Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Encryption Procurement: Setting a Standard

Copyright SANS Institute
Author Retains Full Rights

SANS ANALYST PROGRAM

Sponsored by Utimaco

Encryption Procurement: Setting a Standard

A SANS whitepaper

Written by: Stephen Northcutt and Barbara Filkins

Best Practices

Enterprise Encryption RFP How-To

Request for Proposal (RFP) / Request for Information (RFI) Checklist for Vendor Overview / Selection

Executive Summary

How can an organization balance its encryption needs against the cost and complexity of an enterprise solution? The complexity, stemming from an expanded mobile workforce, greater exposure of essential systems to adverse and catastrophic events, and increasing regulatory compliance, demands an approach to information security that protects the confidentiality, integrity, and availability of data both in motion and at rest. Data encryption is a key element in modern enterprise security strategies to protect data. Large, complex organizations need an effective and flexible solution that supports enterprise privacy and security policies, provides strong encryption at the user and device level, allows centralized management and recovery, and takes into consideration the uncompromising forces of lower budget/costs, demands to achieve ROI, and increasing security risks.

One approach is a competitive bid process designed to select the best solution for the organization. Key to this process is a well-constructed request for proposal (RFP) that requires vendors to match their solutions, products, and services against well-defined enterprise goals, objectives, requirements, and best practices.

To help the security community transition from a piecemeal approach to encryption, SANS has provided this whitepaper and RFP checklist to help you and your organization develop an RFP for enterprise encryption. This paper addresses two main topics:

- **Best practices for encryption procurement** – What needs to be considered to reach an enterprise encryption solution? Which best practices should be addressed? This section summarizes the checklist, which provides specific requirements that a vendor must meet with their solution, product, and services.
- **Enterprise Encryption RFP Step-by-Step** – What needs to be considered in the competitive bid process in order to select a vendor that will deliver the best solution? This section summarizes how to use the RFP checklist as part of a competitive bid. Keep in mind that this is only a summary. The actual process can be more involved depending on the size and complexity of your organization.

Enterprise solutions for encryption must meet overall objectives of seamless integration, ease of use, adequate performance, effective cost, and manageability as well as the functional and technical requirements. Your winning vendor should provide a realistic project plan, schedule, and budget that you can use as the basis for including data encryption into the security architecture of your enterprise. Ideally, your RFP process will result in a successful, long-term relationship between the winning vendor and your organization.

Best Practices

First and foremost, establish the requirements. Decide on what is 'required' (i.e., mandatory) versus 'desired' (nice to have but not essential). If a key length of 256 bits is mandatory, a product limited to 128 obviously does not meet the requirement and should not be considered, even if all desired requirements for the administrative interface are met. This is a timely and costly process, and should be reserved for when you're ready to make your final choice.

Due Diligence

As you assess each vendor's response to your requirements, you must validate that a product really works, integrates, scales and protects as stated, and that maintenance and support services perform as advertised. This means contacting customer references, whose installations should be of similar size, scope, and complexity as those of your organization. Let a vendor know that, if you are familiar with another company using its product, your organization reserves the right to contact that company directly without the vendor's permission. Validate a vendor's products and claims through independent research. 'Google' the vendor and its products. Peruse the literature of product support groups. Request reports from Gartner or Forrester – best to get these from the vendor who should have copies. Consult Dun and Bradstreet, Hoovers, or Edgar for information regarding a vendor's business and overall stability. As a final step, consider asking your top vendors for a field trial of their product, which includes testing in your environment.

Requirements

Make sure your requirements completely address the functionality and features your organization needs. (The SANS RFP checklist can help here!) Require encryption algorithms that are robust, meet applicable standards, and have been tested. Ensure that the product can be used to enforce encryption-dependent policies that apply to your employees, business associates, and customers.

The solution must be able to provide strong encryption support to your users without hindering their productivity or use of essential applications. Inevitably, a user will either bypass a security control or find a less secure workaround if the security control imposes a burden, is cumbersome to use, or slows down the performance of user's workstation or other device.

Compatibility

The solution should integrate well with your current infrastructure and be compatible with any constraints imposed by your environment. What systems does it support? A product that only supports Linux clients clearly does not meet the needs of an enterprise that has both Linux- and Windows-based clients. Ask for examples of how a product behaves under circumstances similar to your critical scenarios. Ask a vendor reference for a description of what a user will encounter when his laptop, configured with the product, wakes up from hibernation. Do you require that the encryption product integrate with your enterprise Microsoft Active Directory (AD)? Ask the vendor how the product will integrate with AD to allow your business units to directly manage their keys and devices without imposing on your overworked IT staff. (And consider having the vendor demonstrate this integration during the field trial of their product….)

Clearly specify all versions of software, including operating systems, applications, and utilities, with which the product must be both forward and backward compatible. You do not want to be unpleasantly surprised if the vendor's production release for Windows Vista comes six months after your planned internal deployment of Vista.

Provide a complete description of all software products and hardware platforms, including any integrated devices, so that the vendor can identify any known conflicts. The vendor should describe how the implementation will meet all your performance requirements for redundancy, reliability, response, and usability.

Stability, Scalability and Evolution

Unless you're prepared to accept the risk of alpha-testing what should be the vendor's production version, you need a stable platform. A 'stable' product will apply encryption transparently to the user, not affect performance of the device, and provide graceful termination and/recovery (along with understandable error messages) if a problem does occur. An 'unstable' product will exponentially increase the calls to your helpdesk as users encounter poor device performance, frequent crashes, and possible loss of data (to name a few symptoms).

