Secure Email Architecture

NIH Enterprise Architecture

Version 1.0

December 1, 2005

Table of Contents

List of Figures

List of Tables

1.0 Introduction

The mission of the National Institutes of Health (NIH) occasionally requires its employees to securely communicate with non-NIH partners such as researchers, practitioners, and other key stakeholders. The current Public Key Infrastructure (PKI)-based solution that is internally used at the NIH (i.e., from NIH employee to NIH employee or other federal government agencies) is not feasible for some of NIH's external partners to adopt due to the cost and complexity associated with adopting a PKI-based solution. In response, the NIH Chief IT Architect commissioned a team comprised of information technology (IT) and information security technology experts throughout the NIH's various Institutes and Centers (IC) to develop and recommend technology standards for establishing a non-PKI based solution.

This report documents the Security Domain Team's analysis and describes the recommended NIH-wide architectural standards and guidelines for a non-PKI-based secure email communication solution between NIH and external parties. The solution design pattern and technology standards outlined in this report are not a replacement for PKI-based Secure Multipurpose Internet Mail Extensions (S/MIME) technologies already built into most NIH standard desktop email clients or for the adoption of HSPD-12 directives . Therefore, *the recommendations put forth in this report are considered to be an alternative to supplement existing PKI S/MIME capabilities for scenarios where a PKI-based solution it is not feasible* (i.e., imposes an undue technical complexity or cost burden on an external partner). These standards and guidelines specify common components that have been developed and agreed to by a cross-IC domain team, and that this domain team believes can be implemented throughout the NIH. The domain team's recommendations exceed Health Insurance Portability and Accountability Act (HIPAA) security standards for *Technical Safeguards* by providing transmission security through integrity controls and encryption[1].

Specific outcomes of the Security Domain Team's analysis include:

- a recommendation to update NIH's architecture principles for the security domain;
- a recommended secure email pattern (non-PKI-based) that identifies a logical design to be employed and leveraged when current PKI-based S/MIME technology is not practical (i.e., imposes an undue technical complexity or cost burden on an external partner); and
- a recommended secure email brick that identifies technical standards, protocols, technologies and products.

The pattern and brick, which are documented in Sections 2 and 3 of this report, present the NIH baseline and recommended target architectural states as of November 2005, and are current as of the publication date on this report.

[1] HIPAA "Appendix A to Subpart C of Part 164 – Security Standards: Matrix" identifies *Integrity Controls* and *Encryption* as "Addressable" as opposed to "Required".

1.1 Security Domain Team

The domain team, a team of twelve IT and information security subject matter experts (SME) from various ICs throughout the NIH, convened for eight working sessions over ten weeks to develop the secure email architecture pattern and brick presented in this report. The following list identifies the team members who contributed to this effort:

- Larry Washburn, NIA
- Tom Carrington, NCI
- David Hester, NIDCD
- Kevin Stevens, ORS/ORF
- Aubrey Callwood, NICHD
- Joyce Ingle, CSR
- William Hermach, NIMH
- Kevin Hobson, CIT
- Donna Stephenson, NINDS
- Mark Silverman, CIT
- Luis Ochoa, NIDCD
- Rich Trouton, NHGRI

1.2 Scope

The Security Domain Team was commissioned to produce architectural recommendations that address non-PKI-based solutions that enable secure email communication between NIH users and external users for whom PKI-based S/MIME is not practical. Activities outside the scope of the domain team's tasking included the following:

- External user email communication not directly controlled by NIH
- Information security after completion of a communication to an external user (i.e., protection of information not in transit from NIH to an external partner or vice versa)
- Communication or collaboration technologies not identified as email communication
- Stationary data security (encryption) solutions

The team's analysis and recommendations align with the NIH's existing security principles and technology architecture, support information systems that comprise NIH's information architecture, and address secure email communication requirements between NIH and external users where current PKI-based S/MIME is not practical.

To develop its recommendations, the team analyzed NIH's current and future requirements, conducted industry and technology trends analyses, and ensured alignment of proposed solutions with NIH's Enterprise Architecture (EA) and security domain principles. As a result, the team's recommendations:

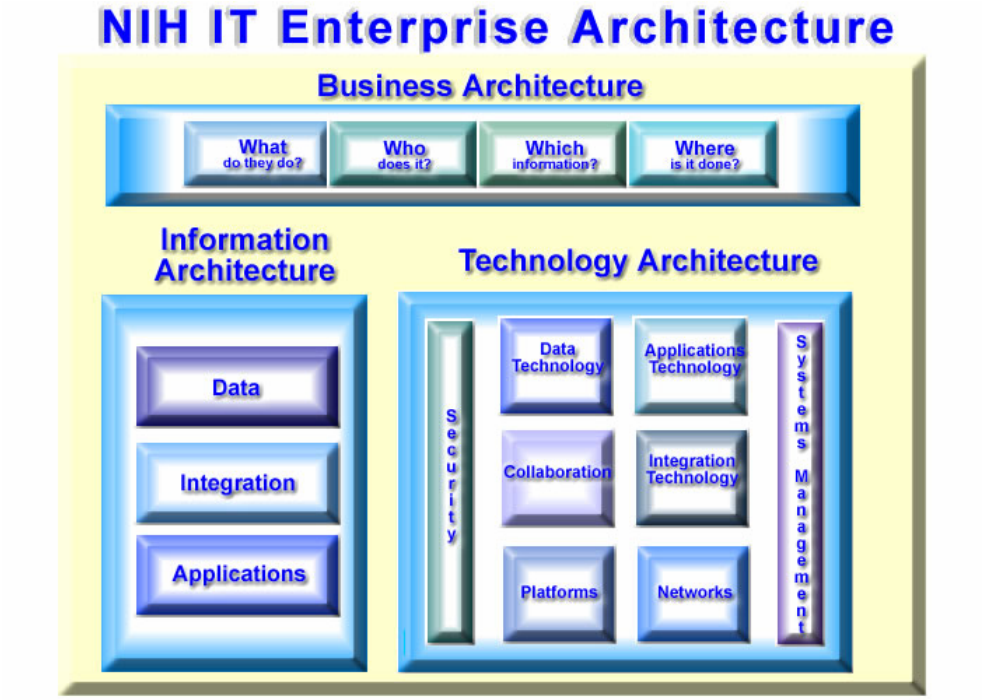
- Operate within NIH's overall technical architecture
- Align with the security domain principles in place at the NIH
- Meet no less than the minimum requirements for secure email communication between NIH and external users
- Minimize undue user burden on NIH and external users
- Minimize undue cost burden on the NIH and external users

- Interface with NIH systems as needed and provide flexibility for external users.

