, no general framework will be able to capture all the detail and nuance of the security requirements for a specific organization. The goal for this framework is to define functional categories of security technology components to promote a systematic examination of their applicability for a specific set of security objectives.

The framework is not vendor specific, but it does contain references to specific technologies. Some sections may also refer to vendor products as examples or to explain security technology details. Such references should not be taken as endorsements of products from individual vendors, and they in no way imply a judgment or recommendation about the suitability of a vendor product for specific purposes.

Part D – Generic Security and Privacy Framework

6.3 Security and Privacy Architecture Overview

An effective information security capability must provide an integrated set of administrative, procedural, physical, and technical controls selected through an explicit risk management process. Although the primary focus of the security and privacy framework discussed in detail below is security technology, it is important to emphasize that few security solutions will consist solely of technical mechanisms. In most cases, security objectives can only be achieved with thorough integration of security policies and processes with other security controls. For example, a significant fraction of security incidents (more than half according to some studies) can be attributed to accidents or mistakes by system users. Technical security mechanisms are an important element of security, but the prominence given security technologies in the following security and privacy framework does not imply that most security problems have technology solutions. More commonly, security objectives will dictate a combination of procedural and technical controls based on appropriate supporting processes and management structures.

The following sections provide an overview of how the three major layers of a conceptual security and privacy framework can be considered as an integrated whole. An effective security and privacy framework should describe the management components that provide organizational accountability, guidance on selection of security controls, and decision-making approaches for management of risk. Security processes describe the major procedural control programs that are comprise either standalone security controls or support technical control mechanisms. Finally, the technical security architecture will describe a set of hardware and software security components that can be used as building blocks to create an integrated and robust security program. Figure 6.1 provides an overview of the generic Security and Privacy Framework, with Technical Security Architecture components highlighted to indicate their focus as the subject of detailed descriptions in Section 6.4.

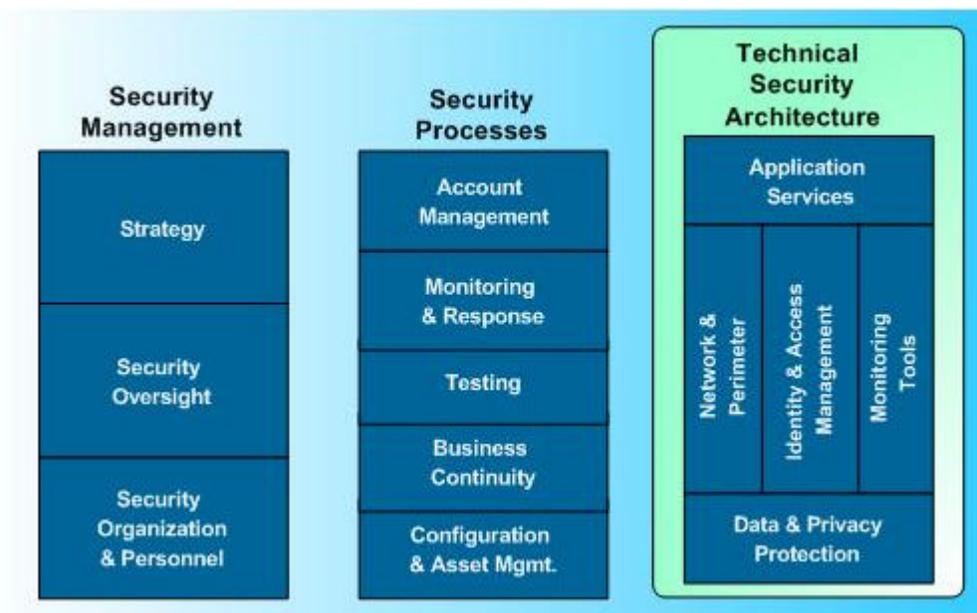


Figure 6.1 Overview of Generic Security and Privacy Framework

6.3.1 Security Management

The Security Management layer of the framework contains the organizational structures and mechanisms for making decisions about the development and deployment of a security program. It consists of the strategy and vision components that set overall security direction; oversight activities for assessing the effectiveness of security controls, and the personnel and organizational components that provide long-term accountability for security operations.

Security Management consists of the following major components:

- Security Strategy
- Security Oversight
- Security Organization & Personnel

Security Strategy

Security Strategy provides direction and planning for information security. The organization strategy may be documented in several ways, including mission and vision statements; policy, procedure, and standards frameworks; and security architecture blueprints or plans. The security strategy provides the guidance for risk management decisions for selection and deployment of security controls, including both process controls and technical controls. The security strategy accounts for current and future business directions to provide a basis for selecting and operating security controls that support the organization's functions. The security strategy must also respond to new threats, technologies, and user requirements through a proactive risk management process.

Security Oversight

Security Oversight provides programmatic monitoring functions that evaluate how effectively a security program meets internal or external security objectives. Internal security objectives are primarily those driven by and documented in the security strategy, including related policies and standards. External goals typically consist of industry standards or regulatory requirements for which compliance is mandatory. Oversight functions will usually include a combination of internal structures, such as an audit program, and external activities, such as third party or regulatory audits.

Security Organization & Personnel

Security Organization & Personnel addresses the design of a security organization, its operational functions, and related personnel security programs. The effectiveness of a security capability is directly related to the clarity of security role definitions, management accountability, and reporting relationships. Personnel programs address the need to train the entire organization on security and privacy issues, and to provide specialized training in risk management, security development, and security operations to appropriate personnel. For example, a security awareness plan will set the organization's expectations regarding information security, and communicate the responsibility each individual has to protect the confidentiality, integrity and availability of information assets. Personnel security programs define the types of background checks or access authorization processes that approve and assign access privileges for sensitive resources.

6.3.2 Security Processes

Security processes define operational steps for implementing or supporting security controls. Management and technical security controls also have associated processes that provide necessary support and oversight for their effectiveness. The major security process components described below represent security functions that are primarily process in nature. However, each of these security processes can be implemented with or assisted by technical security tools that improve their efficiency or accuracy.

The Security Processes layer consists of the following major components:

- User Access and Account Management
- Monitoring & Response
- Security Testing
- Disaster Recovery and Business Continuity
- Configuration and Asset Management

User Access and Account Management

User access and account management includes the processes needed to register users, create user credentials, and set up user access accounts. It includes processes for modifying and managing system accounts, and for terminating access when it is no longer required. Additional processes that aid user account management may involve processes to change user credentials, such as passwords, or other user information.

Monitoring & Response

Monitoring and response processes support the collection and analysis of log information and other forms of security information. The goal is usually to either identify security incidents or determine the operational status of security systems. Forensic and other investigative goals may also be addressed through similar monitoring techniques. Related monitoring processes define operational requirements for collecting, storing, protecting, archiving, and retrieving audit and log information.

Security Testing

Testing processes provide the means to examine existing or planned security controls for effectiveness and appropriateness. Testing processes may be incorporated into a software development life-cycle, change management process, or other defined procedures for software, hardware, or system deployment. Testing processes may also address *ad hoc* testing for specific purposes, such as in response to security incidents or as part of a regulatory compliance program. Security testing often parallels other system and software testing methodologies, although specialized tools and techniques are usually required to probe security configurations and potential weaknesses. Security testing processes may address several architectural elements in an information system environment, including applications, servers or hosts, and network components.

Disaster Recovery and Business Continuity

Disaster recovery and business continuity processes define the processes and plans that limit damage from natural or man-made disasters. Business continuity processes provide guidance for re-establishing the organization's critical functions. As part of the planning

Part D – Generic Security and Privacy Framework

process for disaster recovery and business continuity planning, processes to identify system and application criticality, and to classify the sensitivity of data, may be required.

Configuration and Asset Management

Configuration and asset management processes define procedures for assessing and applying upgrades and configuration changes to systems, servers, and applications. These processes include steps to define and apply security-hardening steps to new or existing operating system and application software, and to manage security upgrades and fixes. Related processes include processes for updating virus definitions, maintaining an inventory of information system assets, and managing system changes that could affect the security posture of an organization.

6.3.3 Technical Security Architecture

The Technical Security Architecture defines hardware and software security systems and components that can be used to create security controls. Technical security components rarely, if ever, function without the support of appropriate security management structures and security processes. Security management activities, such as strategy development and risk management, are critical to the selection and deployment of technical controls that achieve the desired security objectives. Support processes for the operation, maintenance, and upgrade of technical security systems are vital to their effectiveness.

Technical security components are classified for convenience into the following categories, defined briefly below, and in greater detail in Section 6.4.

- Application Services
- Network and Perimeter Security
- Identity and Access Management
- Monitoring Tools
- Data and Privacy Protection

Application Services

Application Services include security functions deployed as part of or integrated with applications: embedded security functions such as authentication, access control, and auditing; interfaces or APIs that allow applications to call or take advantage of external security functions; web services security that provide user and transactional security in a web services environment; and transaction security that provides end-to-end security functions in multi-tier architectures.

Network and Perimeter Security

Network and Perimeter Security defines services and devices that protect the network environment and the perimeter of an information system. These security functions include traffic filtering and network access control; virus detection and interception of harmful or malicious content; intrusion detection and prevention systems for recognizing and blocking potential security attacks on network, servers, or applications; and remote access functions that provide secure access for remote users.

Part D – Generic Security and Privacy Framework

Identity and Access Management

Identity and Access Management defines security functions that manage user identities and control user access to information resources. Components in this domain include identification and registration; user and system authentication; authorization and control of access privileges; directory services for storing and managing user credentials and other security information; and user administration and provisioning systems, including related functions such as delegated administration and user self-service capabilities.