Ask for proof that the product scales -- customer references and case studies should include installations of similar size, scope, and complexity to those of your organization.

Do not rely on a vendor's 'future plans' to meet your current requirements. Remember – you are looking for an enterprise solution that can evolve with your needs. Your initial deployment may be for workstation and laptop encryption but you may plan on expanding to smart phones or removable media over the next year. You do not want to pay for that option in the first 12 months if you don't use it, but you do want the functionality when you need it.

Manageability

You need a product that can provide flexible solutions at the user and device level but be managed centrally. The vendor should fully describe the standard management processes for an environment that has a varying number of users and a variety of operating systems, applications, and end-user devices. If your enterprise has a systems or network management framework, you may want to require the selected product to integrate with that framework. Have the vendor describe how the product integrates with your enterprise backup and recovery tools, both for user devices and for administrative servers.

Good key management is at the heart of an enterprise security solution. The key management has to be compatible with existing IT infrastructures and must work with a wide range of deployment scenarios.

The capability to determine organizational compliance with regulatory or corporate standards is essential. Ask the vendor to describe how their audit / reporting functionality meets regulations or policies with which your organization must comply, the data collected (and the ability to customize that collection), and how the audit data itself is securely managed, controlled, and archived. You need to know how the information is reported so that management can easily review and act on critical events.

Maintainability

Understand how the software will be deployed and maintained. Does the process for installing and updating a large number of clients (say 10,000 plus) require extensive administrative effort? Is changing the client configuration disruptive to the end user? What degree of configuration changes to your infrastructure (e.g., firewall and server settings) are required to manage (e.g., install, update, receive log files) client devices on the network?

Viability

Your organization will be making a substantial investment in the vendor and their encryption product, so it's important to understand their business and have a feeling for their background and track record. Will the vendor remain viable? Ask for their size, customer base, financial standing and any relevant industry ratings. Run a Dun and Bradstreet report or check Edgar on-line if the company is publicly held. Ask for their annual report. Request that they provide an audited financial statement for at least the past three years.

Is their product mature? Request the number and frequency of major releases and size of the customer base. Are they active in the industry? Ask who their solution partners are, their perception of market direction, and how both affect their technology roadmap.

Service and Support

Evaluate which services you need from the vendor. Training for end-users and system administrations is an obvious requirement, but how and where the training is conducted may require special services to be procured. Understand the maintenance terms of the maintenance agreement, how product releases are distributed, and what the notification/alert process is if a vulnerability associated with the product is uncovered. At some point, you may need to acquire non-standard professional services from the vendor. Ask about customization services, to ensure that their customization of the product does not invalidate your maintenance agreement.

Pricing

Product pricing, representative of the solution detail, is one of the most critical pieces of the vendor's response to your RFP: The vendor must provide a price for the total proposed solution based on the information you provide in the RFP. Price is not only a factor in vendor selection; it will also be used to accurately determine the actual budget for your planned deployment. Ensure that the vendor identifies its pricing/licensing model for enterprise solutions, including any discounting tiers and limitations. Make sure that the vendor provides the detailed bill of materials proposed for your enterprise and corresponding prices, indicating which items are a one-time charge (initial software and hardware purchase), which are recurring (annual maintenance and support), and which are special services (on-site support, end-user training, customization).

Enterprise Encryption RFP How-To

The SANS checklist has been developed to reflect best practice considerations. Its successful use depends on several steps described below.

1. **Plan your project.** A well-run competitive bid is like any other project. It requires a budget, a project plan, and a schedule. In requesting resources, make sure you support your business case to management by showing that their investment of limited funds for vendor diligence will significantly reduce the risk of selecting the wrong vendor, that a field trial of the product costing a few thousand dollars in employee labor will far outweigh the prospect of discovering the product does not work as expected after award.

2. **Focus your RFP.** SANS has provided a generic statement that seeks to convey the essence of the procurement. You and your management need to review this statement and revise it as needed. It should clearly state your goals and objectives for this procurement and could be considered a basis against which all responses will be evaluated. It could also be used to prove to regulators your due diligence in meeting requirements, and push liability to vendors who don't meet their own claims.

3. **Describe your organization.** Characterize your environment as accurately as possible, including the level of detail needed to allow a bidder to provide a realistic solution and price quote. A simple description of the number of servers and number of workstations may suffice. Conversely, if you require the vendor to seamlessly integrate with your enterprise environment, a more detailed description of your physical and logical network is probably in order. Details can include type of business, office location(s), number of users, and your network topology, including:

   a. Administration concept (central vs. decentralized)

   b. Deployment mechanism

   c. Maintenance/upgrade procedures

   d. Number and types of workstations, servers, and mobile devices

   e. Applications

   f. A description of the data you need to protect. (Consult with executive management and/or your legal counsel if you need to provide organization -sensitive information, such as IP address and access point information, to a bidder.)

4. **State your requirements.** Document the detailed requirements an enterprise encryption solution must meet – features and functionality, integration requirements, management and administration needs, reporting and audit needs, and (perhaps most critical) how the solution will impact your business processes and users. Use the SANS RFP checklist as a basis for your requirements, but don't limit yourself to using it exactly. You may want to expand on some of these items. Conversely, you may want to restate or even remove items so as not to limit vendors that might reply. Review each requirement to determine whether it is 'required' (i.e., mandatory) or 'desired." Note: In this RFP checklist, 'desired' DOES NOT mean the same as 'optional' since a configuration option can be a 'mandatory' requirement.)