1.3 Alignment With the NIH Enterprise Architecture Framework

As illustrated in the following figure, the NIH EA framework recognizes three distinct component architectures — business architecture, information architecture, and technical architecture.

Figure 1. NIH EA Framework



The Security Domain is a technical domain of the NIH Technology Architecture. To learn more about the NIH EA framework visit the NIH EA Website[2].

1.4 Analysis

Secure email (email encryption) is a sub domain within the larger domain of IT Security. It integrates with NIH's current and future technical infrastructure and specific hardware and software technologies to ensure secure email communication between email senders and recipients. Establishing standards for secure email communication provides users with appropriate levels of assurance that sensitive communications and exchange of information via email will not be compromised, whether originating internal to or outside of the NIH infrastructure.

The Security Domain Team worked from the following premises when conducting its analysis:

[2] http://enterprisearchitecture.nih.gov

- Secure email communication is a mechanism to protect sensitive information such that its receipt or interception by a third-party during transmission does not compromise the secure nature of the information. Senders and recipients communicating via secure email have trusted status. Parties not holding trusted status are unable to view the secured communication or attachments.
- Solution(s) must establish trust between internal and external senders and recipients.
- Solution(s) must allow NIH users to send a secure email communication and/or attachment that is received and read by a recipient who is inside or outside of the NIH infrastructure.
- Solution(s) must allow an external party (i.e., a user not holding a trusted identity with NIH) to register by some means before sending a secure email communication and/or attachment that is received and read by a recipient who is inside the NIH infrastructure.
- Solution(s) must minimize operational impact on the user.
- Solution(s) must minimize cost impact on NIH and external users.

1.5 Security Principles

One of the domain team's objectives was to validate the existing security domain architecture principles. As a result of this analysis, the Security Domain Team recommends:

- No changes to eleven of the thirteen existing principles
- Modifications to two of the thirteen existing principles to provide a clearer position on *Security Control Availability* and *Security Control Default*
- The addition of a new principle, *Alignment with Security Policies*

1.5.1 Validation of existing principles

Table 1 presents the eleven existing security principles the domain team validated.

Table 1. Security Architecture Principles

Principle	Rationale
Level of Security: Information systems (including application, computing platforms, data and networks) should maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of information.	As a practical matter, perfect security cannot be achieved in any information system. Therefore, security controls should be applied to reduce risk to an acceptable level.
Security Control Selection: The selection of controls should be based on a risk analysis and risk management decision.	The selection of new controls should consider both the degree of risk mitigation provided by the control and the total cost to acquire, implement, and maintain the control.
Security Control Management: Technical security controls will not be implemented without the implementation of associated management and operational controls.	Unmanaged security controls can present a greater risk than the absence of security controls.
Security Planning: Information system security will be built into systems from their inception rather than "bolted-on" after system implementation.	The cost and complexity of adding security controls to a system after it is already in production is significantly greater.
Measurement: All functional security requirements that define "what" a system or product does will have associated assurance requirements to define "how well it does it".	Security controls will be able to be reviewed or audited through some qualitative or quantitative means in order to ensure risk is being maintained at acceptable levels.
Security Control Modularity: Safeguards will be modular so that they may be removed or changed as the system and enterprise risk profile changes.	It is prudent to minimize the interdependence of controls so that controls can be conveniently interchanged or modified.
Security Control Standardization: Selection of controls will consider the ability of the control to be applied uniformly across the NIH enterprise and to minimize exceptions.	Achieving standards based environment will reduce operational costs, improve interoperability, and improve supportability.
Compartmentalization and Defense-In-Depth: The architecture will embrace the concepts of compartmentalization and defense-in-depth.	Compartmentalization localizes vulnerabilities and defense-in-depth establishes a series of imperfect countermeasures.
Manual Operations: Controls will minimize the need for manual operations.	Manual operation can create vulnerabilities and cause disruption of service due to misinterpretation and misconfiguration.
Levels of Protection and Response: Controls will not impose unreasonable constraints or operate in a manner that causes unreasonable response.	Controls should provide only the required level of protection, alerting, and response.
Separation of Duties: The designer and operator of a security control will be independent.	Separation of duties ensures there is not a conflict of interest in design of the security control.

1.5.2 Recommended Changes to Security Principles

The domain team's review of existing security domain principles identified the need to refine existing definitions to provide for enhanced levels of security. The rationale for recommending these changes originates from the domain team's concern that exclusion of clear language explicitly stipulating shut down states and default conditions may lead to potential gaps in security controls. The recommended modifications to the *Security Control Availability* and *Security Control Default* principles are as follows:

- *Security Control Availability* reflects the addition of the new language "Controls should fail-closed to the most restrictive condition" to what is currently, "*Controls will have the capability to shut down gracefully and be restored automatically to the conditions prior to shut down*."
- *Security Control Default* incorporates the rewording of existing terminology from "*Controls will default to a lack of permission"* to domain team-recommended terminology, *"*Controls will default to the most secure condition."

Table 2, *Recommended Changes to Security Architecture Principles*, illustrates these proposed changes.

Table 2. Recommended Changes to Security Architecture Principles

Principle	Rationale
Security Control Availability: Controls will have the capability to be shut down gracefully and restored automatically to the conditions prior to shut down. Controls should fail-closed to the most restrictive condition.	Controls will be highly available to minimize periods of vulnerability.
Security Control Default: Controls will default to the most secure condition.	This approach reduces the number of points of vulnerability.

1.5.3 New Security Principle

The domain team's review revealed the absence of a principle specifically coordinating technical security controls with existing NIH security policies. For this reason the team recommends a new principle as follows:

> **Alignment with Security Policies:**
>
> Security policies should drive the implementation of technical security controls.

The rationale for this principle is:

> Technical security controls are put in place to enforce compliance with existing Security Policies. Technical security controls should not be put in place for the sake of technical controls.

The domain team submits that the adoption of this principle will further enhance adherence and compliance with NIH security principles while minimizing the risk of

adopting controls that provide little or no additional advantage to the overall security of the NIH security architecture.

1.6 Benefits

The Security Domain Team identified benefits of how NIH, its partners, and the public will benefit from adopting and adhering to the architecture principles, standards and guidelines put forth in this report. These benefits relate specifically to the sub domain of secure email:

- Provides an alternative approach to secure email communications with external users *when PKI-based S/MIME is not practical or currently operational*
- Provides common standards to be employed across the NIH while accounting for various external user configurations
- Provides an approach to communicate securely with a broad range of external NIH partners and non-affiliates who require recurring, or low volume, secure communication and are not PKI-based S/MIME capable.