Monitoring Tools

Monitoring tools include technical components that collect, analyze, or manage information about system or user activity. This domain includes tools for logging system and user activity, reporting on access privileges, and analyzing system information to detect potential security incidents and events. Vulnerability assessment tools provide the ability to scan network, servers, and applications for weaknesses that may provide a point of attack to compromise systems. Forensics tools provide mechanisms to collect information about system behavior and user activity during investigations. Patch and configuration management tools provide aids to detect or deploy patches and updates, or to maintain the integrity of host or application software.

Data and Privacy Protection

Data and Privacy Protection refers to technology components that protect the confidentiality, integrity, and availability of data. Encryption techniques, either applied to communications channels or to stored data, provide the basis for many of the protective mechanisms employed in this domain. Also included under this general heading are tools to provide message integrity, non-repudiation of transactions, and secure email and file transfers.

6.4 *Technical Security Architecture Framework*

6.4.1 Introduction

This section presents a conceptual view of the Technical Security Architecture domain within the overall Security and Privacy Architecture Framework. The goal of this section is to define technology components that can be used to design and deploy security controls based on hardware devices and software elements. This conceptual architecture framework will be used as a basis for selecting and customizing components that will become part of the FSA Security and Privacy Architecture Specification.

6.4.2 Criteria

Components defined in the Security Technical Architecture were chosen to satisfy the following basic criteria:

- Security components in the framework cover the breadth of security technologies without significant overlap between categories.
- The technical security categories group functionally related capabilities that are often deployed with similar technologies or with groups of integrated technologies.
- The security technologies described within each category represent available tools that are commonly in production or will be in the near future. Exotic technologies that are impractical because of cost or immaturity are not included.

6.4.3 Content

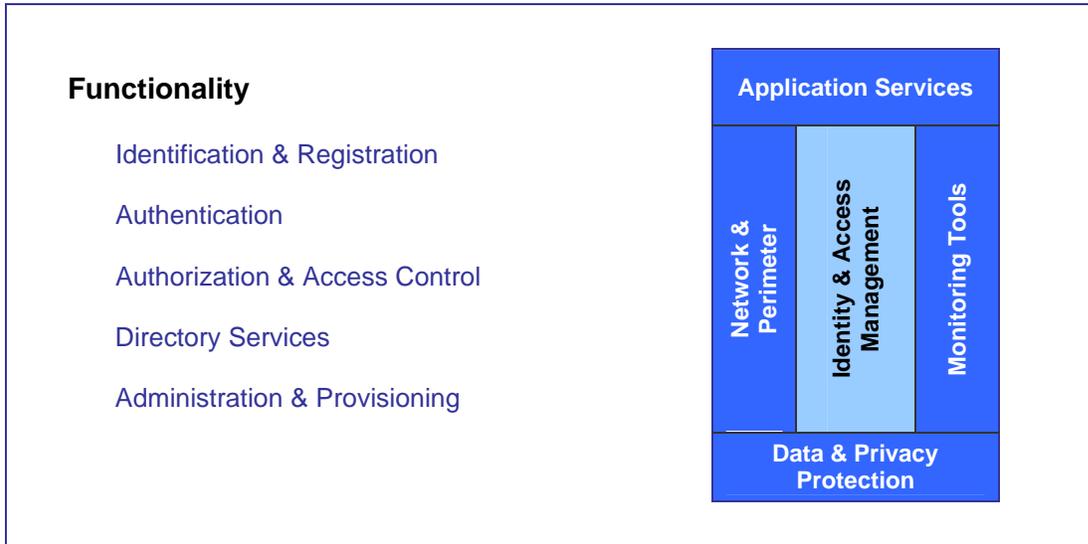
The Technical Security Architecture consists of five major domains, described in the following order:

- Identity & Access Management
- Data & Privacy protection
- Application Services
- Network & Perimeter Security
- Monitoring Tools

Each section consists of:

- Objective** the overall goal or security purpose served by the category.
- Description** definition of the security technology components within each domain.
- Context** explanation of the relationships and dependencies between the domain and other security technologies.
- Functionality** definition of the security functions provided by each component within the domain.

6.4.4 Identity & Access Management



Objective:

Identity and Access management services provide security functions that identify and manage entities, and control access to resources.

Description:

Identity & Access Management systems integrate functions that manage user identities and control access to resources. Identity management functions consolidate identity data necessary for making authentication and access control decisions, and automate the provisioning of access rights to applications and resources for various user populations based on business policies. Access management functions protect information systems by mediating access of internal or external users to specific application data, function, or other resources. Identity & Access Management systems typically integrate directory services, authentication services, access management services, and provisioning systems. Figure 6.2 shows a conceptual framework depicting major elements of an identity management system.

An integral feature of Identity & Access Management is centralized application of security policy to administer user privileges. This capability increases the accuracy and cost-effectiveness of user account setup, modification, and termination. Administration can be either centralized or delegated, and many multiple identity sources and security data repositories may be supported. Additional functionality to increase the effectiveness of identity and access management functions include

Part D – Generic Security and Privacy Framework

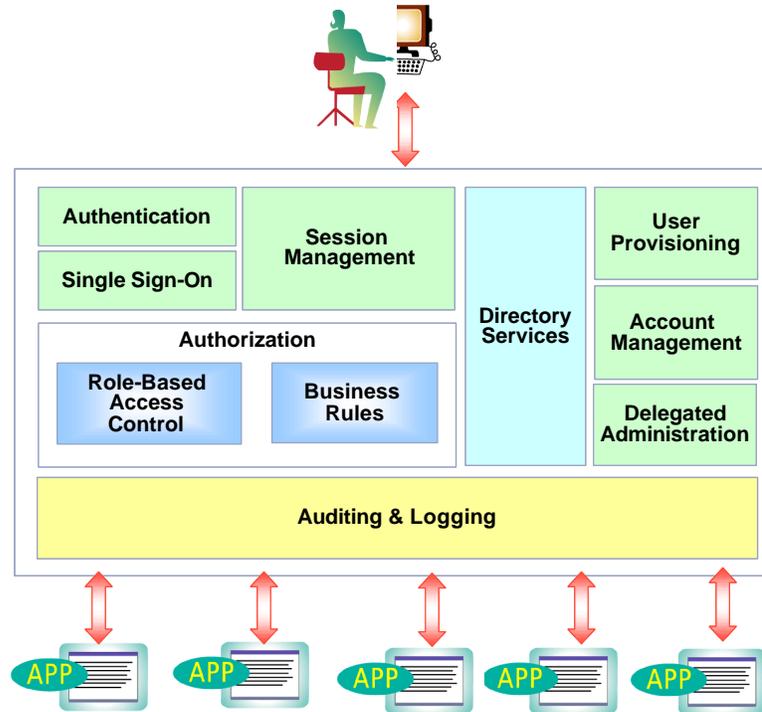


Figure 6.2. Major functional components of a typical Identity and Access Management Solution

role-based access control, federation of identity across multiple organizations, and single or reduced sign-on for groups of applications. Ancillary functions that may be incorporated into Identity & Access Management include password synchronization, enforcement of password policies and other authentication credential requirements, support for multiple authentication mechanisms, password reset capabilities, self-service registration functions, security approval workflow, and automated user account updates fed by Enterprise Resource Planning systems.

Identity and access management infrastructures have evolved to be independent of similar operating system functions. Identity & Access Management systems are typically deployed as separate security components that provide security services to operating systems, applications, or network devices. As a consequence, a critical step in planning or design is to develop an effective strategy for integrating Identity & Access Management services into new or existing systems and applications. Some design choices that must be considered include:

- Selection and management or synchronization of security data repositories
- Interfaces or APIs used for communication between applications and Identity & Access Management services
- Whether access control decisions will be mediated within applications, externalized to the Identity & Access Management system, or be a shared function
- Which administrative and provisioning functions will be performed by the Identity & Access Management system, and which functions operating system administrators or application administrators will retain.

Context

Identity & Access Management components interact with a variety of other security technology functions and solutions. Typically, Identity & Access Management mechanisms are integrated with the overall security technical architecture in the following way:

- Network & Perimeter components provide traffic filtering and access capabilities to protect the underlying network and host environment infrastructure. Identity & Access Management components provide authentication mechanisms for administrators of network devices and remote access users connecting through dial-up or VPN connections.
- Monitoring Tools provide a repository for archiving auditing and logging information (i.e. successful and failed login attempts, file access, etc.) collected by various components of the Identity & Access Management system. In turn, Identity & Access Management components provide monitoring systems with the necessary authentication and access control mechanism to restrict access to sensitive system information.
- Data & Privacy protection mechanisms provide capabilities to encrypt communication channels (e.g., using SSL for Internet links and web applications). Identity & Access Management components may provide the authentication mechanisms and credential repositories for creating, managing, and communicating user credentials, such as digital certificates or encryption keys, that are required for encryption or that identify systems or users. Public key infrastructure (PKI) technology typically makes use of Identity & Access Management components to store and manage digital credentials, and conversely may supply authentication services.
- Application Services components provide the necessary APIs to integrate the Identity & Access Management capability with applications, operating systems, databases, legacy applications, and other computing environments (midrange and mainframe platforms).

Figure 6.3 shows an example of how Identity & Access management integrates with monitoring tools. In this scenario, an end-user requests access to a web application. The web application authenticates the user by calling an Identity & Access Management function that enforces the organization's access control policy. The Identity & Access Management system requests credentials from an authentication solution that uses an enterprise directory. Simultaneously, monitoring tools preserve an audit trail of the system and user activity that is linked to the appropriate Identity and Access Management events.