5. **Decide on an organizational point of contact.** This is the person who is responsible for interfacing with all the bidders. Depending on the nature of your enterprise, you may need to restrict access by the vendor during the competitive process to a single person, not necessarily someone directly involved in IT.

6. **Prepare RFP package and instructions for the vendor response.** Ensure that instructions to bidders are clear. The SANS checklist has areas highlighted in GOLD where you plug in your own information, and update as needed. Make sure that the format for the vendor proposal ensures consistency across all bidder responses and allows for fair evaluation of each proposal against a consistent set of criteria. Evaluation criteria may include how well the solution meets enterprise goals, objectives, and requirements, what the overall and detailed prices are, and an assessment of vendor stability.

7. **Conduct a competitive bid process.** Publish an RFP that allows each bidder to present his recommended solution. The goal is to select the best-priced and best-featured solution under highly competitive conditions.

8. **Award.** Use the winner's response to develop your overall budget and timeline to increase the resilience of the enterprise security architecture.

Request for Proposal (RFP) / Request for Information (RFI) Checklist for Vendor Overview / Selection

Version 5.0 • May 15, 2007

General information

Our organization,

insert name of organization seeking the encryption solution (or "Organization")

seeks an encryption solution that can provide uniform standards for the entire enterprise. We seek a security solution that combines the advantages of "best-of-breed" technology with the benefits of an integrated, scalable, and manageable solution. We wish to avoid the difficultly faced by many enterprises that must manage multiple point-security type products and the resulting drain on management resources. Our goal is to acquire and implement a robust enterprise solution, flexible enough to support individual user and device needs yet allow effective and efficient centralized administration, management, and recovery.

Organization Description

The following section describes our organization so you, the vendor, can get a feel for our deployment scenario and use this information to establish as basis for your response to Section 5.0, Pricing and Components.

Insert brief description of "Organization", including type of business, geographic placement of offices, high-level network topology, number and type of workstations, number and types of servers, number of users, and any other information that may be relevant to the vendor.]

Contact information

Provide contract information for the RFP.

Vendor Response

Please complete the following sections according to the instructions in each section. ***Review requirements, tailor or update areas indicated in GOLD, and determine whether requirement is "required" (i.e., mandatory) or "desired". Note: In this RFP checklist, 'desired' DOES NOT mean the same as 'optional' since a configuration option can be a 'mandatory' requirement.)***

1.0 BUSINESS / BACKGROUND REQUIREMENTS

1.1 Describe your customer base. Provide a list of customers including company name, industry, and number of licenses. Note: If you can't list the company name, just list the industry.

1.2 Enterprise security solutions cannot work in isolation. They have to be compatible with a broad range of industry leading solutions as demonstrated by technology partnerships. Provide a list of your solution partners.

1.3 How many full-time employees do you employ? Describe.

1.4 How many of those full-time employees are dedicated to desktop encryption? Describe.

1.5 How many major releases have there been of your product (maturity)? Describe.

1.6 What is your company's Gartner Rating? Describe.

1.7 What is your company's financial standing? Explain / provide information.

1.8 What is your perception of market direction and how does this affect your technology roadmap? Describe your anticipation of industry / customer trends, how your product plans will meet these trends, and your approach to ensure that your solution can adapt and improve while continuing to provide value to an existing customer base.

2.0 PROFESSIONAL SERVICES

In order to meet implementation objectives, our organization may require specific services from you for the services listed below. In developing your costs in Section 4.0, please consider the following information: ***Tailor this list to meet the needs of "Organization" seeking the encryption solution, including number of users in each category and training delivery method (e.g., on-line, instructor-led)***

- Training for _____ end-users
  insert number of
- Training for _____ system administrators
  insert number of
- Certification program for _____ designated staff
  insert number of
- Implementation services
- Update services
- Specify level needed for support services
- Customization
  Specify details if known

2.1 Training: Describe end-user / administrator training courses / options you offer.

2.2 Security certifications: Provide a list of any security certifications you offer or support that are related to your product. List third parties, if any, that are authorized to administer the certification.

2.3 Implementation: Describe your offerings for supporting the initial configuration and installation of your product including:

2.3.1 If applicable, provide a list of third parties (e.g., consultants, service providers) that you have certified to provide implementation services on your behalf,

2.4 Maintenance/update services: Describe your offerings including:

2.4.1 What services are included in your software maintenance/update program?

2.4.2 What is your normal revision cycle for standard releases?

2.4.3 What is the normal distribution path for standard releases? Is it the same path for emergency releases/hot fixes?

2.4.4 What is the normal documentation provided with your standard releases? (Provide example(s).)

2.4.5 What is your notification process to clients in the case of hot fixes or emergency releases?

2.4.6 How quickly are bug fixes generated or released from the time that the problem or issue is initially reported or discovered?

2.5 Support services: Describe your offerings including:

2.5.1 What services are included in your support service program?

2.5.2 Is there a knowledge base accessible to end-users? To system administrators?

2.5.3 What are the various levels of standard service that you provide in terms of category of users supported, response time, and hours of availability (i.e., Platinum Support means two-hour response to all users, 24x7x365)?

2.5.4 Is on-site support available? Provide the terms as outlined in your standard agreement.

3.0 SOLUTION ARCHITECTURE / OVERVIEW

Provide a comprehensive overview of your product and how it can meet our specific requirements as provided in Section 4.0 and addressing the specific concerns for each area as outlined below.