2.0 Secure Email Pattern

A pattern is a logical model of technology — a design idea that can be reused and leveraged across the enterprise. It is a blueprint that identifies components at a design or logical level (for example, a data server or an application server), and shows the roles, interactions, and relationships of components at that level[3].

The following section details the Security Domain Team's recommended secure email pattern (non-PKI-based).

2.1 Pattern 1: Secure Email Middleman

2.1.1 Description

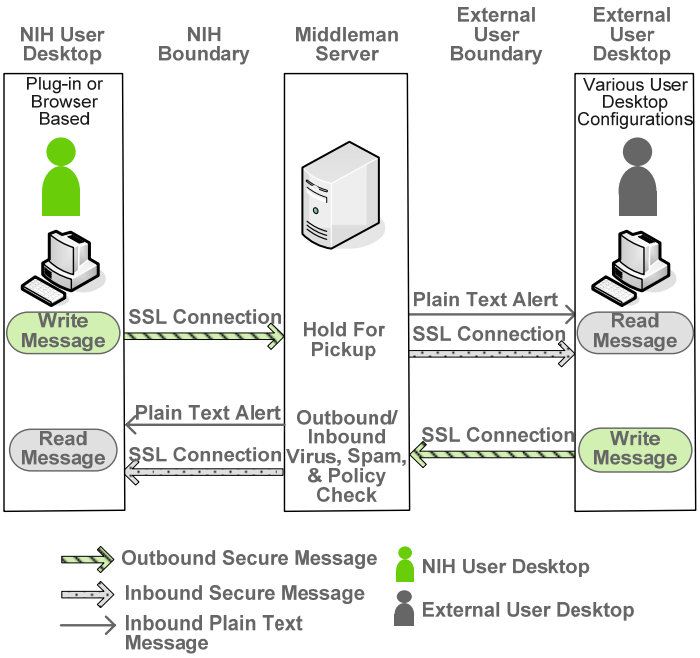
This pattern depicts an alternative method for NIH and external users to exchange secure emails that are received and read by external users *when PKI-based S/MIME is not practical or currently operational*.

2.1.2 Secure Email Middleman Solution

The Secure Email Middleman Solution provides NIH users and external users with the capability to send a secure email communication and/or attachment that is received and read by a recipient who is inside or outside the NIH infrastructure. The pattern facilitates the identification and adoption of non-PKI based technologies and solutions to secure email communications prior to transmitting across a network and receipt at recipient locations. *It is not intended to replace current PKI-based S/MIME technology, but rather provide an alternative approach when PKI-based S/MIME is not practical or currently operational*.

[3] From "Patterns and Bricks are an Architect's Two Best Friends," J. Shulman, Gartner, Inc., 5 Jan. 2004.

Figure 2. Secure Email Middleman Pattern



The Secure Email Middleman Solution identifies a logical and functional amalgamation of various secure email architectures. The pattern relates two flows defined as (1) NIH user message origination and receipt by an external user, and (2) external user message origination and receipt by a NIH user. Outbound and inbound virus, spam and policy checks occur at the middleman server location; although, this does not limit additional capabilities at the NIH or External User boundary.

The Secure Email Middleman Pattern consists of the following core components:

- **NIH User Desktop** (i.e., the NIH User) – resides inside the NIH boundary and writes and reads secure email messages The desktop can either employ a plug-in or be browser-based. Outbound messages are secured inside the NIH boundary and transmitted via plain text to the email gateway server. Assignment of secure or encryption status occurs at the gateway server as appropriate. The secure message is then transmitted to a middleman server, which is outside of the NIH boundary, for relay to an External User recipient. Inbound message alerts are communicated via Plain Text Alert and delivered by secure SSL connection.
- **NIH Boundary** - the point from the NIH User Desktop through NIH's IT infrastructure. This pattern intentionally does not define a single point where the NIH infrastructure ends in order to allow flexibility in potential solutions. NIH will maintain control over all activities and messages remaining within its infrastructure. Solutions assume that email will be routed through a given product's email gateway server where a "secure" transmission decision occurs.

- **Middleman Server** - the environment where the message is no longer exposed to unauthorized parties during transmission. This boundary is applicable to both inbound and outbound messages. The middleman server provides the means to establish trust between NIH users and external users, minimize burden to both parties, and facilitate final delivery of secure messages. External users will login to a staging web server to retrieve their secure email via Secure Sockets Layer (SSL).
- **External User Boundary** - the point from the External User Desktop through the External user's IT infrastructure. Depending on the disposition of the external user (i.e., partner, non-affiliate or other), NIH may or may not control or be familiar with aspects of the external user environment. The middleman server located between the NIH Boundary and External User Boundary implies no direct contact between the two parties.
- **External User Desktop** – resides inside the External User boundary and writes and reads secure email messages. In contrast to the NIH User Desktop, the NIH does not have control over the External User Desktop environment. Consequently, the External User Desktop can have various configurations. Regardless of configuration, and to ensure trust, outbound messages are secured and transmitted via SSL connection to the middleman server for relay to an NIH recipient. Inbound message alerts are communicated via plain text alert and securely delivered by an SSL Connection.

  Various methods exist for external users to subscribe to the middleman server. This will occur when an external user "registers" with the middleman server (service provider). They can register either when they receive an encrypted message from an NIH user for the first time, or when they initiate an encrypted transmission to an NIH user for the first time.

2.1.3 Benefits

The Secure Email Middleman Solution pattern provides the following benefits:

- Enables secure communications with external users where PKI-based S/MIME is not practical or currently operational
- Provides common standards to be employed across the NIH while accounting for various external user configurations
- Provides capabilities for NIH personnel to send a secure email communication and/or attachment that is received and read by a recipient who resides inside or outside the NIH infrastructure
- Provides capabilities for outside personnel (i.e., partners and non-affiliates) to send a secure email communication and/or attachment that is received and read by a recipient who is inside the NIH infrastructure
- Provides scalability benefits for NIH and external users
- Minimizes usability impact on NIH and external users
- Minimizes cost impact to NIH and external users

- Provides for browser-based and plug-in solutions
- Provides vendor support for both NIH and external users
- Maximizes support to internal and external end users
- Minimizes effort and burden on both internal and external users
- Provides flexibility to co-exist with current government PKI based S/MIME solutions and requirements
- Provides flexibility to adopt future government standards and requirements regarding information security
- Provides the NIH with capabilities to manage NIH users
- Provides effective policy enforcement, authentication and identify management via a third party for hosted solutions
- Provides for auditing capabilities by establishing trust credentials between senders and recipients
- Provides NIH with the ability to continue security activities at the server level, i.e. external attacks originating via email (e.g., spam, virus detection, spoofing, etc.)