Part D – Generic Security and Privacy Framework

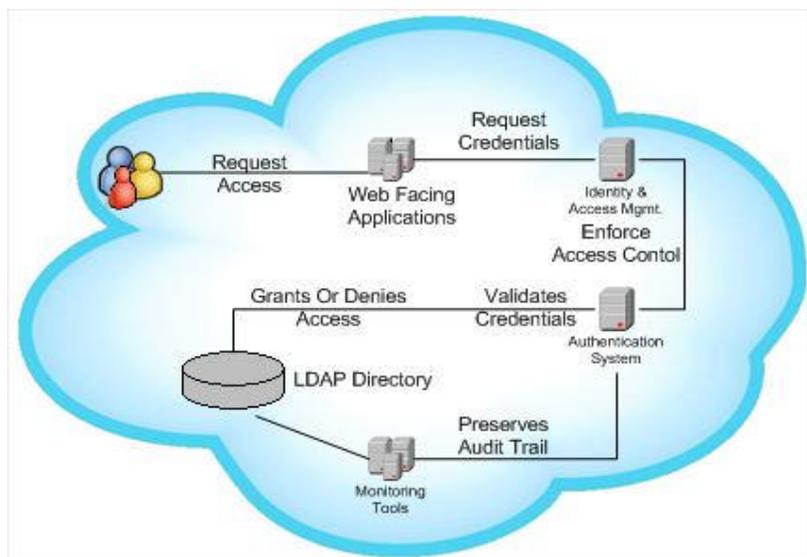


Figure 6.3. Identity & Access Management Scenario

Identity & Access Management Functionality

Identification & Registration

Identification & Registration collects information about entities and creates user accounts and credentials. Registration consists of processes and associated tools used to initially establish the identity of a person or other entity by collecting or validating the appropriate information. Registration may also involve creating appropriate user accounts or completing other administrative actions needed to enter user information in a directory.

A typical identification and registration process includes:

- Collect identification information
- Validate identification information
- Collect registration information
- Register individual and create credential
- Create user account
- Associate identification or credential with access privilege

Functionality available in Identity & Access Management systems may assist with one or more of these processes. For example, a registration function may provide a web page as an entry point for collecting information from a user requesting a new account.

The ability to effectively control access to system resources depends on accurate identification of individuals during the registration process. Ensuring proper identification and registration of users is especially important in an environment, where users register themselves over the Internet. There are several ways to implement Identity & Registration including:

Part D – Generic Security and Privacy Framework

□ Manual processes

A manual process usually requires users to physically submit documents as part of the identification and registration process. Manual processes are typically deployed in organizations that lack the capability to validate identity by integrating human resource systems with web applications.

□ User Self-Service

User Self-Services mechanisms provide end-users with the capability to initiate and conduct transactions using a web application. In addition, users can register online by answering key questions to validate their identity. User self-services are typically integrated with web applications to automate registration of users over an organization Intranet/Internet.

□ Enterprise Resource Planning (ERP) Integration

ERP is a business management system that integrates all facets of the business, including planning, manufacturing, sales, and marketing. As the ERP methodology has become more popular, software applications have emerged to help business managers implement ERP in business activities such as inventory control, order tracking, customer service, finance and human resources. ERP systems are typically integrated with directory services to automate the registration of users as they start working in the organization.

Authentication

Authentication is the process of validating a user credential associated with a previously-identified entity. Authentication within computing systems encompasses both users and systems or processes. Typically, a user wishing access to a system presents credentials (such as a password, token, digital certificate, or biometric characteristic) that is validated by comparison with or analysis of information or characteristics collected during registration of the entity. Authentication services are required by any system that must restrict use to a defined set of users. Establishing an authenticated identity is also critical to several other security functions required to maintain individual accountability, such as assigning access privileges, auditing user activity, or asserting authorship of a transaction. It is possible to use multiple authentication methods, with the type of authentication selected to provide a level of assurance commensurate with the sensitivity of the systems being accessed or the information being requested.

Authentication mechanisms may be used singly or in combination (“two-factor” authentication). Common authentication mechanisms include:

Part D – Generic Security and Privacy Framework

□ Username/Password

Username and passwords are a combination of an identifier and a shared secret, typically an alphanumeric string of characters. Username and password authentication mechanisms are the most commonly deployed, but suffer numerous, well-documented shortcomings and vulnerabilities. Supplementary functions within an Identity & Access Management system can address the weaknesses of using passwords, such as functions that enforce length requirements, password composition rules, password expiration, and prevent password reuse.

□ Token

A token is a hardware device that provides an authentication credential, either by storing user information or by supplying information used in an authentication process. A common type of token (RSA SecurID) supplies a time-synchronized one-time password. Tokens mechanisms usually augment shared-secret information, such as a PIN or password. They are typically deployed in situations that require stronger assurance of authenticated identity than is available with a password alone.

□ Biometrics

Biometric mechanisms provide authentication based on measurable physical characteristics. Biometrics measure or record some physical characteristic of a human users, such as a fingerprint, voice pattern, hand geometry, retinal topology, iris patterns, or facial characteristics. The biometric information is then analyzed and compared with information previously collected or measured during a registration process.

□ Smart cards

Smart Cards are electronic devices that contain memory and may include processing capabilities. Smart cards store and process user credentials and records. They may also be used in conjunction with digital certificates and other physical security mechanisms.

□ Digital certificates

A digital certificate is an electronic data set that contains identifying information about a user. The information contained in the certificate is validated through use of a public-private key encryption protocol linking the identifying information to a certificate-issuing body, the Certificate Authority (CA). Digital certificates have many applications (including digital signing, data encryption, message encryption, and non-repudiation), but they are used by authentication systems to verify the identity of a user. An individual wishing to use a digital certificate for authentication applies to a CA through a registration process. Digital credentials are extremely resistant to forgery, but are currently employed in limited, specialized environments because of the practical difficulties experienced in developing large-scale systems for distributing, managing, and revoking certificates.

Authorization & Access Control

Authorization & Access Control consists of processes and tools that regulate the access privileges of entities (either users or processes). Access to specific information systems, applications, functions, and resources can be regulated. An

Part D – Generic Security and Privacy Framework

Authorization & Access control system ensures that an authenticated user has sufficient rights to perform required operations. Additionally some organizations plan to deploy granular access control for system resources and functions.

Authorization can be implemented with static access control lists (ACLs), dynamic rules based on business logic, or some combination.

ACL's contain a list of rights to data or functions that a user can perform on an object, such as read, write, and execute. Access rules based on context or business logic can make more sophisticated access decisions that analyze the current state of the user. ACLs and business rules are usually stored within the Identity & Access Management system, typically in the same directory or database repository that houses user security data. Major functionality available in access control systems includes:

□ Role based access control

Role Based Access Control groups access privileges into job-based profiles that can be assigned to users as a unit. Access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role. Role-Based Access Control provides improved management of access, but must often be supplemented with user-based extensions or exceptions to attain the desired level of flexibility.

□ Context based or policy-based access control

Context-based or policy-based access control functions provide mechanisms for dynamic resolution of access control decisions, rather than requiring static, list-based access policies. This functionality allows access to resources based on business logic that is not easily stored statically in a database. For examples, some access decisions must be made at the time of the request; such as limitations on access based on location or time of day. Other access decisions have a transactional component that depends on current state or the content of a request, e.g., limiting an approval function to a specific dollar amount.

□ Web Access Management, or Web Access Control

Control of access to application resources in the web environment is often considered as a separate capability from access control in general. This is primarily based on the availability of vendor products that target access management functions for web applications, rather than any fundamental difference in access control requirements. Convergence of functionality is apparent in vendor offerings in this area. Some commercial products now have interfaces or agents for connectivity to mainframes and enterprise applications (e.g., HR or CRM systems) that extend authentication and access control functionality to these environments.

□ Single Sign On

Single Sing-On is an authentication process that provides access to two or more applications following a single login. Single Sign-on reduces or eliminates the need for the user to enter further authentications when switching from one application to another. Single Sign-On is typically deployed to streamline the authentication process for users.

Part D – Generic Security and Privacy Framework

Directory Services

Directory services provide storage mechanisms for security information used to make authentication and access control decisions. Security data may include user passwords, credentials, digital certificates, access privileges, organizations, groups, roles, resources, etc. Fundamentally, directories just define relationships between data elements, while security services such as authentication and authorization manage the risk associated with them. Distributed security systems rely heavily on the directory as an information repository and a communication protocol. Application-specific identity-stores support some of the same basic functions as traditional directory servers. The role of directories is evolving to encompass more middleware functions that can integrate heterogeneous applications. As a result, directory hub environments help to bind diverse application components into a logically integrated application environment from a security perspective.

Directory services mechanisms include:

□ Directory services

Directory services provide storage mechanisms for user information and credentials. The Lightweight Directory Access Protocol (LDAP) provides the most common communications protocol for directories. Directories enable organizations to create a centralized repository of user information that can be called by security systems or applications. Directories are typically deployed to provide a single repository of identity information that can be leveraged by multiple applications to authenticate users. Directories may also store other security information, such as access control lists, user attributes, or access rules that implement business logic.

□ Meta-Directories

Meta-Directories collect identity information from other directories and repositories. Meta-directories enable organizations to integrate disparate identity repositories. Meta-Directories are typically deployed to provide a uniform source of identity information by integrating heterogeneous application repositories.

□ Relational databases

Relational Database Management Systems (RDBMS) store data in the form of related tables. Relational databases are powerful because they require few assumptions about how data is related or how it will be extracted from the database. RDBMS are typically deployed to store the data that needs to be frequently searched and updated, or when complex queries and reporting functions are required.