3.1 Functionality and Features: Provide a summary of your product's features, addressing the specific requirements in Section 4.1, to include:

- Security and encryption
- Authentication and authorization
- Key management
- Backup and recovery
- Security administration

3.2 Product Architecture: Describe you product's overall architecture and ability to support and integrate with our current environment, addressing the specific requirements in Section 4.2, with particular emphasis on:

3.2.1 Architecture: Provide an overall of your product's structure (e.g., multiple clients supported by single server, multiple servers required, agent required on client machine). Provide specific information related to:

3.2.1.1 Minimum hardware requirements for processor, memory, and disk space

3.2.1.2 Memory / disk requirements for decryption

3.2.1.3 Impact of installed product on overall usable disk space

3.2.1.4 Management server hardware and software requirements

3.2.2 Standards: Describe the standards your product follows/supports.

3.2.3 Scalability: Discuss and show your product scales. Reference current customers/installations of similar size, scope, and complexity to our organization. Provide customer references.

3.2.4 Extensibility: Describe how your product will allow us to add functionality as needed.
Provide examples of future needs of "Organization" that will require additional functionality

3.2.5 Interoperability: Describe how your product would integrate with our environment, with specific attention to the following:

3.2.5.1 How would your product achieve common authentication for our existing infrastructure?

3.2.5.2 How will the native management tool provided by your product work with our current authentication system to allow a flexible and extensible approach that leverages our investment in our other systems?

3.2.5.3 How does your product integrate with Directory Services to reduce additional management overhead, reduce work for our staff and administrators, and allow our different units to manage their keys and devices according to their unique needs?

3.2.5.4 How does your product integrate with Windows Vista BitLocker Drive Encryption? (Note: BitLocker is the sector-based full disk encryption product included with Vista Enterprise and Ultimate Editions but not in previous Microsoft operating systems (e.g., XP). BitLocker uses the AES 128 and 256 algorithms and provides "power off protection".) In your response, please address the following, either directly or reference where the item is addressed elsewhere in your response:

- What is your partnership status with Microsoft? Explain.
- Can you centrally manage and administer BitLocker functionality? Please address the following: (i) central configuration and application of policies on BitLocker enabled devices; (ii) central management of encryption key backup and recovery on BitLocker enabled devices; (iii) single console management of BitLocker and non-BitLocker encrypted drives.
- What is your logging, reporting, and auditing capability relative to BitLocker? What specific device/drive status reports on BitLocker do you provide?
- Can you implement protection for other Microsoft operating systems you support simultaneously with BitLocker (e.g., heterogeneous operating system environment that contains both XP and Vista)?
- Do you support helpdesk challenge/response for forgotten BitLocker passwords?

3.2.6 Performance: Describe how your product can be implemented so that it meets our performance requirements for redundancy, reliability, and response.

3.2.7 Compatibility: Describe how your product is compatible with other versions of Windows, both forward and backwards compatible with Windows 9x and Vista. Describe any known conflicts with other software products contained in our environment to include products to fragment disks, partition disks, provide anti-virus, and so forth.

3.3 Management and Administration: Summarize how your product supports centralized management addressing the specific requirements in Section 4.3. In your description, address the following:

3.3.1 Identify any additional modules or applications needed for the management of your product, in addition to the basic encryption product(s)

3.3.2 Ability to integrate with third-party security or system management tools (e.g., Microsoft System Center/Forefront).
Provide list of products that "Organization" uses or plans to use

3.3.3 Flexibility and adaptability of the management products in an environment that a) has a varying number of users, b) a variety of operating systems, and c) a variety of management options (e.g., fixed devices, mobile devices, email, file sharing) and variety of end-user devices

3.4 Reporting, Auditing, and Compliance: Summarize how your product meets our auditing and reporting requirements, addressing the specific requirements in Section 4.4, highlighting any features of your product that can enhance our ability to meet our needs in these areas. In your description, address the following:

3.4.1 Integration of audit functionality with the basic product (e.g., is an additional module required?)

3.4.2 Type of data collected

3.4.3 Security management and control of audit data

3.4.4 Archiving features for audit data

3.4.5 Reporting functionality provided

3.5 Installation, Configuration, and Deployment: Describe how your product supports flexibility in installation and configuration options within our existing IT environment, addressing the specific requirements in Section 4.5. In your description, address any potential impacts to the configuration of our infrastructure, such as firewall configuration settings and server services, necessary to manage (e.g., install, update, receive log files) client devices on the network.

4.0 Specific Product Requirements

For each requirement in Section 4.0, please provide a concise explanation of how your proposed solution will meet the specific requirement, including any additional detail requested in the requirement paragraph (e.g., requirement paragraph 4.2.1.18.

4.1 Functionality and Features

4.1.1 SECURITY AND ENCRYPTION

The security of the data is of prime importance. Data encryption is a very effective method of ensuring data security. It is important to use tried and tested, robust security algorithms. The solution must provide the following:

	Required	Desired
4.1.1.1 Secure state-of-the-art encryption algorithms to include:		
4.1.1.1.1 Choice of standardized, tested, public algorithms		
4.1.1.1.2 Option for 128/256 encryption key lengths		
4.1.1.1.3 FIPS compliance (US customers only) per http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf		
4.1.1.2 Protection available in all states of the device: off, on, standby, hibernate, online, offline.		
4.1.1.3 Defense against attacks during all stages of the boot process.		
4.1.1.4 Ability to withstand attacks using alternate boot media.		
4.1.1.5 Ability to configure forced encryption on entire removable media, including pre-existing data. Note: Re-formatting of devices to meet this criterion is acceptable although not preferred.		
4.1.1.6 Ability for removable media to be encrypted by one user and read by other authorized user(s). Note: Feature to be used for team collaboration in enterprise environments.		
4.1.1.7 Protection of files from intrusion while machine is running.		