2.1.4 Limitations

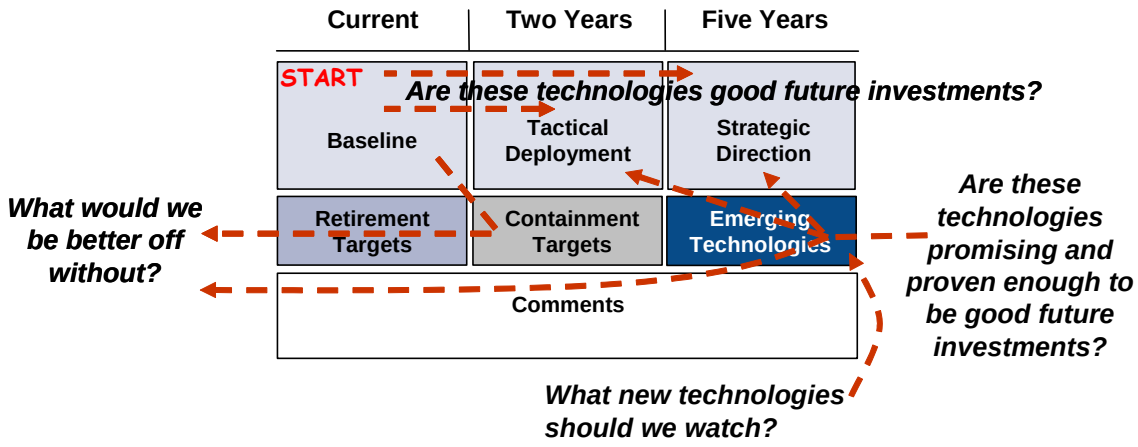
The limitations of the Secure Email Middleman Solution pattern are:

- Does not explicitly identify gateway email server requirements inherent to current industry secure email solutions
- Does not elaborate on secure email initiation or reply only capabilities at the external user's desktop, (i.e. the external user can compose a new message, or is restricted to reply-only capabilities based on communication from an NIH user)
- Is susceptible to early technological obsolescence because secure email technology solutions will continue to evolve during NIH adoption timeframes and will require ongoing monitoring against the pattern

3.0 Secure Email Brick

Technical Bricks are a tool that documents and communicates NIH's out-going, current, planned, and future (2 – 5 year horizon potential) technology standards. As such, they depict both the current (as-is) and future (to-be) states of NIH's technical environment. A single brick represents a very specific component of NIH's technology architecture. The following diagram depicts a technical brick.

Figure 3. The Technical Brick



Bricks represent the physical building blocks of the technical architecture upon which NIH IT solutions are developed and deployed -- both hardware and software. They describe both the baseline and target technologies for the components identified in design patterns. Bricks provide device-specificity for the patterns, specifying the technology to be used in the architecture. Bricks capture:

- A description of the technology and its role.
- Specific implications, dependencies, and deployment and management strategies.
- The maturity of the specific piece of technology. Maturity is monitored as follows:
  - *Baseline*: Technology or process element(s) currently in use at NIH.
  - *Tactical*: Technologies that are to be used in the near or tactical time frames (next two years). Currently available products needed to meet existing needs are identified here.
  - *Strategic*: Technologies that provide strategic advantage and are to be used in the future. Anticipated marketplace products are usually identified here.
  - *Retirement*: Technology and/or process elements that are targeted for divestment over the architecture planning horizon (five years).
  - *Containment*: Technology and/or process elements targeted for limited (maintenance or current commitment) investment during the architecture planning horizon. Items placed in containment require a waiver prior to implementation.

- *Emerging*: Technology and/or process elements to be evaluated for future integration into the target architecture based on technology availability and business need (key for evergreening).

3.1 Brick Development Methodology

The Security Domain Team developed and followed a structured methodology for evaluating potential technical standards and proposing NIH's current and future direction for these standards (as documented in the Secure Email brick, Section 3.2). This methodology included the following components:

- An assessment, which was based on a survey sent to all ICs, of NIH's baseline environment. The intent of this assessment was to understand the breadth of secure email technologies which NIH currently uses or has experience. This baseline assessment also indicated the extent to which specific products or standards represent de facto standards.
- A market assessment of the maturity, trends, capabilities, and availability of products and solutions for the secure email (email encryption) sub-domain. This assessment was supported by both independent industry research and a formal Request For Information (RFI) that the domain team released during a two-week period beginning October 7, 2005 and ending October 21, 2005. *Appendix A* presents the RFI.
- An evaluation of potential products or solutions based on a set of weighted decision criteria. Using these weighted decision criteria, the domain team "scored" potential standards based on what it learned from the baseline, market assessment and responses to the RFI. It is important to note that *decisions were not made from resulting "scores", but rather were considered as decision support information only*. Table 3, *Secure Email Decision Criteria*, presents the decision criteria that the domain team developed and their relative weighting as low, medium or high.

Table 3. Secure Email Decision Criteria

Criteria	Definition	Weighting
Existing NIH Installed-Base	NIH's experience with the technology and the use and adoption of the standard throughout NIH ICs.	Low
Fit With Existing NIH and Other Standards, Technologies and Systems	Known interoperability issues that a potential standard may have with existing technology standards such as compatibility.	Medium
Maintainability/Supportability	Effort and specialized skill sets required to support a technology standard.	Medium
Cost	Cost Estimate - Total cost of ownership given NIH adoption of the standard.	Medium
Strategic Value	Subjective - Breadth of solution's capabilities in order to leverage an investment.	Medium
Flexibility	Breadth of applicability to multiple stakeholder classes.	Medium
Security	Ability and/or effectiveness of the potential technology standard with the NIH security environment	Medium
Vendor Viability	Health of solution vendor in terms of stability, projected longevity, and likelihood of future existence to support the solution and later versions.	Medium

Industrial Installed Base	Use and adoption of standard throughout industry in general (commercial and public).	Medium
Product Lifecycle	Expected time solution will be in use and supported by the vendor.	Medium
Availability	Availability, failover and performance of the secure email technology as it relates to server uptime, client uptime and network uptime.	Medium
Level of Assurance	Ability of solution to confirm individual's identity.	High
Burden	IT requirements, user registration and cost on non-affiliated individual should impose no more than a minimal burden.	High

As a result of its analysis, the domain team developed the following brick:

- Secure Email

3.2 Brick 1: Secure Email

Description.
Method of establishing trust and securing email communications and attachments exchanged between NIH and external users.