Administration & Provisioning

Administration and provisioning services are a key element of Identity & Access Management. These services collect, manage, and communicate user identity and access privilege information through the administrative interfaces of applications, operating systems, and other managed platforms. In contrast to authentication and access control mechanisms, administration and provisioning systems do not

Part D – Generic Security and Privacy Framework

mediate real-time security decisions. Instead, they provide account setup, management, and other centralized support functions critical to the effective assignment and monitoring of user identities, access authorizations, and audit records.

Traditionally, setting up access privileges for new users has taken days, if not weeks, to complete, delaying access workers need to do their jobs. A key function of Administration & Provisioning tools is automation of account setup, allowing new users to be immediately productive when joining an organization. In addition, automated account management functions facilitate local flexibility and rapid response to changes in personnel, roles or policies, most importantly to terminate an account when a user leaves or no longer requires access. Major components include:

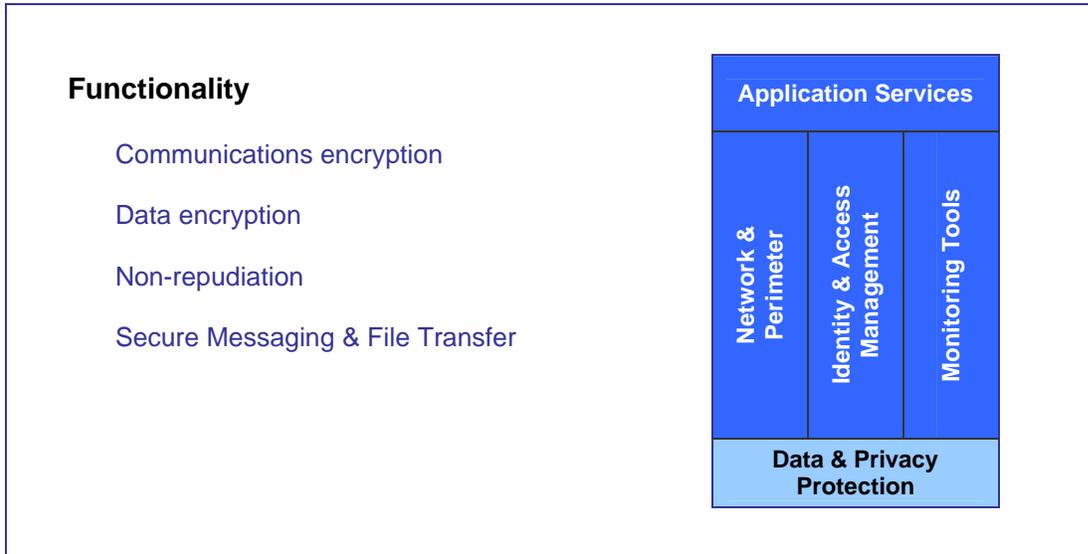
□ **User and resource provisioning system**

User and resource provisioning systems enable centralized control of account setup, modification, and termination. Advantages include more accurate control of user access, enhanced reporting capabilities for auditing user access privileges across multiple systems, and the ability to quickly detect and remove access for terminated users. User and resource provisioning systems typically implement functions for grouping access privileges that can be assigned based on job function. Auxiliary functions may include password synchronization across diverse systems; security approval workflow functions; integration with Enterprise Resource Management systems to enable automated account provisioning and termination; and user self-service functions (e.g., for self-registration or user-initiated password resets.)

□ **Delegated Administration**

Delegated administration allows distribution of account management tasks to designated administrators who are responsible for specific subsets of users. Typically, delegated administration tasks are subdivided based on organizational structure. The organizational structure may include external partners, and usually allows strict limitations on the administrative tasks that are delegated. Delegation of administrative authority can decrease the administrative overhead associated with user account management. A delegated administration function has the additional advantage of placing authorization decisions in the hands of administrators who are typically more closely associated with the end users, and therefore have a better understanding of the access privileges needed for particular job functions.

6.4.5 Data & Privacy Protection



Objective:

Data & Privacy protection mechanisms safeguard data from unauthorized access during transmission or storage.

Description:

Data and Privacy Protection mechanisms use encryption and non-repudiation services to safeguard the confidentiality and integrity of information. Encryption is one of the most effective ways to achieve data security. In order to read an encrypted file, an individual must have access to a secret key or password that enables decryption of the data. These security components enable widespread implementation of cryptographic services in applications and the enterprise infrastructure. Usually organizations aggregate information types into data classifications that guide the selection of appropriate Data & Privacy Protection mechanisms.

Context

Data & Privacy Protection components integrate with most other security architecture technology elements. Data & Privacy Protection mechanisms are integrated in the following way:

- Network & Perimeter components provide traffic filtering and access capabilities to protect communications channels and data stores from unauthorized traffic and malicious content. Data & Privacy protection mechanisms provide the capabilities to encrypt communication channels with remote systems, or between sensitive nodes (such as security devices) of an internal environment.
- Identity & Access Management components provide authentication credentials and enforce access rights. Data & Privacy protection mechanisms provide encrypt functions for communication channels

Part D – Generic Security and Privacy Framework

- (e.g., SSL for web applications). Encryption algorithms and key management protocols such as PKI may provide functionality (authentication, encryption, digital signing) used by both systems.
- Monitoring Tools provide a repository for archiving logs (i.e. successful & failed messaging attempts, integrity checks, revoked credentials, etc.). In addition, Data & Privacy protection mechanisms provide the ability to encrypt communication channels with monitoring applications or to protect the confidentiality and integrity of data (with encryption, message signing, hashing, etc.) stored in auditing and logging databases.
 - Application Services components provide transactional security services to messaging applications. In addition, Data & Privacy protection mechanisms provide capabilities to encrypt communication channels for end-to-end systems and application transactions.

Figure 6.3 illustrates an example of secure file transfer mechanisms that enable an application to securely transfer batch files for processing. An application authenticates the credentials of the requesting by validating them credentials against an enterprise directory. The application then establishes an encrypted session between the system end points to protect the file contents during transfer.

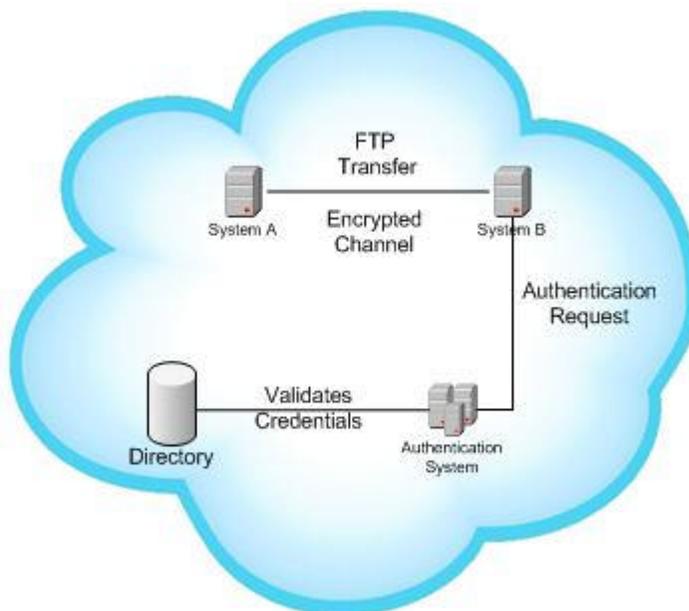


Figure 6.3 -Data & Privacy Protection Scenario

Data and Privacy Protection Technology Functionality

Communications Encryption

Communication encryption systems include hardware and software mechanisms that protect the confidentiality of data in transit. Encryption is usually deployed to safeguard sensitive data being transmitted across a network, preventing eavesdropping and ensuring privacy. Encryption and decryption generally require

Part D – Generic Security and Privacy Framework

the use of some secret information, referred to as an encryption *key*. For some encryption mechanisms, the same key is used for both encryption and decryption (symmetric encryption, or private key encryption); for other protocols, the keys used for encryption and decryption are different (asymmetric, or public/private key encryption, or just public key encryption). Common communications encryption implementations include:

❑ **Secure Sockets Layer (SSL)**

SSL is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public/private key mechanism to authenticate the server and to securely exchange a session key for symmetric encryption of data transferred over the SSL link. SSL is commonly deployed to encrypt Internet communications channels for conducting secure transactions over the Internet. However, it is also frequently used for inter-application or inter-process communications within an application architecture, to protect the transfer of sensitive application or security data.

❑ **IP Security (IPSEC)**

IPSEC is a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSEC is typically deployed to implement Virtual Private Networks (VPN's). Although gaining acceptance, IPSEC is not universally available despite its status as an IETF standard.

❑ **Virtual Private Network (VPN)**

VPNs are constructed by using public networks (e.g., the Internet) to securely connect nodes. VPN systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. VPNs are typically deployed at organization Internet gateways to create encrypted virtual tunnels that are transparent to the end-user.

❑ **Secure Shell (SSH)**

SSH is an application used to log into systems over a network with the purpose of executing commands in remote machines, and to move files from one machine to another. SSH can also be integrated with other security solutions to provide strong authentication and secure communications over insecure channels. SSH is typically deployed as a replacement for rlogin, rsh, rcp, and rdist services.

Data encryption

Data encryption services are mechanisms that protect the confidentiality of stored data. Encryption of stored data is conceptually straightforward, but is subject to a variety of practical limitations. Performance issues caused by the overhead of encryption and decryption steps are usually major considerations. Another important issue is how to provide for archiving and retrieving encrypted data in the event that the owner of the encryption key becomes incapacitated or leaves the organization. Various key escrow mechanisms have been developed to protect encryption keys while preserving the confidentiality of encrypted data. In many cases, data encryption is applied selectively to protect sensitive data, as defined by an organization's information security policy.