4.1.2 AUTHENTICATION AND AUTHORIZATION

Because organizations have become more porous with fuzzier boundaries separating the inside from the outside, traditional perimeter defenses are no longer sufficient. Authentication and authorization are critical elements of a comprehensive enterprise security solution. It is important to effectively enforce consistent security policies in a heterogeneous and decentralized computing environment with a variety of users including employees, business partners and customers who use many different types of end devices. A granular policy enforcement method is needed for maximum user and administrator flexibility. The solution must provide the following:

	Required	Desired
4.1.2.1 Role-based access control.		
4.1.2.2 Optional multi-user authentication for critical security actions.		
4.1.2.3 Option for 128/256 encryption key lengths.		
4.1.2.4 Authentication options include one or more of the following:		
4.1.2.4.1 Microsoft Graphical Identification and Authentication (GINA) for single sign on to the encryption system and workstation and Credential providers for Vista		
4.1.2.4.2 User ID / password		
4.1.2.4.3 Smart cards		
4.1.2.4.4 Token (USB)		
4.1.2.4.5 Biometrics		
4.1.2.4.6 TPM		
4.1.2.4.7 Kerberos		

		Required	Desired
4.1.2.5	Support for multi-factor authentication and/or token-based authentication systems to achieve higher security classification levels and/or to mitigate risks involving improper password management.		
4.1.2.6	Ability for an administrator to lock-down and/or "kill" end-user device(s) if the device(s) is (are) believed to be missing or compromised, including the capability to disable all accounts and/or delete keys necessary to decrypt the data.		
4.1.2.7	Role-based, hierarchical administrative and access control that includes:		
4.1.2.7.1	Definition of administrative and access control roles that provide different levels of access to the software and its functionality.		
4.1.2.7.2	Ability to assign specific tasks/functions to specific administrative roles.		
4.1.2.7.3	Ability to assign global administrative and access control to specific, defined set of policies and configurations.		
4.1.2.7.4	Ability to assign local administrative and access control to specific, defined set of policies and configurations.		
4.1.2.7.5	Ability to establish local administrative and access control roles that allow local-level administrators to modify local policies and configurations but restrict access to global policies and configurations.		
4.1.2.7.6	Ability to delegate limited access by local-level administrator to global policies or configurations, if required.		
4.1.2.7.7	Ability to revoke prior administrator privileges by current administrator at that level or above (e.g., no administrative lockout).		
4.1.2.8	Support external authentication mechanisms (e.g., LDAP, AD, RADIUS) for administrative authentication.		
4.1.2.9	Securely authenticate and encrypt any interface to external authentication mechanisms.		
4.1.2.10	Support mutual authentication for any external authentication mechanisms used.		
4.1.2.11	Ability to configure and enforce rules for strong passwords (e.g., no consecutive characters, include/exclude special characters, require upper and/or lower case, set minimum length).		
4.1.2.12	Single-sign on from pre-boot authentication to Windows for greater ease-of-use to include:		
4.1.2.12.1	Password synchronization so that, if the Windows password changes, the pre-boot password account is automatically updated so that the passwords remain synchronized.		

4.1.3 KEY MANAGEMENT

Good key management is at the heart of an enterprise security solution. The key management has to be compatible with existing IT infrastructures and must work with a wide range of deployment scenarios. The solution must provide:

	Required	Desired
4.1.3.1 Key server administration, utilizing central administration methodology like Public Key Infrastructure of distributing key authority to any number of servers in authority chain.		
4.1.3.2 Key recovery to include:		
4.1.3.2.1 Administrative key recovery capability		
4.1.3.2.2 Split key functionality for administrative key recovery		
4.1.3.2.3 Optional notification to end-user (or client as in workstation) of administrative key recovery		
4.1.3.2.4 Self-service mechanism for end-user to retrieve lost key, even when not connected network to retrieve lost key. Note: This is crucial for laptop and mobile PDA solutions.		
4.1.3.3 Ability to run key server database and key management interface on separate servers.		
4.1.3.4 Ability for hardware-based security modules that provide physical tamper-resistant environment for secure key storage and processing.		

4.1.4 BACKUP AND RECOVERY

Disaster recovery and business continuity are major issues for enterprises. The solution must easily facilitate recovery from a number of different failure scenarios. The solution must support:

	Required	Desired
4.1.4.1 Data recovery in case of OS failure, hardware failure (other than physical failure of the hard disk), or loss of contact with the client assigned to the device (e.g., employee termination or death).		
4.1.4.2 Provisions for the backup and recovery of the administrative database.		
4.1.4.3 Mechanism to recover forgotten passwords, online and offline.		

4.2 Product Architecture

4.2.1 PRODUCT ENVIRONMENT – GENERAL

Our organization seeks an enterprise encryption security solution that supports the general features outlined below. The solution must support:

	Required	Desired
4.2.1.1 Ability to scale to [enter number of users].		
4.2.1.2 Ability to scale in terms of management options (i.e., fixed devices, mobile devices, email security, file sharing, etc.).		
4.2.1.3 Support of modern communication standards/protocols (e.g., XML, SOAP).		
4.2.1.4 Integration with LDAP or Active Directory (Explain if product requires or performs any changes to the Active Directory structure.)		
4.2.1.5 Ability to be configured for redundancy or high availability.		
4.2.1.6 Ability to load-balance the services.		