The technology elements documented in the Secure Email brick provide for the following:

- An alternative method of secure email communication where a PKI-based S/MIME solution is not practical (i.e., imposes an undue technical complexity or cost burden on an external partner)
- The capability to establish trust between internal and external senders and recipients
- The capability for an NIH user to send a secure email communication and/or attachment that is received and read by a recipient who is inside or outside the NIH infrastructure
- The capability for an external user to send a secure email communication and/or attachment that is received and read by a recipient who resides inside the NIH infrastructure
- The minimization of operational impact and cost on NIH and external users

Table 4. Secure Email Brick

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic (2-5 year)
	■ Sigaba ■ Tumbleweed	■ Sigaba ■ Tumbleweed
Retirement (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
		■ Certified Mail ■ Oasis Web Service Standards
Comments		
■ There is no existing baseline to handle NIH external non-affiliate requirements. ■ Technologies and vendors identified in the brick are not a replacement for PKI-based S/MIME technology; rather, these are considered to be alternatives when S/MIME is not practical. ■ The secure email (email encryption) market is currently in a nascent state with multiple solutions. Research-based analysis indicates secure email (email encryption) technologies will continue to advance and reach mainstream adoption in the next 2 to 5 years. ■ NIH should continue to track developments in alternative architecture patterns as well as hybrid models with the ability to enhance current email encryption and secure exchange solutions for inbound and outbound partner and non-affiliate exchange. ■ Tactical and strategic deployments must ensure that licensing arrangements provide for unlimited external users at no additional cost to NIH. ■ Vendor licensing levels are established by internal user, internal user and plug-in, or Central Processing Unit (CPU). ■ Deployments must limit cost burden on NIH external partners and non-affiliates. ■ The current solution provides for external user login to a staging web server to retrieve secure email by SSL. Tumbleweed and Sigaba have an option of sending a password protected secure email directly to the desktop of previously registered external users. ■ Solutions that currently provide “reply only” capabilities for external users may require NIH to register those users on the product’s server (i.e.. external users who need to originate secure email communications with internal users may cause NIH to incur licensing costs and administrative burden). ■ Oasis Web Service Standards include Security Assertion Markup Language (SAML). SAML may provide enhanced features or capabilities for secure email communication.		

4.0 Gap Analysis

The domain team identified gaps in capabilities provided by vendors in the secure email technology segment. Gaps are attributable to incomplete and varied solution offerings and vendor reliance on PKI-type solutions[4]. The domain team’s analysis and research indicates that within 2-5 years, secure email offerings will realize mainstream adoption; as a result, the domain team identified the following gaps associated with information included in the brick:

- Secure email vendors provide solutions that may not fully align with the Secure Email pattern at this time. Although individual vendors may vary in their technical

[4] However, as vendors in this market enhance their product offerings (either through product development or consolidation) industry analysts expect this capability gap to close.

and architectural approaches, the pattern represents an NIH strategic architecture perspective with expected market movement towards fully compliant solutions in the tactical and strategic timeframes.

- Although Certified Mail provides the capability for an external user to originate and send a secure email to an internal user, the vendor reported that the product is not normally deployed in this manner. For this reason, and because the product provides additional capabilities of interest to NIH, the domain team determines it warrants continued monitoring (hence its position in the Emerging category).
- Technology segment vendors rely predominantly on PKI solutions in lieu of other technologies. As a result, non-PKI-based solutions are immature in the market place today.
- Industry standards and solutions do not fully account for secure email solutions that address the need to communicate with non-affiliated external users.
- Non-PKI-based desktop-to-desktop solutions[5] do exist that are capable of establishing trust between sender and recipient. However, they do not minimize cost and burden to NIH and external users.
- Secure email technology and vendor solution capabilities continue to evolve. Technologies such as SAML and Identity-Based Encryption are emerging technologies, and their potential to provide an adequate solution remains unclear at this time.
- Vendor solutions do not provide NIH with the ability to ensure information security after a secure email communication resides at an external user desktop. External user email communication of sensitive NIH information to a third party remains an area of concern.
- NIH must consider costs associated with licensing, subscription and hosted service agreements. Licensing arrangements must be extensible and allow unlimited external users at no additional cost.

4.1 Recommendations

Due to the relatively immature state of the market, the Domain Team recommends continued tracking of technology developments in the secure email technology segment related to each gap identified in Section 4.0, *Gap Analysis*. It recommends that NIH reconvene the domain team by June, 2007 to review and document trends for enhanced capabilities in the desktop-to-desktop solution, develop additional patterns, or update the current pattern and brick as appropriate.

- Desktop-to-Desktop solutions with non-S/MIME capable external users remains a "would like to have" capability for the NIH; however, the industry does not currently offer NIH-desired capabilities to ensure full authentication or trust establishment. Nevertheless, due to government-wide adoption of HSPD-12, PKI-based S/MIME remains a viable alternative for secure email within NIH and between NIH and other Federal agencies. Furthermore, the increasing adoption of PKI in the education and healthcare segments will expand the option for NIH

[5] As opposed to a middleman solution.

to use its PKI-based email solution to securely communicate with external partners.

- Customer needs will drive the evolution of secure email technology and solution capabilities. Market requirements may lead to “break through” advances in secure email technologies; however, at the time of this report publication, the Security Domain Team did not identify any explicit trends in this area. Solutions continue to center around existing technologies and methodologies with minor differences between leading vendors.

- NIH should monitor market developments in the future as vendors attempt to develop new hybrid solutions beyond current architecture offerings.

- The domain team’s scope of analysis did not address the continued security of sensitive NIH information after the email message has left the NIH’’s boundaries of control (e.g., an external user forwarding an NIH-originated email to another external user without exercising appropriate levels of security controls. The domain team recommends further investigation into solutions that mitigate this risk. This aspect of information security is a logical extension to the scope of this report, and technology developments should be tracked through periodic domain team review.

- Adoption of solutions within the pattern and brick proposed in this report require particular attention be paid to cost issues associated with licensing, subscription and hosting agreements. In particular, vendors offer threshold levels up to which NIH may incur individual user licensing costs for both internal and external users. The Domain Team recommends that all agreements contain extensible licenses such that unlimited external users can be added at no additional cost to NIH.