Part D – Generic Security and Privacy Framework

Data encryption approaches include:

□ Drive encryption tools

Drive encryption tools enable system owners to safeguard the confidentiality and integrity of sensitive data. Drive encryption tools are product agnostics applications that are typically deployed to safeguard stored data.

□ Database Encryption

Some commercial databases include data encryption functions as standard or add-on features. Considerations when contemplating use of database encryption functions include performance issues and the impact on other database functions, such as indexing.

□ Pretty Good Privacy (PGP)

PGP is a technique that can be used for encrypting messages, but it also has a function in some versions to protect files or drive partitions. PGP is one of the most common ways to protect messages on the Internet because it is effective, easy to use, and free (for non-commercial purposes). PGP is based on the public-key method, which uses two keys – one is a public key that is disseminate to anyone from whom you want to receive a message. The other is a private key that you use to decrypt messages that you receive.

□ Microsoft Encryption File System (EFS)

EFS, included with the Windows® 2000 operating system, provides file encryption technology to store NTFS files encrypted on disk. EFS specifically addresses security concerns raised by tools available on other operating systems that allow users to physically access files from an NTFS volume without an access check. EFS is typically deployed with Active Directory to provide a centrally managed repository of end-users encryption keys.

Non-repudiation

Non-repudiation mechanisms provide tamperproof evidence that a specific action or transaction has occurred. In addition, non-repudiation services are able to produce legally binding evidence. Non-repudiation may require auxiliary services such as time stamping, receipting, or other functions that validate the success or failure of a transaction. Controls the implement non-repudiation prevent an individual from being able to deny receipt, submission, or delivery of a message. Non-repudiation can be achieved through a combination of message integrity, digital signing, and digital notarization functions.

Non-repudiation services are usually deployed when a specific action or transaction needs to provide legally binding evidence. Examples of these situations are financial transactions where one must obtain legal permission before an action is commenced. The most robust form of non-repudiation uses functions provided by PKI systems for digital signatures.

□ Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is the technology that enables digital security through the utilization and management of digital certificates. A PKI is a networked system of certificate authorities (CAs), registration authorities (RAs),

Part D – Generic Security and Privacy Framework

certificate management systems (CMSs) and X.500 or LDAP directories. It enables two parties unknown to each other to exchange sensitive information over an unsecured network like the Internet. PKI uses public and private keys to authenticate and encrypt information. PKI are typically deployed to enable applications to provide authentication, integrity, confidentiality, and non-repudiation security services to end-users.

Secure Messaging & File Transfer

Secure Messaging & File Transfer mechanisms use authentication, authorization, and encryption services to protect the confidentiality and integrity of email, file transfers, and other electronic transactions. Secure Messaging & File Transfer security services are used to provide a holistic end-to-end messaging security solution. Typically, Secure Messaging & File Transfer mechanism use other services, such as encryption, to protect the data while in transit. Implementations of Secure Messaging & File Transfer include:

❑ Secure Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is a version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology. Originally, it was expected that S/MIME would be widely implemented, making it possible for people to send secure e-mail messages to anyone, even if they are used a different e-mail client. In fact, S/MIME has not been widely deployed due to the intrinsic complexity of key management issues.

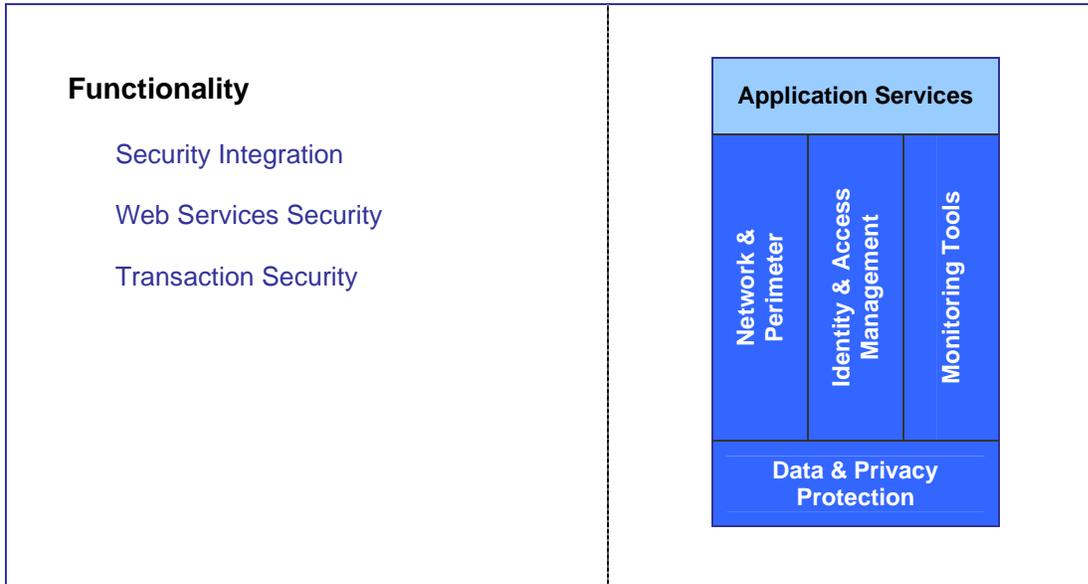
❑ PGP

PGP is a common technique for encrypting email messages. In addition, PGP is one of the most common ways to protect messages on the Internet because it is effective and widely available as freeware for non-commercial purposes. Commercial versions of PGP are also common among institutions that have occasional needs to transfer secure messages or files. PGP is based on the public-key method, which uses two keys – one a public key distributed to anyone you desire to communicate with, and the other a private key used to decrypt received messages. In addition, PGP can be used to encrypt stored data.

❑ Secure File Transfer Protocol (FTP)

Secure FTP provides transparent encryption and authentication services to securely transfer files between systems. Secure FTP is typically deployed to address security concerns of the FTP protocol (which is neither securely authenticated nor encrypted) when transferring sensitive information, user credentials, or batch files between open networks.

6.4.6 Application Services



Objective

Application services provide architectural guidance for the deployment of security services to applications.

Description

A typical organization has a variety of applications that are deployed with embedded security services like authentication, access control and auditing functions. Managing security across multiple applications becomes increasingly difficult as the number of applications and systems grows. Historically, each application, operation system, or platform has deployed its own security functions. Application Services security components allow externalization of security functions, in whole or in part. Application services also provide standards and design approaches for security functions in a web services environment or for transactions in a middleware environment.

Context

Applications services components may call security services from other technology domains.

- Identity & Access Management components store and provide authentication credentials to legacy applications. For example, authorization services deployed as privilege management infrastructures can provide fine-grained access control functions that are called from applications through defined interfaces.
- Monitoring Tools provide a repository for archiving application auditing and logging information.
- Data & Privacy Protection mechanisms provide capabilities to encrypt communication channels for transactions and web services. Encryption

Part D – Generic Security and Privacy Framework

services can also provide external functions to applications that are used to protect individual transactions or transaction components.

Application Services Technology Functionality

Security integration

Security integration services include interfaces, API's, and toolkits that allow integration of applications with external security services. Security services such as authentication, access control and auditing have been typically deployed as part of legacy applications. Increasingly, legacy applications are integrated into multi-tier architectures that wrap legacy functions with user interfaces offering increased functionality or usability. In addition, most external security services require some form of communication with applications, in the form of passing credentials, session management tokens, or calls from applications to security services to execute specific functions. Security integration components include:

□ Application servers

Application servers handle all application operations between users and an organization's backend business applications or databases. Application servers are typically used for complex transaction-based applications. To support high-end needs, an application server has to have built-in redundancy, monitors for high-availability, high-performance distributed application services and support for complex database access. Application servers are typically deployed in multi-tier architectures in which high volumes of transactions are processed.

□ Web Access Management/Web Access Control API

Commercial Web Access Management or Web Access Control systems provide interfaces or APIs for use by applications. Most of the native functionality of these security systems may be externalized to allow custom-developed software to take advantage of authentication, access control, and auditing functions.

Web services security

Web Services security mechanisms are software components that provide the ability to assemble and run solutions dynamically from a series of application services operating to common standards. Because Web services are built using existing standard Internet technologies, they are agnostic to any particular technology platform. Using Web services, applications that were built entirely independently of one another can interoperate. Web services provide open and extensible tools/standards for building secure XML enabled web services.

GSA and DOD recently announced that they joined the Liberty Alliance project in effort to standardize web authentication. The Liberty Alliance includes technology for handling username and password based on the Security Assertion Markup Language (SAML). At this time, organizations are carefully observing the proposed web services security standards in order to determine the impacts to its enterprise security strategy, planning and deployment efforts. Web services security approaches currently include:

Part D – Generic Security and Privacy Framework

❑ **WS-I Security**

WS-I is an open, industry organization chartered to promote Web services interoperability across platforms, operating systems, and programming languages. The organization works across the industry and standards organizations to respond to customer needs by providing guidance, best practices, and resources for developing Web services solutions. The WS-I intends to give corporations guidance on how to use security effectively with Web services in different business situations and clarify any ambiguities in the security specifications for IT providers

❑ **XML – Encryption**

XML Encryption will provide an encrypted key mechanism and a method for providing a Uniform Resource Identifier (URI) for a known key. It will support XML Signature's selective signing, and will support or interoperate with XML Schemas. XML Encryption will also support the requirements of the OASIS XML-Based Security Services Technical Committee (SSTC).