	Required	Desired
4.2.1.7 Single solution suite that supports the following clients: *List client operating systems used by "Organization", indicating version, service packs, and so forth if relevant*		
• Windows 2000		
• Windows XP, SP2		
• Windows Vista		
• Mac OS		
• Linux		
4.2.1.8 Single solution suite that supports the following server operating systems/platforms: *List operating systems used by "Organization"*		
• Microsoft Windows 2003 (32- and 64-bit)		
• Microsoft Windows 2000		
• Unix		
• Linux		
• Novell Netware		
4.2.1.9 Single solution suite that supports the following mobile device operating systems: *List operating systems used by "Organization"*		
• Palm OS		
• Windows Mobile 5.0		
• RIM OS		
• Symbian OS		
4.2.1.10 Single solution suite that supports a variety of end-user devices to include: *Add any devices "Organization" uses*		
• Desktops		
• Laptops / notebooks		
• Tablet computers		
• PDAs		
• Digital cameras		
• Portable / smart phones		
4.2.1.11 Various disk configurations/storage architectures to include: *Add specifics for "Organization"*		
• RAID levels		
• SAN		
• NAS		

	Required	Desired
4.2.1.11 Various disk configurations/storage architectures to include: *Add specifics for "Organization"*		
• RAID levels		
• SAN		
• NAS		
4.2.1.12 Single solution suite that supports all forms of removable media, including but not limited to: *Add any specific media "Organization" uses*		
• CDs		
• DVDs		
• USB flash drives		
• External USB hard drives		
• Compact flash cards		
• SD cards		
• LS120		
• Zip drives		
• Floppy drives		
• Tapes		
4.2.1.13 Ability to support shared workstations (e.g. kiosks) where multiple users may use the same machine.		
4.2.1.14 Multiple partitions on a disk or disk volume.		
4.2.1.15 Partial encryption on both permanent and removable media for data storage flexibility. Software is configurable to allow a portion of removable media to be encrypted, while leaving some of the device unencrypted.		
4.2.1.16 Disk re-imaging.		
4.2.1.17 Digital Rights Management (DRM).		
4.2.1.18 Disk sanitization procedures in accordance with the US Department of Defense 5220.22-M Clearing and Sanitization Matrix. (Note: Explain how the product handles data remnance for both fixed hard drives and the media listed in 4.2.1.12 where 1) encryption is at the media-level and 2) encryption is at the file/folder level.)		

4.2.2 INTEGRATION WITH EXISTING IT INFRASTRUCTURE

Our enterprise would like to leverage our investment in existing infrastructure when deploying new solutions. This reduces capital costs, reduces the number of new components being installed and places less strain on our IT resources, The following requirements outline those products, standards, and protocols used in our infrastructure and with which your encryption product should integrate. The solution must support:

	Required	Desired
4.2.2.1 Compatibility with Windows client to include:		
4.2.2.1.1 Interoperability with Encrypting File System (EFS)		
4.2.2.1.2 Support for Vista including credential providers		
4.2.2.1.3 Integration with Vista BitLocker		
4.2.2.2 Compatibility with major anti-virus malware vendors to include: *Add products "Organization" uses*		
4.2.2.2.1 Symantec		
4.2.2.2.2 McAfee		
4.2.2.2.3 CA		
4.2.2.2.4 Microsoft ForeFront Client Security		
4.2.2.3 Interoperability with Patch Management solutions to include: *Add products "Organization" uses*		
4.2.2.3.1 Patchlink		
4.2.2.4 Interoperability with Desktop Management Solutions to include: *Add products "Organization" uses*		
4.2.2.4.1 Altiris		
4.2.2.4.2 Microsoft SMS		
4.2.2.5 Interoperability with imaging solutions to include: *Add products "Organization" uses*		
4.2.2.5.1 Symantec Ghost		
4.2.2.5.2 Altiris		
4.2.2.6 Integration of the native administration tools for the encryption product with provide your common authentication system to leverage existing investment in current systems.		
4.2.2.7 Additional integration support for authentication and account provisioning or integration with the following:		
4.2.2.7.1 Directory Services -- Active Directory and LDAP		
4.2.2.7.2 Directory Services – Novell NDS		
4.2.2.7.3 Backward compatible with NT domain structure		
4.2.2.7.4 PKI public key infrastructure		
4.2.2.7.5 US DoD CAC cards		
4.2.2.7.6 Shibboleth/OASIS SAML (Note: Shibboleth is a standards-based, open source middleware software which provides Web Single SignOn (SSO). It supports the OASIS SAML v1.1 specification.)		

	Required	Desired
4.2.2.8 Support for virtualization software to include: *Add products "Organization" uses*		
4.2.2.8.1 VMWare		
4.2.2.8.2 Virtual Server		
4.2.2.8.3 Virtual PC		
4.2.2.9 Interoperability with existing disk compression software		
4.2.2.10 Interoperability with shared environments to include: *Add products "Organization" uses*		
4.2.2.10.1 MS Sharepoint		
4.2.2.10.2 MS Exchange		
4.2.2.11 Integration with *insert required backup solution*.		