Change History / Document Revisions

Date	Change Author	Change Authority	Change Event	Resulting Version
December 1, 2005	Gartner, Inc.		Original Production	1.0

Appendix A — Request For Information

Appendix A — Email Encryption RFI

RFI Title: Email Encryption RFI
Release Date: 10/7/200
Response Due Date: 10/21/2005, 4 PM EST

REQUEST FOR INFORMATION
NATIONAL INSTITUTES OF HEALTH

Issuing Institute or Center: Office of the Chief IT Architect

This Request for Information (RFI) is for information and planning purposes only and shall not be construed as either a solicitation or obligation on the part of the National Institutes of Health (NIH), its Institutes or Centers. The purpose of this RFI is to help the NIH understand the market availability, technical characteristics, and functionality of solutions, tools, or products capable of satisfying the technical, functional, and/or operational characteristics described in this RFI. NIH will use this market research information in its evaluation of potential technical standards to be included in its enterprise technical architecture.

NIH welcomes comments from all interested parties on each or all questions contained in this RFI. NIH does not intend to award a contract on the basis of responses nor otherwise pay for the preparation of any information submitted or NIH's use of such information. Acknowledgment of receipt of responses will not be made, nor will respondents be notified of NIH's evaluation of the information received.

Description of Objective
NIH seeks information on available technologies to handle the exchange of confidential information and provide a secure electronic communication correspondence method to exchange information with individuals outside the NIH with minimal or no cost to them.

Description of Environment
Electronic communications may be initiated by NIH staff, external partners, or non-affiliated parties[6]. NIH's relationship with external parties may be limited to a single, one-time secure correspondence or consist of multiple secure correspondences over an extended period of time. NIH will have limited influence over the external party's IT operating environment (i.e., it can not mandate a specific operating system or email client). High importance will reside on establishing certification and authentication, i.e. trust between the external recipient/sender and internal NIH recipients/senders. Technologies of interest to the NIH are capable of the following:

1. Establishing level(s) of identity assurance between internal and external senders and internal and external recipients;

2. Encrypting NIH originated correspondence that can be received, decrypted and read by a recipient who is outside the NIH environment;

3. Encrypting external NIH partners or other non-affiliated party correspondence that can be received, decrypted and read by internal NIH recipients; and

6 External partners and non-affiliated parties can include, but are not limited to, universities, doctors, researchers, research subjects, etc.

4. Meeting all applicable government regulations while providing a cost effective, low impact, easy to use solution for internal and external users.

Description of Evaluation Criteria:

In order to support its evaluation and selection of enterprise-wide technical standards for email encryption technologies, the NIH seeks information on available technologies (i.e., internal software solutions and/or commercially hosted services for enabling the exchange of secure, encrypted email communications between NIH staff and external parties).

For the purpose of this RFI, the NIH defines the scope of this technical domain as encryption and exchange of secure communication between NIH staff and external parties, i.e. external partners and non-affiliated individuals. The information gathered through this market research, combined with information gathered through other research and analysis methodologies, will provide the NIH with important decision support information in its evaluation. NIH will base the selection of its technical standards on the following evaluation criteria:

- Availability – the availability, failover and performance of the technology as it relates to server uptime, client uptime and network uptime.
- Burden – IT requirements, user registration and cost on the non-affiliated individual should impose no more than a minimal burden.
- Cost – estimated total cost of ownership (based on market research statistics and independent research opinions).
- Existing NIH and HHS installed base – NIH and HHS experience with the technology and the use and adoption of the standard throughout NIH and HHS.
- Fit with existing NIH and other standards, technologies, and systems[7] – any known interoperability issues a potential standard may have with existing technology standards.
- Flexibility – the breadth of the standard's applicability to multiple NIH stakeholder classes.
- Industrial installed base – the use and adoption of the standard throughout industry in general (both commercial and public enterprises).
- Level of Assurance – Evaluates the ability of the solution to confirm an individual's identity.
- Maintainability/supportability – the effort and specialized skill sets required to support a technology standard.
- Product Life cycle – the expected time the product will be in use and supported by the vendor and the ability to maintain currency of its functionality and operation. A longer life cycle is desirable from a training and hardware investment perspectives.
- Security – the ability and/or effectiveness and fit of the technology within the NIH security environment.
- Strategic value – the breadth of product capabilities in order to leverage an investment.
- Vendor viability[8] – the health of the product vendor in terms of its stability, projected longevity, and likelihood it will exist in the future to support the product and later versions of the product.

[7] For information about existing technologies at NIH, please refer to the NIH Enterprise Architecture website at http://enterprisearchitecture.nih.gov.

[8] Vendor viability will be determined by its financial health, position in the market place, external research sources, and any market factors that could compromise the vendor's existence.

It is important to reiterate that this RFI is not intended to gather information needed to address each of the decision criteria above. *Received data will be combined with information gathered through other research and analysis methodologies to support NIH's overall evaluation*.

Request for Information:

To support the NIH's market research, the NIH requests responses to the following questions. Please limit your response to no more than 20 pages in MS Word format and submit prior to the due date indicated above.

General Information

1) Please provide the following:
   - Your organization's name
   - Your organization's address
   - Your organization's website
   - Contact Name
   - Contact Telephone
   - Contact Email address
   - Number of employees in your organization
   - Your organization's current and gross revenue for 2004
   - Are the products you are considering included in the GSA Schedule? Or available on another GWAC such as NITAAC?

Product Information

2) Please identify any product(s) or solution(s) you believe address the requirements for email encryption and exchange of confidential information. For each product/solution you identify, please provide the following information as available/applicable:
   - Product/solution name
   - Date of product's first production release (v1.0, no beta versions)
   - Current production version
   - Planned product schedule (i.e. future product enhancements, upgrade cycle of the product, Next major release plan)
   - Please discuss its features, functionality, and capabilities
     - Revenue based on product sales
     - Number of customers, by private and public sectors, using the version of the product being considered in this RFI

3) Please discuss how your product(s) or solution(s) satisfy the evaluation criteria described under *Description of Evaluation Criteria*.

4) Do you currently have any products, solutions, or implementations at NIH or HHS? If so, to what extent (e.g., which Institutes or Centers? How many?).

5) Please indicate the depth and breadth of this product's (these products') usage throughout industry in general (i.e., private and public sectors)? How many customers (by private and public sectors) are using this product? In what industries? Please provide an overview of current or planned product and service partnerships for this market.