❑ **XML – Signature**

XML Signatures are digital signatures designed for use in XML transactions. The standard defines a schema for capturing the result of a digital signature operation applied to arbitrary data (often XML). Like non-XML-aware digital signatures (e.g., PKCS), XML signatures add authentication, data integrity, and support for non-repudiation to the data that they sign. However, unlike non-XML digital signature standards, XML Signature has been designed to both account for and take advantage of the Internet and XML.

❑ **XKMS – Key Management Standard**

XML Key Management Specification (XKMS) defines protocols for the registration and distribution of public keys. The keys may be used with XML Signatures, a future XML Encryption specification, or other public key applications for secure messaging. No underlying public key infrastructure is required, but the protocols are compatible with several systems, including Pretty Good Privacy (PGP), Public Key Infrastructure X.509 (PKIX) and Simple Public Key Infrastructure (SPKI).

❑ **XACLM – XML Access Control Markup Language**

XACML is a framework for defining a set of privileges required to perform an operation, including access to identity information and external functions (like access policy and time of day).

❑ **SAML – Security Assertion Markup Language**

SAML is a framework for exchanging identification information; for example, a trusted third-party (such as a PKI CA or a network login server) could provide a signed set of assertions identifying my identity. SAML is the basis of the Liberty Alliance federated single sign-on facility; Microsoft may also adopt Passport to use it. SAML defines mechanisms to exchange authentication, authorization and non-repudiation information, allowing single sign-on capabilities for Web services.

Part D – Generic Security and Privacy Framework

Transaction security

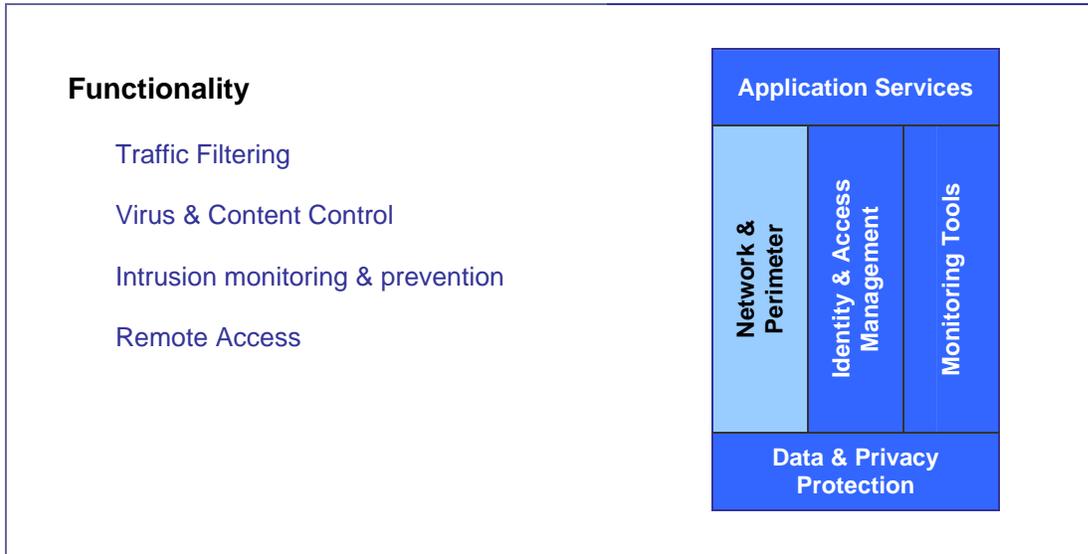
Transactional security mechanisms provide end-to-end authentication, access control, and auditing services for systems in multi-tier architectures. For instance, a common situation in the design of web server applications is that transactions to back-end databases or legacy applications originate from applications or application server platforms (such as Weblogic or Websphere). Such calls often use generic system accounts for access. There are several risks with this architecture:

- The generic system accounts are typically given broad access privileges to the core databases or legacy systems, which often contain sensitive information.
- The generic system accounts may not have the same level of security controls (e.g., authentication, access control, encryption, audit logging) that would be required for an individual user account on the same system.
- User security credentials may not be associated with individual transactions, making it difficult to authenticate or authorize transactions based on the user's privileges, or to audit the transaction activity. This lack of accountability also compromises the non-repudiability of the transaction.

Transactional security components identify architectural options for providing end-to-end security. Potential approaches include:

- Use of transactional middleware that provides security functions (authentication, access control, encryption, audit logging) at the individual user level, the system entity/process level, or both.
- Building accountability features into the application to track the identity of the user requesting a transaction, either to record the activity for future reference, or to pass the user security credentials to the backend database or legacy application.
- Use of web services security standards that provide security functions to enable end-to-end security in a web services environment.

6.4.7 Network & Perimeter Security



Objective:

Restricting unauthorized access to increasingly complex and distributed networks.

Description:

Network & Perimeter functions include network access control mechanisms designed to enforce security policy at boundaries between networks. As such, perimeters are more than just firewalls. A typical large organization's perimeter includes firewalls as a primary defense mechanism, logical partitioning of network segments, network intrusion detection at key junctions in the network; host-based intrusion detection on critical application servers; and additional boundary protection services such as virus-checking, and Web or e-mail content scanning. In addition, perimeter services are increasingly integrated with VPN services, which extend an organization's internal network with remote sites or users.

Context

Perimeter infrastructure components integrate with all the other security architecture technology areas:

- Identity & Access Management components store and provide authentication credentials to remote users and network device administrators. Network & Perimeter components provide traffic filtering capabilities to protect the underlying Identity & Access Management infrastructure, and is usually a point of integration to make sure communications between security components are handled appropriately by firewalls and other network functions.
- Monitoring Tools provide a repository for archiving logs created by network devices (e.g., firewalls, routers, VPN gateways, Intrusion Detection Systems, and virus detection systems). Network &

Part D – Generic Security and Privacy Framework

Perimeter components provide network access control capabilities to segment and protect the monitoring environment.

- Data & Privacy protection mechanisms provide the capabilities to encrypt communication channels for application and file transfers. In addition, Network & Perimeter components enable remote users with VPN clients to safeguard communication channels.

Figure 6.4 illustrates an example of how Network & Perimeter remote access capabilities enable remote users with a VPN client to obtain access to corporate Intranet resources. The VPN device will leverage encryption mechanisms to safeguard the information in transit. In addition it will authenticate the user using an Identity & Access Management system that requests and validates credentials from an enterprise directory. In any event the audit trail for the connection, authentication, and authorization of users is preserved by taking advantage of the capabilities in monitoring tools.

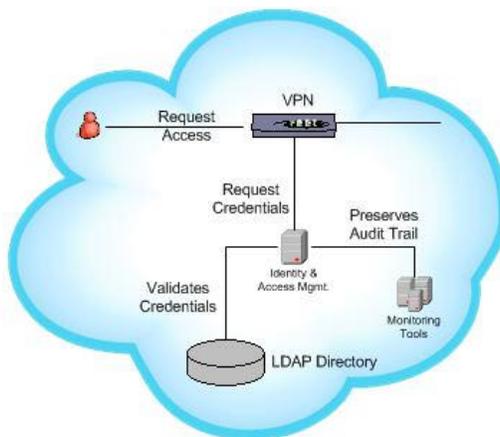


Figure 6.4 Network & Perimeter Scenario

Network & Perimeter Technology Functionality

Traffic filtering

Traffic filtering components inspect and regulate network traffic based on source, destination, type of message, and content. Organizations deploy traffic filtering and control systems to constrain access to network resources. For instance, firewalls examine and constrain network traffic, thereby allowing certain applications and resources to send or receive traffic through the perimeter. Subsequently, load balancing and fail-over mechanism are deployed to assure the availability of the underlying infrastructure. In addition, networks are logically segmented to isolate resources and enforce security policy. Traffic filtering mechanisms include:

□ Firewalls

Firewalls are systems, or combinations of systems, that enforce a boundary between two or more networks. Packet filtering firewalls inspect and filter network traffic at a coarse, physical level, thereby allowing only certain IP

Part D – Generic Security and Privacy Framework

addresses (or ranges of addresses) and applications to send or receive traffic through the perimeter. Other firewalls, such as application proxies and stateful inspection technologies, mediate traffic based on application data content or on the existence of valid sessions that match incoming traffic with corresponding requests from the internal network. Firewalls are typically deployed to segregate networks (i.e. Private Networks vs. Internet). In addition, Firewalls enable organizations to enforce security policy on allowable traffic at the Internet gateway.

□ **Routers**

Routers are devices that forward data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs, or a LAN and its ISP's network. Routers are typically deployed throughout the organization at key network exchanges. Routers may perform simple firewall functions that enable an organization to enforce an access control list or security policy.

Virus and Content Control

Virus and Content Control capabilities enable organizations to filter contaminated content at various enforcement points. Network anti-virus products come in two forms: E-mail desktop/server-based and gateway based. E-mail desktop/server-based anti-virus software is loaded on e-mail servers or on desktops to scan incoming/outgoing e-mail messages and system files for viruses.

Gateway-based Virus & Content Control capabilities enable organizations to enforce security policies at network boundaries. Some of these products work as network appliances or are integrated into proxy server software. A common feature is the ability to scan data as it is transferred via HTTP, FTP and SMTP protocols. Virus & Content Control mechanisms include:

□ **Anti-Virus**

Anti-virus solutions enable organization to scan data and incoming or outgoing emails in the organization. As with intrusion detection a consideration for virus filtering is whether to employ filters along the network perimeter, on the system, or a combination of both. Anti-virus solutions are typically deployed at the organization's Internet gateway to scan incoming email messages and attachments. In addition, anti-virus solutions are deployed enterprise wide to individual end-systems.

□ **Content Screening**

Content screening solutions enable an organization to monitor HTTP, and FTP traffic over the network. Content screening applications can also be used in conjunction with proxy-servers, allowing the organization to monitor other Internet protocols. As with other solutions, performance problems can be expected with busy networks without load-balancing capabilities. Content Screening solutions are typically integrated with proxy servers to monitor and filter Internet connections.

Part D – Generic Security and Privacy Framework

Intrusion Monitoring and Prevention:

Intrusion monitoring and prevention tools are used to detect the existence of potential network or host attacks on systems so that protective action can be taken. Intrusion monitoring systems recognize common attack patterns from a database of known “attack signatures” developed by vendor and industry research. Some intrusion detection and prevention systems also analyze traffic and usage patterns to allow detection of anomalous patterns. Intrusion monitoring and prevention tools provide a fast and automated mechanism for organizations to be pro-active in identifying and stopping intruders. Intrusion monitoring and prevention includes:

❑ Network Intrusion Detection System (NIDS)

A NIDS solution captures and analyzes packets of information as they travel across the network. In addition, NIDS interprets hostile activity on the network by recognizing the network traffic patterns that indicate attacks. NIDS sensors are typically deployed in front of the Internet gateways as well inside the organizations.

❑ Hosts IDS

Host IDS solutions detect intruders or abuse by analyzing audit data from the operating systems it supports. Using a host security policy, the tool points policy violations (i.e. such as multiple login failures) that maybe caused by an attacker. It also detects more subtle irregularities in user behavior that can indicate a masquerading user or other potential troublemaker. Host IDS are typically deployed in addition to Network IDS sensors to provide an additional layer of security to systems that contain sensitive data.

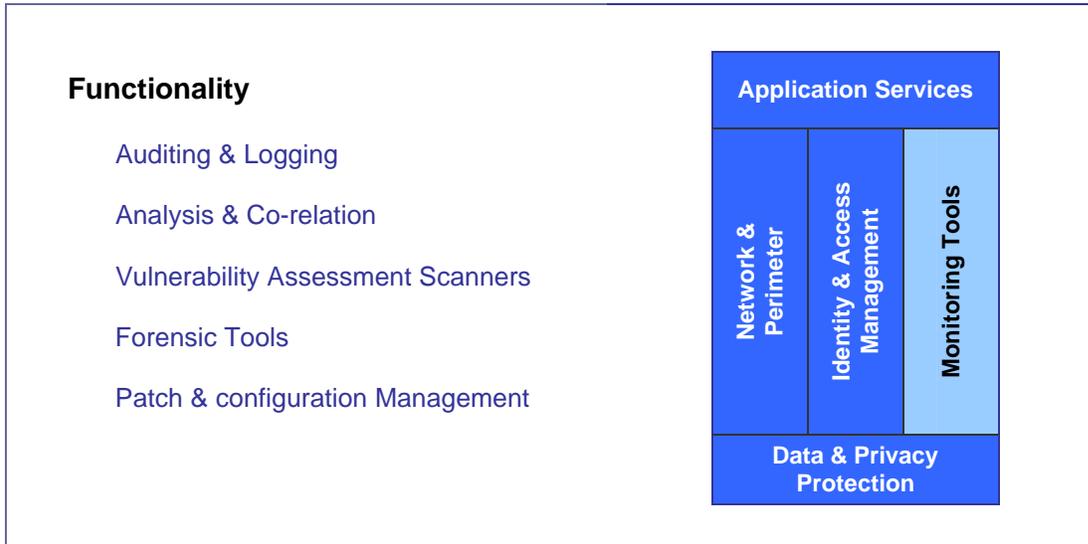
Remote access

Remote access functionality enables external entities or users to securely communicate with internal systems and applications. Virtual Private Network (VPN) clients establish encrypted tunnels, to provide a secure connection through an otherwise insecure network, typically the Internet. As a result, VPN gateways are usually deployed between multiple environments to share services and resources. In addition, VPNs allow administrators to perform remote administration tasks on internal environments, such as development, production, and business partner systems. Remote access mechanisms include:

❑ Virtual Private Network (VPN) Clients & Gateways

VPNs let enterprises transmit network traffic securely over a shared network, such as a public IP network. VPNs create encrypted tunnels between a remote workstation, a remote site, or between a trading partner site and the enterprise network. VPN’s gateways may be used between work environments (i.e. branch offices and company headquarters) to provide secure communications without requiring dedicated network links. In addition, VPN clients provide a secure method to for remote users to access corporate resources over public networks like the Internet.

6.4.8 Monitoring Tools



Objective:

Monitoring Tools acquire, archive, and analyze information to ensure the integrity, confidentiality, and availability of information.

Description:

Monitoring Tools provide the capability to acquire, archive, analyze, and report on event information from various environments. Generally, organizations preserve audit records to measure performance and assess security issues. For that reason there is a need to preserve the integrity and availability of the logged information.

Typically, organizations operate in a heterogeneous environment that inhibits the effective collection and analysis of auditing information. Several monitoring technologies are available that can standardize the collection of logged information. Monitoring tools also provide a means to make better use of audit and logging data by facilitating comparison of activity across different environments, providing multiple visualization and reporting functions.

Context

Monitoring Tools provide services to other security architecture areas, and may rely on other security technology functions to work effectively. For example:

- Network & Perimeter components provide traffic filtering and access capabilities to protect the underlying audit and logging servers. In addition, monitoring components provide a repository for archiving and analyzing events from network devices (i.e. firewalls, routers, VPN, IDS, etc.).
- Identity & Access Management components provide authentication credentials and access control to end-users of audit log systems. In

Part D – Generic Security and Privacy Framework

addition, Monitoring components provide a repository for archiving and analyzing events (i.e. successful and failed login attempts, file access, etc.).

- Data & Privacy protection mechanisms provide capabilities to encrypt communication channels used by monitoring applications. Monitoring components provide a repository for archiving logs created by Data & Privacy components (i.e. successful and unsuccessful file transfers, integrity checks, revoked credentials, etc.).
- Applications services components provide the necessary APIs to integrate the monitoring capabilities with legacy applications. Monitoring components provide a repository for archiving and analyzing application logs.

Figure 6.5. illustrates monitoring tools that acquire, archive, analyze, and report event information. In this instance network perimeter components (i.e. firewalls, routers, VPN, Anti-Virus appliances, etc.) relay event logs over an encrypted channel to remote logs servers. At the same time, Application and Identity & Access Management components relay account management and application event logs to remote logging servers for analysis and correlation. Authorized staff has access to a viewing and reporting application that produces environment reports and allows for the submission of queries for detailed analysis of collected information. Also note that, in the organization depicted, auditing logs are treated as highly sensitive information that demands the use of a two-factor authentication system (e.g. token).

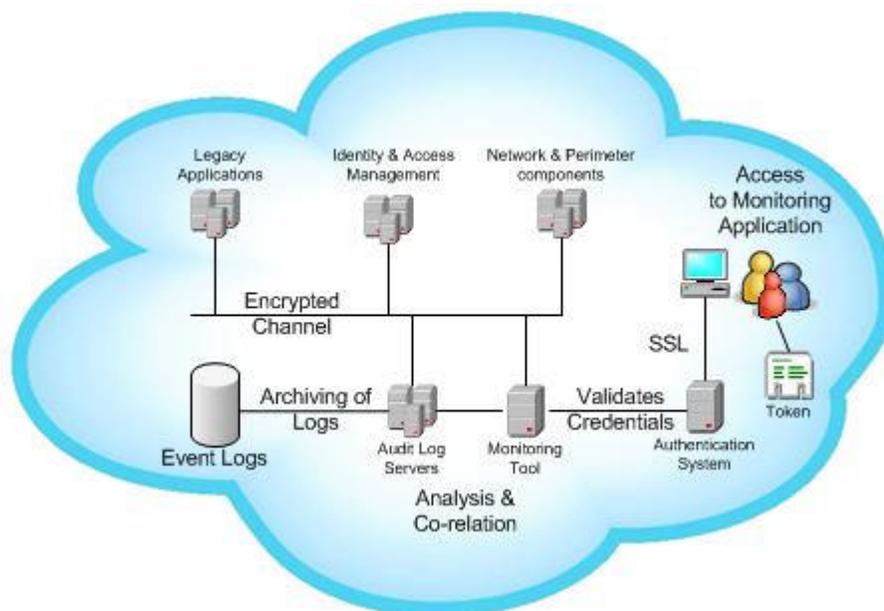


Figure 6.5 – Monitoring Tools Scenario

Monitoring Tools Technology Functionality

Auditing & logging

Auditing and logging mechanisms acquire and archive event information from multiple environments in centrally managed systems. Audit logs typically record information about users, information systems affected, and the time of the events. Audit logs are useful both for maintaining accountability and for investigating suspected security breaches. Most applications include an audit component that logs various types of information about system activity, some of which include security logging. Security logs help security personnel in identifying vulnerabilities, assessing risks to exposure, and determining if the appropriate security controls are in place to comply with security policies and standards.

By deploying enterprise-monitoring capabilities, organizations can centrally manage and collect audit logs from different environments (i.e. operating systems, databases, intrusion detection systems, firewalls, routers, applications). Typically, systems produce large amounts of security audit information, critical for forensic analysis of potential security breaches and attacks, but difficult to store and manage. Auditing and logging includes:

Analysis and correlation

Analysis and correlation mechanisms examine event information from multiple sources to recognize patterns that indicate potential security attacks. Security events occurring throughout the enterprise are aggregated and analyzed to spot similarities and trends. This analysis enables security personnel and contractors to fix vulnerabilities, shut down troublesome IP addresses, and fortify assets that come under frequent attack.

Event correlation is the capability to find similarities among two or more events and use these differences to derive a better understanding of what is actually happening in the organization perimeter. Analysis and correlation engines collect, aggregate, normalize, analyze, and evaluate monitoring to produce reports and visual displays of security status. Analysis and correlation includes:

❑ Managed security monitoring services

Third party managed security service providers offer several outsourced monitoring services, including firewall administration and intrusion detection system monitoring. Several outsourced providers also offer analysis and correlation services that draw security monitoring information from multiples sources within one or more organizations. The goal of the analysis and correlation step is to detect traffic and use patterns that may indicate security attacks or incidents. Some commercial monitoring systems provide similar capabilities that can be deployed within an organization, but the expertise and effort required to use them effectively may be prohibitive for smaller organizations. An additional advantage of the out-sourced environment is the larger domain from which attack patterns may be drawn, compared to experience developed within the limited environment of a single organization.

Part D – Generic Security and Privacy Framework

❑ Correlation engine applications

Correlation engines provide the capability to find similarities among two or more events and use these differences to derive a better understanding of what is actually happening in the organization perimeter. Correlation engines are typically deployed to acquire and analyze information from infrastructure components across an enterprise, or even between enterprises or environments. Correlation engines are usually managed by a central support organization.

Vulnerability Assessment Scanners

Vulnerability Assessment Scanners are automated tools that identify system configurations that can be exploited by security attacks. Vulnerability Assessment Scanners tools locate, analyze, and report technical vulnerabilities, in networks, hosts, and applications, that can be fraudulently or accidentally exploited. Vulnerability Assessment Scanners also assess the network architecture and may map network topologies. Similarly, penetration-testing services evaluate perimeter and host security measures from outside of the network perimeter. Penetration testing processes typically include analysis of system configurations, network architecture, and technical weaknesses.

Forensics tools

Forensic tools are used to identify the source and consequences of security breaches. Forensic tools are designed to collect and preserve system data in such a way that it can be submitted as evidence in criminal or civil legal proceedings.

Patch & Configuration Management

Patch and configuration management tools automate the deployment of patches and system configurations in accordance with organizational guidelines, standards, and security policy. Configuration management tools enable organizations to standardize the deployment of system changes in a heterogeneous computing environment. Configuration management tools monitor, analyze and report security updates in order to keep pace with newly discovered and reported system vulnerabilities. These tools also enable organizations to reduce the total cost of security operations by decreasing the number of personnel and the time required to manually update systems. Patch and Configuration Management includes:

❑ Patch management applications

Patch management applications can identify, download, and automate installation of the myriad of patches that are needed to keep servers up to date. Patch management applications are typically deployed in a centrally managed environment.

❑ System imaging tools

System imaging tools enable organizations to quickly deploy standard workstations and servers builds. Use of system and application imaging tools increase software standardization, allow rapid recovery if servers or workstations are compromised, reduce overhead, and enforce security policy. Standard system or application images are usually deployed over the network with minimal administrative support.

7 Appendix

This Appendix contains:

7.1 Diagram of Generic Security and Privacy Framework

The diagram depicts the Technical Security Architecture layer of the Generic Security and Privacy Framework described in Section 6.

7.2 TO 124 Project Work Plan.

APPENDIX 7.1

Technical Security Architecture

Application Services

Integration Interfaces

Interfaces or APIs used to integrate applications with external security services

Web Services Security

Security standards and functions for protecting web services transactions

Transaction Security

End-to-end authentication, access control, and auditing of system & user entities in multi-tier architectures

Network & Perimeter

Traffic Filtering

Inspect and block harmful network traffic based source and destination addresses & ports, or existence of valid sessions; includes network segmentation strategy and design

Virus & Content Control

Inspect traffic and block malicious content such as viruses, worms, Trojan horses, or other unacceptable content

Intrusion Monitoring

Detect attempted attacks on networks, operating systems, and servers; alert operations personnel to initiate appropriate incident response

Intrusion Prevention

Detect and block attempted attacks on host operating systems and applications

Remote Access

Provide secure VPN and dial-up services

Identity & Access Management

Identification & Registration

Identify and enroll users, and create security credentials

Authentication

Validate user credentials when access to a system is requested; includes single sign-on and session management functions

Authorization & Access Control

Assign and enforce access privileges for specific data and resources based on authenticated identity of user

Directory Services

Store and manage user information, security credentials, & other security data

Administration & Provisioning

Provision and manage user and system accounts, including password synchronization and user self-service functions

Monitoring Tools

Auditing & Logging

Recording, storing, and reporting user and system activity and access privileges

Analysis & Correlation

Consolidating and processing audit data, log data, and other security information to detect patterns that indicate potential security incidents

Vulnerability Assessment

Tools to inspect networks, host systems, and applications for potential security weaknesses

Forensics Tools

Tools to inspect systems and security information to gather evidence about suspected security breaches

Patch & Configuration Management

Tools to detect or deploy system patches, updates, or fixes; tools to maintain the integrity of host or

Data & Privacy Protection

Communications Encryption

Protect confidentiality and integrity of communications channels with encryption techniques

Data encryption

Protect confidentiality and integrity of data stored in databases with encryption

Message Integrity & Non-repudiation

Provide evidence that will prevent repudiation of authorship or content of a transaction; prevent unauthorized modification of transmitted data and/or detect modification attempts

Secure Messaging & File Transfer

Protect confidentiality and integrity of email messages and file transfers

APPENDIX 7.2

ID	Task Name	Mar			Apr				May				Jun					
		9	16	23	2	9	16	23	30	6	13	20	27	4	11	18	25	1
1	Project Kickoff																	
2	Hold internal kickoff meeting																	
3	Conduct team orientation																	
4	Discuss project roles and responsibilities																	
5	Hold project kickoff meeting																	
6	Discuss project objectives																	
7	Plan initial security workshop agenda																	
8	Conduct Security Architecture Workshops																	
9	Conduct initial Security Architecture Workshop																	
10	Prepare workshop objectives																	
11	Prepare workshop participant list																	
12	Prepare workshop discussion guide																	
13	Prepare security architecture topics list																	
14	Hold initial security architecture workshop																	
15	Summarize workshop discussion and distribute for comment																	
16	Revise workshop discussion and distribute updated summary																	
17	Conduct Security Framework Review Workshop																	
18	Prepare workshop objectives																	
19	Schedule workshop meeting location																	
20	Prepare workshop participant list																	
21	Prepare workshop discussion guide																	
22	Hold Security Framework Review workshop																	
23	Summarize workshop discussion and distribute for comment																	
24	Conduct Security Architecture Implementation Strategy Workshop																	
25	Prepare workshop objectives																	
26	Schedule workshop meeting space																	
27	Prepare workshop participant list																	
28	Prepare workshop discussion guide																	

APPENDIX 7.2

ID	Task Name	Mar				Apr				May				Jun			
		2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15
31	Develop Conceptual Security & Privacy Architecture Framework	[Redacted]															
32	Define Security & Privacy Architecture Framework objectives	[Redacted]															
33	Define use scenarios for framework	[Task bar]															
34	Analyze security and privacy business objectives from workshop	[Task bar]															
35	Identify existing audit findings, standards, or regulatory compliance issues	[Task bar]															
36	Identify relevant best practices for security and privacy architecture	[Task bar]															
37	Define framework structure and component content and format	[Redacted]															
38	Identify candidate framework components	[Task bar]															
39	Develop definitions for framework components	[Task bar]															
40	Assign framework components to framework structure	[Task bar]															
41	Develop component content	[Task bar]															
42	Define Interim Security & Privacy Architecture Report format	[Task bar]															
43	Prepare Interim Security and Privacy Architecture Report	[Task bar]															
44	Distribute interim report for review and approval	[Task bar]															
45	Brief DOE Architecture group	[Task bar]															
46	Develop FSA Security & Privacy Architecture Specification	[Redacted]															
47	Review comments from Interim Security & Privacy Architecture Report	[Task bar]															
48	Identify existing FSA security and privacy architecture documentation	[Task bar]															
49	Refine the generic Security & Privacy Architecture Framework for FSA environment	[Task bar]															
50	Cross-reference security architecture components with business & technical requirements	[Task bar]															
51	Review FSA Software Life Cycle	[Task bar]															
52	Define Final Security & Privacy Architecture Report format	[Task bar]															
53	Create Final Security & Privacy Architecture Report	[Task bar]															
54	Distribute draft Security & Privacy Architecture Specification for review and approval	[Task bar]															
55	Develop Security Architecture Implementation Strategy	[Redacted]															
56	Perform gap analysis against Security & Privacy Architecture Framework	[Task bar]															
57	Develop plan to integrate implementation strategy into FSA Software Life Cycle	[Task bar]															
58	Define project initiatives to address framework gaps	[Task bar]															
59	Define high-level schedule and project estimates to deploy security architecture	[Task bar]															
60	Distribute draft Security Architecture Implementation Strategy	[Task bar]															

APPENDIX 7.2

ID	Task Name	Mar				Apr				May				Jun				
		2	9	16	23	30	6	13	20	27	4	11	18	25	1	8	15	22
61	Develop & Execute Security Architecture Communications Plan																	
62	Brief business leads on conceptual framework																	
63	Brief CIO on conceptual framework																	
64	Brief business leads on FSA specification & implementation strategy																	
65	Brief CIO on FSA specification & implementation strategy																	
66	Manage Project																	
67	Develop project work plan																	
68	Prepare project issues tracking list																	
69	Manage work plan and budget																	
70	Track and resolve issues																	
71	Track and report status to PMO																	
72	Conduct weekly project status meetings																	
73	Prepare meeting agenda																	
85	Hold weekly status meeting																	
97	Prepare and distribute meeting minutes																	