4.2.3 EASE OF USE, PRODUCTIVITY AND PERFORMANCE

Security is often seen as a hindrance to user productivity. It is critical for a solution to be extremely easy to use to ensure that it is used by the end-user and not bypassed by users because it is considered too cumbersome to use. The solution must:

	Required	Desired
4.2.3.1 Be easy to learn and use by end users.		
4.2.3.2 Provide easily understood system messages.		
4.2.3.3 Provide transparent encryption / decryption of data and files to the user once the disk(s) are fully encrypted (or the client is fully configured).		
4.2.3.4 Require minimum setting of configuration parameters by the end-user.		
4.2.3.5 Show no noticeable performance degradation for user applications.		
4.2.3.6 Support single sign on. (Users can authenticate with their Active Directory credentials and password synchronization occurs with no user interaction.)		
4.2.3.7 Allow remote password reset for offline end-users needing assistance,		
4.2.3.8 Allows an easy start for the initial encryption process after software is first loaded.		
4.2.3.9 Support a disk encryption process that does not take more than 20% longer than defragmenter on the same device (e.g., workstation, laptop).		

4.3 Administration and Management

4.3.1 ADMINISTRATION AND MANAGEMENT

Central management is a critical ability in an enterprise-class solution with hundreds or thousands of users. It is important to provide a consistent and effective level of security in a heterogeneous environment with various types of end-user devices (e.g., desktops, laptops, removable media, PDAs, etc.) running on differing operating systems. The solution must:

	Required	Desired
4.3.1.1 Provide effective central management for an installed base of *[insert number such as 100]* or more clients.		
4.3.1.2 Be easy to configure and/or customize for different locations and / or end-users, both locally and remotely.		
4.3.1.3 Be easy to support by both local and remote support teams including remote recovery, remote access in both locked and unlocked states.		

	Required	Desired
4.3.1.4 Securely authenticate and encrypt all communications between the management station/ application and clients.		
4.3.1.5 Provide an alert or "phone-home" capability in the event someone tries to "brute force" a device.		
4.3.1.6 Support a unified management approach for an operational environment as defined in the section titled "Organization Description" above.		
4.3.1.7 Be able to run the management server under a virtual machine (e.g., VMWare).		

4.4 Reporting, Auditing and Compliance

4.4.1 REPORTING, AUDITING AND COMPLIANCE

It is important for a security administrator to have an updated, accurate view of the security status of all the users and devices in the organization at all times. Internal and external compliance regulations mandate detailed logs and records of all the activities. The solution should provide maximum flexibility in user-defined reports, as well as deliver standard reports that allow management to easily review and act on critical data. The solution must provide:

	Required	Desired
4.4.1.1 Centralized, automated logging of current encryption state for all client devices.		
4.4.1.2 Local, secure logging of audit data on client devices.		
4.4.1.3 Ability to configure auditing to include the collection of the following types of data: authentication date and time, local decryption and encryption activity, local policy and administrative changes.		
4.4.1.4 Audit trails for end-user functions that include the following data elements: *Specify the elements needed by "Organization".*		
4.4.1.5 Audit trails for administrative functions that include the following data elements: *Specify the elements needed by "Organization".*		
4.4.1.6 Time-stamped audit trails for the following: operator entries, actions that modify or delete entries, other. *Specify any other reports/elements needed by "Organization".*		
4.4.1.7 Access control to view audit data (e.g., role based access).		
4.4.1.8 Secure storage of audit data.		
4.4.1.9 Encryption of audit logs.		
4.4.1.10 Auditing of access to audit logs (e.g., time/date of access, user name accessing data).		
4.4.1.11 Ability to archive audit logs.		
4.4.1.12 Reporting functionality. *Describe as a set of requirements what functionality is being looked for by "Organization".*		
4.4.1.13 Integrated audit capability.		
4.4.1.14 Interoperable with computer forensic solutions to include: *Specify any products used by "Organization".*		
• Guidance Software Encase Product Suite		
• Technology Pathways Product Suite		

4.5 Configuration, Installation and Deployment

4.5.1 CONFIGURATION, INSTALLATION, AND DEPLOYMENT

Installation and maintenance of the software must be simple, painless and minimally disruptive. It has to be easily deployed on a large number of clients (10,000+) with minimal administrative effort. The solution must support:

		Required	Desired
4.5.1.1	Centrally-managed, network-based, remote installation of product to a large number of devices, either using external software delivery or via the operating system native software distribution format, such as Windows' MSI format files.		
4.5.1.2	Use of automated installation scripts / installers with no interaction required by user or local administrator.		
4.5.1.3	Audit trails for administrative functions related to configuration, installation or update of the product.		
4.5.1.4	Minimal configuration changes to existing network infrastructure, such as firewall settings, for product installation and/or updates to reduce impact on the organization.		
4.5.1.5	Programmatic implementation for product updates, configuration changes, and policy changes programmatically, either from centralized demand-push or from a local configuration-pull (e.g., user requests update at workstation).		
4.5.1.6	Ability to securely manage encrypted clients by Wake-On-LAN.		
4.5.1.7	Ability to granularly restrict local configuration by end-user and/or local administrators.		
4.5.1.8	An encryption process that is resilient to unexpected lockups and/or operating system failure during the actual encryption process.		
4.5.1.9	Ability to suspend and resume the encryption process for a given disk to provide flexibility when migrating extremely large disks.		

5.0 Pricing and Components

Please provide all solution pricing for the total, proposed solution according to the information provided in this request for proposal.