Costs and Fees Structure

6) Pricing and implementation.
   - Provide an overview of the costs and fee structure associated with your solution offerings for a very large-scale federal solution.
   - Please explain your pricing model(s) and its handling of users internal to NIH (i.e., license-based, unit based, usage – full to limited, etc.)
   - Please explain your pricing model(s) and its handling of users external to NIH (i.e., license-based, unit based, usage – full to limited, etc.) Provide any training and/or certification program fees
   - Provide any documentation fees and media type

Services

7) Provide an overview of your service capabilities for the secure email market.

8) Provide an overview of NIH required resources and effort to meet implementation needs and/or describe your relationship with any 3rd party implementation partners if applicable.

9) Address product support services for NIH, external partners and non-affiliated individuals, i.e. help desk, security support, maintenance, etc.

10) Describe training methods (e.g., web-based, computer-based training (CBT), in-class, etc.) available with your product for both end-users and system and security administrators.

Technical

11) Provide an overview of your solution's architecture and technology components. Please align your approach to one or more of the architectures listed below (see glossary for clarification).
   - Desktop-to-Desktop
   - Boundary-to-Boundary
   - Staged Pair
   - Staged Boundary
   - Staging Server
   - Hybrid or Other

12) Describe all solution options (in-house & outsourcing solutions).

13) Describe platforms supported by your solution.

14) Describe web-servers supported by your solution.

15) Describe application servers supported by your solution.

16) Describe database servers supported by your solution.

17) Describe your solution's minimum desktop requirements.

18) Describe operating systems supported by your solution.

19) Provide an overview of how your solution leverages current industry best practices or future trends as these relate to email encryption architecture and technologies?

20) What trust, certification and authentication models does your solution support? Please describe in detail as appropriate, e.g. PKI, SSL, PGP, S/MIME, IBE, etc.

21) Does your solution support the use of SAML assertions from trusted third party credential providers in accordance with the Federal E-Authentication initiative?

22) Describe encryption technology sources employed as part of your solution, i.e. proprietary, open source, partnerships, industry standards, etc.

23) What encryption models does your solution support? Specifically address symmetric and asymmetric encryption as well as cryptographic algorithms providing the foundation of your solution.

24) Does your solution support list servers and Outlook Group lists? If so, explain how.

25) What applications integrate with your product?

26) Does your solution require or support any third party systems. If so, please describe.

27) Provide a brief overview of additional solution features not addressed in the preceding questions.

Implementation

28) What is the typical timeframe for IOC and FOC at a large government client such as NIH? Please provide information on your completed implementations at comparable government agencies or implementations in the commercial or non-profit sectors.

29) Explain your implementation and/or integration process for NIH staff, partner and non-affiliated parties?

30) Explain your implementation, integration and/or support process for Kiosk, PDA, Blackberry, and other common devices with capability to conduct electronic correspondence.

Regulatory Compliance

31) To what extent are you limited to conduct business under the Buy American Act with the Federal Government?

32) How does your solution comply with government/industry standards, legislative and regulatory requirements including, but not limited to the following: OMB MO404, FISMA, Health Insurance Portability and Accountability Act (HIPAA) of 1996 and Privacy Act of 1974?

33) Is your product Common Criteria, FIPS etc certified?

34) Is your product Section 508 compliant/accessible? Cite your 508 policy and provide information on testing and verification.

General

35) Describe how both internal and external users "use" the system. What activities/requirements must a first time user undertake/fulfill? What is the first time user experience like, setup etc? Describe the user experience after first time use.

36) Describe additional functionality supported by your solution, i.e. anti-virus, anti-spam, email security rules, web-based secure email, etc.

37) How do you address security vulnerabilities? Please describe the process how your company mitigates against security vulnerabilities?

38) Address your capability to provide solution capabilities across geographical regions, i.e. North America, South America, Asia, Europe, Australia, etc. (user may reside outside of the United States)

NIH welcomes responses from all individuals and organizations on each or all of these questions. Responses are due by 4 p.m. EST on Friday, October 21. Responses will not be accepted after this time.

Glossary

External Party	Any entity or individual who resides outside the NIH network and will send secure communication to or receive secure communication from NIH.
Full Operating Capability	Point at which the application is fully production operational both in terms of functionality and scope of users. NIH defines Full Operating Capability (FOC) to include external parties, i.e. partners and non-affiliated parties.
Initial Operating Capability	The point at which the application is operational at less than full functionality or below final end user levels. Additional functionality or user groups will be added to bring the application to FOC.
Desktop-to-Desktop	Correspondence encryption occurs at sender's device and decryption occurs at receiver's device.
Boundary-to-Boundary	Correspondence encryption occurs at sender's boundary and decryption occurs at the receiver's boundary.
Staged Pair	Correspondence encryption occurs at sender's desktop with transmittal to a middleman server. Certification/authentication against receiver's key occurs at middleman server. Final decryption occurs at the recipient's desktop.
Staged Boundary	Correspondence encryption occurs at sender's boundary with transmittal to a middleman server. Correspondence undergoes decryption/re-encryption at a middleman server with the receiver obtaining a plain text alert and encrypted correspondence transmission to receiver's desktop. Transmission from the middleman server and receiver's desktop is via SSL.

Staging Server	Correspondence sent through SSL connection to middleman server where it is held for pick-up. A plain text alert notifies the recipient via a plain text message and message is read at the desktop through a SSL connection.
Hybrid	Architecture framework does not fully align with industry definitions or contains aspects of multiple frameworks identified in the RFI. Frameworks specifically identified include desktop-to-desktop, boundary-to-boundary, staged pair, staged boundary and staging server.

Appendix B —Glossary of Terms

Appendix B — Glossary of Terms

Term	Definition
Asymmetric Encryption	Encryption method using two keys. One key encrypts the message and a second key decrypts the message. Commonly known as public-key encryption.
Baseline Environment	Brick space used to identify technologies and/or process element(s) currently in use at the NIH.
Boundary-to-Boundary	A secure email architecture where (1) email encryption occurs at the sender's boundary at a gateway email server, and (2) the message is transmitted directly to the recipient boundary, (3) decryption occurs at the recipient boundary, and (4) the message is read at the recipient's desktop. The architecture provides for a virus, spam and policy at the boundary point. This architecture does not employ a middleman server.
Brick	NIH technical standards that specify products, technologies, or protocols in use or planned, as well as those earmarked to be retired or contained.
Containment	Brick space used to identify technology and/or process elements that are targeted for limited (maintenance or current commitment) investment.
Decision Criteria	Thirteen evaluation criteria vetted and assigned decision weighting by the Security Domain Team. Decision Criteria provided the domain team with guidance when evaluating RFI responses, technologies and solutions proposed by vendors.
Desktop-to-Desktop	A secure email architecture where (1) email encryption occurs on the sender's desktop, and (2) the message is transmitted directly to and decrypted directly on the receiver's desktop. The desktop-to-desktop architecture does not employ middleman servers nor does it commonly provide for virus, spam and policy enforcement. In generally accepted parlance, this architecture is also known as End-to-End.
Email Gateway Server	A node on a network that serves as an entrance to another network. The email gateway server routes outbound traffic from a NIH user desktop to the outside network(i.e., Internet). The email gateway server will determine message disposition and the security/encryption requirements.
Emerging	Brick space used to identify technology and/or process elements that are to be evaluated for future use based on technology availability and business need. These technologies may not be new to the marketplace, but are simply not yet in use at NIH. In this case, the products may be a fit for emerging needs at NIH.
External User	Any user who resides outside the NIH security boundary. External users may be a user residing at a trusted partner or a non-affiliated user. The NIH does control external user desktops or environments in which they operate; consequently, external user desktop configuration and operating environments will vary.
Hybrid Solution	Domain team terminology defined to encompass email encryption solutions that fall outside of, or incorporate, aspects of five current industry architecture standards: Desktop-to-Desktop, Boundary-to-Boundary, Staged Pair, Staged Boundary, and Staging Server. The domain team incorporated the hybrid concept into its RFI to solicit identification of potential new technologies, architectures, etc.
Hype Cycle	Gartner proprietary research that analyzes a particular technology segment and places individual technologies within the segment into maturity categories including: Technology Trigger, Peak of Inflated Expectations, Trough of Disillusionment, Slope of Enlightenment, and Plateau of Productivity. Each technology is also assigned a timeframe before it reaches the Plateau of Productivity, i.e. the period before a technology is widely accepted and effectively performs the functions identified during the Technology Trigger and Peak of Inflated Expectations.
IBE	Identity-Based Encryption uses a public-key encryption methodology where the public key is arbitrary, e.g. an email address.
Middleman Pattern	Amalgamation of the Staged Pair, Staged Boundary, and Staging Server standard architectures. Domain team analysis and research determined this pattern will effectively depict staged capabilities necessary for the NIH to engage in secure email communication with external users without restricting the NIH to a single technology.

Term	Definition
NIH User	Any user who resides within the NIH security boundary and is subject to NIH security policies. The NIH user will require secure email communication capabilities to meet regulatory requirements for interaction with external users.
Non-affiliated User	Any user who resides outside the NIH security boundary. The non-affiliated user is a subset of external users. A non-affiliated user can be either an individual user at an NIH partner or have no previously established relationship with the NIH. In the scope of this report, non-affiliated users are considered to be those individuals with no or limited prior interaction with the NIH, i.e. authentication and trust issues exist. Generally, non-affiliated users will have one-off or lower volumes of secure communication.
Partner	Any user or user organization having an established and trusted relationship with the NIH. The partner is a subset of external users. A partner will have a higher volume of secure email with the NIH and generally, but not always, have established trust and authentication credentials.
Pattern	Logical models of technology or design ideas that can be reused and leveraged across NIH.
PGP	Pretty Good Privacy is a common means to protect messages transmitted via the Internet. Based on the public-key method, PGP uses two keys (1) public key disseminate to anyone from whom you will receive messages, and (2) personal private key used to decrypt received messages.
PKI	Public Key Infrastructure is a system of digital certificates, Certificate Authorities, and other registration authorities that establish trust credentials between parties participant to an Internet transaction. In the scope of this report, the Internet transaction is a secure exchange of an email message and/or attachment.
Retirement	Brick space used to identify technology and/or process elements targeted for de-investment during the architecture planning horizon (five years).
SAML	Security Assertion Markup Language is an XML-based framework that ensures secure communications through exchange authentication, authorization, non-repudiation, and single sign-on capabilities for Web services. SAML sits above the Secure Sockets Layer and strengthens SSL security.
S/MIME	Multipurpose Internet Mail Extensions is a specification for formatting non-ASCII messages thereby enabling transmission over the Internet. Email clients supporting MIME can send and receive graphics, audio, and video. Secure Multipurpose Internet Mail Extensions supports encryption of messages and is based on the RSA public-key encryption technology. RSA is the standard for industrial strength encryption.
SSL	Secure Sockets Layer is a protocol used to transmit sensitive messages/data in a secure state via the Internet. SSL employs cryptographic system with two keys to encrypt data (1) public key, and (2) private key (recipient key). SSL is denoted by establishing a secure connection between a client and a server over which data can be securely transmitted.
Staged Boundary	A secure email architecture where email encryption occurs (1) at the sender's boundary, (2) the message is sent to a middleman server where it is decrypted using a Service Provider key, (3) a plain text message is sent to the recipient notifying them of a waiting message, and (4) the encrypted email is delivered via SSL connection.
Staged Pair	A secure email architecture where email encryption occurs at the sender's desktop, the message is sent to and is decrypted at a middleman server via the Internet Service providers key, the message is re-encrypted and sent to the recipient's desktop where it is decrypted using the recipient's key.
Staging Server	A secure email architecture where (1) the sender transmits the email message via SSL connection to a middleman server where it is held for pick-up, (2) the recipient receives a plain text notification that they have a message, and (3) the recipient follows instructions to retrieve the message via SSL connection.
Strategic	Brick space used to identify technologies that provide strategic advantage and might be used in the future. Usually, marketplace leaders are identified here, as they are likely to provide better benefits and meet the anticipated needs of the business.
Symmetric Encryption	Form of encryption where the same key is used to encrypt and decrypt a communication.

Term	Definition
Tactical	Brick space used to identify (1) technologies that are recommended for use in the near or tactical time frames (next two years), and (2). currently available products needed to meet existing needs.
Trough of Disillusionment	Maturity level on the Gartner Hype Cycle between Peak of Inflated Expectations and Slope of Enlightenment. Technologies in this maturity category experience decreasing visibility and customer experiences do not meet with earlier expectations. Eventually the technology will bottom out in the Trough of Disillusionment and begin to gain steady acceptance in the market place.

Client Contact Information

Helen M Schmitz
Acting Chief IT Architect
Telephone: +1 (301) 496-2328
Email: schmitzh@mail.nih.gov

Gartner (Contractor Support) Contact Information

Stanley D. Maoury, Jr.
Gartner Consulting
Telephone: +1 (703) 226 4767
Facsimile: +1 (703) 226 4702
Email: stanley.maoury@gartner.com