5.1 Provide a catalog of all items, including hardware, software, and support services that are generally used in your solution(s), providing a description of each item and its associated list price.

5.2 Describe your pricing/licensing model for enterprise solutions, including any discount tiers. Please indicate any and all limitation to your enterprise pricing.

5.3 Describe any standard discounting that you provide, such as GSA.

5.4 Itemize all items, including hardware, software, and support services that you propose for our enterprise, providing a description of each item, its associated list price, and its discounted price, if applicable. For each item, indicate which costs are one-time and which items are recurring. Note: If you are providing more than one solution, list each solution separately according to the instructions above.

5.5 Provide prices for any additional special services, such as on-site, end-user training, customization, and certification training (if applicable) according to the information provided in Section 2.0.

5.6 Provide a total cost for each proposed solution, backed by the detail used for developing prices for 5.4 and 5.5.

About the Authors

Stephen Northcutt

Stephen Northcutt founded the GIAC certification and currently serves as President of the SANS Technology Institute, a post graduate level IT Security College (www.sans.edu). Stephen is author/coauthor of *Incident Handling Step-by-Step, Intrusion Signatures and Analysis, Inside Network Perimeter Security (2nd Edition), IT Ethics Handbook, SANS Security Essentials, SANS Security Leadership Essentials* and *Network Intrusion Detection (3rd edition)*. He was the original author of the Shadow Intrusion Detection system before accepting the position of Chief for Information Warfare at the Ballistic Missile Defense Organization. Stephen is a graduate of Mary Washington College. Before entering the field of computer security, he worked as a Navy helicopter search and rescue crewman, white water raft guide, chef, martial arts instructor, cartographer, and network designer.

Barbara Filkins

Barb Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls 'policy, process, platforms, pipes, AND people.' Most recently she has been involved with HIPAA security issues in the health and human services industry, with clients ranging from federal agencies (DoD and VA), municipalities and commercial businesses. Her interest in information security comes from the impact infosec has on all aspects of the system lifecycle as well as its relation to many of the issues – privacy, identity theft, exposure to fraud, and the legal aspects of enforcing information security – faced by modern society dependent on automation. She holds the SANS GSEC (Gold) and GCIH (Silver, working towards Gold), and the GHSC.

SANS would like to thank

utimaco®
The Data Security Company.

Last Updated: July 23rd, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS DHS Continuous Diagnostics and Mitigation Workshop with Training	Washington, DCUS	Aug 01, 2014 - Aug 08, 2014	Live Event
SANS San Antonio 2014	San Antonio, TXUS	Aug 11, 2014 - Aug 16, 2014	Live Event
Cyber Defense Summit & Training	Nashville, TNUS	Aug 13, 2014 - Aug 20, 2014	Live Event
SANS SEC401 Bootcamp @ Malaysia 2014	Kuala Lumpur, MY	Aug 18, 2014 - Aug 23, 2014	Live Event
SANS Virginia Beach 2014	Virginia Beach, VAUS	Aug 18, 2014 - Aug 29, 2014	Live Event
SANS Chicago 2014	Chicago, ILUS	Aug 24, 2014 - Aug 29, 2014	Live Event
SANS Pen Test Bangkok 2014	Bangkok, TH	Aug 25, 2014 - Aug 30, 2014	Live Event
SANS Delhi 2014	New Delhi, IN	Aug 27, 2014 - Sep 02, 2014	Live Event
SANS Tallinn 2014	Tallinn, EE	Sep 01, 2014 - Sep 06, 2014	Live Event
SANS Brisbane 2014	Brisbane, AU	Sep 01, 2014 - Sep 06, 2014	Live Event
Security Awareness Summit & Training	Dallas, TXUS	Sep 08, 2014 - Sep 17, 2014	Live Event
Retail Cyber Security Summit	Dallas, TXUS	Sep 08, 2014 - Sep 17, 2014	Live Event
SANS Crystal City 2014	Crystal City, VAUS	Sep 08, 2014 - Sep 13, 2014	Live Event
SANS Albuquerque 2014	Albuquerque, NMUS	Sep 15, 2014 - Sep 20, 2014	Live Event
SANS Bangalore 2014	Bangalore, IN	Sep 15, 2014 - Sep 27, 2014	Live Event
SANS ICS Amsterdam 2014	Amsterdam, NL	Sep 21, 2014 - Sep 27, 2014	Live Event
SANS Baltimore 2014	Baltimore, MDUS	Sep 22, 2014 - Sep 27, 2014	Live Event
SANS Seattle 2014	Seattle, WAUS	Sep 29, 2014 - Oct 06, 2014	Live Event
SANS DFIR Prague 2014	Prague, CZ	Sep 29, 2014 - Oct 11, 2014	Live Event
SANS Hong Kong 2014	Hong Kong, HK	Oct 06, 2014 - Oct 11, 2014	Live Event
SOS: SANS October Singapore 2014	Singapore, SG	Oct 07, 2014 - Oct 18, 2014	Live Event
SANS Perth	Perth, AU	Oct 13, 2014 - Oct 18, 2014	Live Event
GridSecCon 2014	San Antonio, TXUS	Oct 14, 2014 - Oct 14, 2014	Live Event
SANS Network Security 2014	Las Vegas, NVUS	Oct 19, 2014 - Oct 27, 2014	Live Event
SANS Boston 2014	OnlineMAUS	Jul 28, 2014 - Aug 02, 2014	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced