Global Information Assurance Certification Paper

Encryption Key Recovery

GSEC Certification Practical Assignment V.1.4b

By Don Leipprandt

January 23, 2004

Abstract

The purpose of using encryption technology is to ensure proper authentication, confidentiality, data integrity and non-repudiation. There are many pieces of this technology that need to be addressed to build these assurances, not only within the technology itself, but also within the management of the technology, the data or process the technology is protecting, and through proper training and education of the users and administrators of this technology. Well-defined procedures and controls must also be implemented to ensure the safety of the data you are trying to protect.

There are numerous ways to undermine the effectiveness of cryptography, the technology itself can break, the encryption algorithm could be cracked or an individual can deviate from the proper process(s). One of the ways to help protect your cryptographic processes is through the proper implementation and use of its key management system. This paper will address the purpose of encryption, encryption key recovery, the benefits and risks of key recovery, and key recovery items to consider when determining the best alternative for developing and implementing an encryption key recovery strategy. Even though key recovery does introduce additional security risk, after you have read this material I think you will agree that implementing a proper key recovery strategy will outweigh the associated risk.

Purpose of Encryption

As defined by www.techweb.com encryption is the reversible transformation of data from the original plaintext to a difficult-to-interpret format as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity.

Encryption is actually an ancient form of hiding information from those that you do not want to know the detail of it. At the same time it is necessary to educate the users of the data on what they must do to read the encrypted information. The process to read the information from its encrypted state is called decrypting. In ancient times one of the most simplified forms of encryption was to spell words using the alphabet backwards. An example of this would be anywhere in the document that you wanted to use the letter 'A' you would use the letter 'Z', the letter 'B' would be represented by the letter 'Y', 'C' would be 'X' and so on. Thus the encrypted form of the term 'Viking' would be 'Erprmt'. Today, encryption is much more sophisticated; encryption keys are formulated by using mathematical encryption algorithms.

Data, regardless of the media on which it is maintained, will always be vulnerable to exposure simply due to its existence. Public data can be allowed full exposure while non-public data needs to be protected to different degrees based upon the data classification scheme your company has implemented. An example of data classification would be: information that is classified as

'restricted' can only be seen by specific individuals within the Corporation such as Corporate Officers, another classification may be 'confidential' which could be defined as only people working in the Research and Development Department can access the information, the lowest level of classification could be 'public' which could mean that if the information were released or leaked to the public it would cause no harm to the company.

Cryptography is a useful tool to secure data from unauthorized access; however, it will also prevent authorized users from obtaining access should the encryption key not be available [3]. The encryption key is essentially the combination to the safe, appropriate and prudent care must be taken to protect the confidentiality and integrity of these keys, just as you would the combination to your safe. Not having access to the encryption key is essentially the same as losing the combination to the safe. The major difference is that you can eventually force your way into a safe, while encryption keys can be unbreakable. Thus your encrypted information could be lost forever. The philosophy of creating a backup key inherently increases the risk to the encrypted data based upon the fact that there are now multiple keys instead of only a single key. This is essentially the same as keeping the combination to your safe in multiple locations in case you forget or lose it. This is the basic premise for planning and implementing a proper and secure key management program.

As with any technology there is risk associated with its use and its non-use. The non-use risks of encryption technology are relatively clear, your data could be viewed and/or changed by someone inside or outside of your organization, potentially allowing proprietary information to be viewed by a competitor, allowing financial information to be released prior to the appropriate time, or effectively crippling any of a number of competitive advantages that have entailed years of effort. The use of encryption technology can substantially reduce risk associated with the transmission and storage of data, however it is not an end-all be-all solution and must be a component of a well architected defense-in-depth strategy [11]. The use of encryption technology presents it own set of challenges that must be addressed. The key recovery portion of the system could prove to be more complex than implementing basic encryption itself [3]. Due diligence will be necessary to ensure the key recovery process will meet the business and regulatory requirements for the encrypted data.

Encryption Key Recovery

There are several components necessary to provide a robust Encryption Key Management Service, including key ordering and distributing, how do I get a key assigned to begin encrypting my data and how does the key get to me so that I am assured no one else has copied the key; re-keying, how do I get a new key when mine expires; revoking, how does a key get revoked if it has been compromised or the person it was assigned to has a new assignment or left the company; and the focus of this paper, recovery, how is the key restored if it has

become corrupted or lost.
Information technology recovery processes have a tendency to be overlooked or intentionally bypassed because they create additional overhead in terms of the cost of supplementary hardware, software, storage, maintenance, and personnel, not to mention that it will generally add to the complexity and possibly extend the delivery time to get a new application into production.

If an encryption key is lost, corrupted or destroyed the only way to decrypt the data is through a process referred to as Key Recovery. It is of utmost importance that processes be implemented to ensure that designated encryption keys are recoverable; unless a decision was made that these keys will not be recovered under any circumstances. A back up, or identical copy of the key must be created and maintained for any encrypted information, unless you are willing to accept that this information could be lost forever should the original encryption key not work. If the original encryption key cannot be used for whatever reason the data will not be able to be decrypted if a back up key does not exist. The purpose of backing up these keys is to be able to decrypt data that would not otherwise be recoverable [7]. Some keys may not need to be recovered such as with transmitted information that could simply be resent with new keying material, such as telecommunications [7].

All the information that would be necessary to recover or verify cryptographically protected information is referred to as Key Recovery Information or Keying Material. This material includes all information that is required for the key to be functional, along with key creation time, key owner, owner of the protected data, and what conditions need to be met to recover the keying material [3]. Key recovery information may differ based upon individual key recovery techniques or the associated application [8]; this should be clearly defined in your key recovery standards documentation.

A decision will need to be made regarding if and when keying material needs to be recoverable. This decision should be determined based upon several criteria: type of key (signature, authentication, encryption), what it will be used for, who owns the key, responsibility of the party that requested or needs the recovery, will the recovered key be usable upon recovery, and the value of the encrypted data [3]. If your business leaders have made a conscious decision not to recover any encryption keys, thus there is no need for back up keys, this needs to be documented and communicated through the appropriate policy, standards and communication procedures. Keep in mind that key recovery will allow a trusted agent access to these back up keys, therefore key recovery can only be used in organizations that allow others access to these keys [5].

Benefits of Encryption Key Recovery

Key recovery is nothing new, however with the increased focus on disaster recovery capabilities since the events of September 11, 2001 it is important that key recovery be given strong consideration during the information technology disaster recovery planning, documenting and testing phases for any employee, contractor or application using encryption technology. Recovery of these keys should not be viewed as a process that is not likely to be needed, but one that will eventually be needed to some extent, either to recover a single key because the key has been lost, corrupted or inaccessible for some reason or to recover all of the keys due to a disastrous event such as a fire, tornado, hurricane, etc. It is unlikely that if your organization is encrypting all of its sensitive data and all of the encryption keys are destroyed during a natural or man-made disaster that the organization will easily recover or ever recover for that matter it they did not have back up keys. According to the Disaster Recovery Journal, of the companies that experience a disaster 43% never reopen and 29% close within two years; 1 out of 500 data centers will experience a severe disaster each year, a company that experiences a computer outage that lasts more than 10 days will never fully recover financially and 50% of those will go out of business within five years of the disaster. On the positive side of these disaster related statistics a company that is able to recover quickly and have minimum downtime and loss of data would enhance their customer reputation [10].

Although additional copies of encryption keys will inherently increase the risk to the data, multiple copies of keys can be necessary for several reasons: 1) a key is lost or corrupted, 2) the employee, or owner of the key, is unavailable (vacation, illness, termination, etc.), 3) a potentially more drastic event which triggers the business resumption/disaster recovery procedures. Keep in mind that if keys are lost, destroyed or inaccessible for whatever reason and there is no back up key, the data could potentially remain encrypted forever. Thus lost forever. Re-creation of the data can be extremely time consuming, non-productive and costly due to man-hours and/or regulatory fines. In some cases it may be impossible to recreate the data, in others it may not be useful information by the time it is finally recreated.

Risks of Encryption Key Recovery

Encryption along with proper procedures provides assurances that the data will only be viewable by authorized individuals. However, as with any security technology or process, it is only as strong as its weakest link, thus anyone that is not properly protecting his or her encryption key could prove to be the weak link in the chain. This risk increases exponentially if the weak link is an encryption backup key administrator, which could have access to all of the encryption keys across the enterprise.

A major challenge of the key recovery process is to maintain tight security controls over the encrypted data while allowing recovery of the data potentially by someone other than the original owner of the data [6]. Some keys such as private signature key, private authentication key, symmetric random number generator key, public key transport key should not be stored in an alternate location simply due to the nature of the key [3]. Backing up or archiving private signature keys and authentication keys can negate any claims of non-repudiation [6]. Storing back up signature keys will provide opportunity for others such as system administrators to access these keys. Once an opportunity by anyone else to use or access the signature key is discovered, it will disallow or strongly weaken any non-repudiation claim. Therefore these types of keys should not be backed up or copied for any reason [4]. Extreme care must be taken when determining which encryption keys are backed up and which are not. This is one reason that proper thought, planning and implementation of this technology is so important, to ensure that it works as intended.

Another risk is that the backup key(s) will be outside the control of the custodian of the original key. In some cases the back up key may be entrusted to a third party vendor, which potentially makes the trust relationship increasingly important and inherently less secure. If a third party is going to manage your keys, it is of critical importance that the contractual obligations be clearly identified to ensure the third party assumes their share of the accountability toward the management of these keys. This process must be audited on a regular basis to ensure it continues to meet the necessary security requirements. Any system that stores or transmits sensitive data must be treated with extreme care to ensure that proper controls are established and a continuing compliance effort must follow to ensure these controls do not collapse, become diluted over time due to changes or become weakened because of the discovery of new vulnerabilities.

The failure to conduct proper key recovery procedures could have a potentially devastating impact to your business in terms of the recovery process not working thus making your data irretrievable, or the security wrapped around the processes being weak and data falling into the wrong hands. Either way this means the encryption technology did not work as it was intended. It is important to understand that this technology, like all others, will work properly if managed properly. If this technology does not work as expected it could have a truly devastating impact on your business.

Considerations for Implementation

The most common reasons to conduct the key recovery process is because a user has lost their key or their key has been corrupted. Based upon an individual company's work hours and/or culture, this type of recovery could be necessary any time of day or night; therefore it may be essential to provide an

enterprise support group with the capability of recovering these keys. It is of utmost importance that clear policy, standards and procedures are developed regarding the key recovery process to mitigate the risk of a key being recovered for the wrong reason or falling into the wrong hands. If these keys are utilized for user authentication a localized procedure may need to be developed to get the employee working as quickly as possible to avoid unnecessary user downtime. Providing access to these back up keys to large groups of people, such as an enterprise information technology help center, creates additional exposure to the protection of these encryption keys and inevitably to the protected data. The people associated with the key recovery process need to be of the highest integrity. By having control over these keys they could potentially access what is probably your most sensitive data. Strict controls must be established and enforced; improper usage of this access must have an associated appropriate penalty.

From a business continuity planning perspective, the most comprehensive planning methodology is that of planning for the worst-case scenario. Your key recovery strategy should use this same viewpoint. This methodology will assist a recovery that is smaller in scope and magnitude, by implementing only the necessary portions of the overall recovery plan. If a disastrous event should occur you must have your backup keys stored off-site to ensure they are not destroyed due to the disastrous event. One of the first steps in preparing a disaster recovery plan is to prioritize critical business processes along with their associated applications and data; this methodology will help to ensure the most critical systems, applications and data are properly prioritized for recovery. This will also help to define the scope of the disaster recovery testing that should occur to validate the planning process. If any of the data used by these critical applications is encrypted, an encryption key recovery plan will need to be included in this planning effort and the encryption keys recovered accordingly. If you restore your encrypted data, but have not restored or recovered your encryption keys you will not be able to access your encrypted data.

Sensitive information is generally the most critical to the organization. Where does encryption key recovery for this data rank among recovery efforts? Does it logically fall in line with the recovery of your encrypted data? If not, your recovery strategy may need to be reviewed. As an example, it makes no sense to recover your encrypted data on day two of the recovery process, if your encryptions keys will not be recovered until day 10 of the recovery process because there would be an eight-day delay in accessing the recovered data. Some data may have different back up and recovery procedures based upon its sensitivity. These factors need to be rolled into the decision making process of the entire recovery effort. If your disaster recovery planning is already in place prior to implementing an encryption technology, your disaster recovery planning will need to be updated. If you do not update your disaster recovery plan to include the encryption key recovery, the next time the disaster recovery plan is tested you will find the encrypted data to be inaccessible. Testing your disaster

recovery plan is critical to ensure that it works as planned.

Different standards should be created and monitored based upon the category of the key. There are three different key lifecycle categories: 1) current key, defined as the key that is currently being used either for encryption or authentication purposes. The current key is the most important because it is the one that is being used for the current projects, email, etc. If this key is unavailable it could have the most immediate impact on the key owners productivity. 2) The previous key, defined as the key that was in use prior to the current key. This key should remain easily recoverable because it is the most likely one to need to be recovered to view older information. 3) Older keys are defined as any key older than the previous key. Based upon the key lifecycle these keys will vary in age and should have limited need to be recovered [4]. The lifecycle of the "Older Keys" should correlate with the lifecycle of the data the key is protecting. There is no need to maintain the back up encryption keys if the data has been disposed of. The opposite is true as well, if the encryptions key(s) have been disposed of, the encrypted data is no longer of any value.

The key recovery policy should address each of these categories, current, previous and older, separately because there should be distinct differences as to the need and requirements for recovery. A security decision will need to be made based upon the above criterion. Escalation procedures and identification of the person responsible for the key recovery decision should be pre-determined and documented. There also needs to be a well-defined key recovery request process that is strictly adhered to, easily auditable and periodically audited to ensure compliance to the policies and standards set forth. The penalty for relinquishing encryption key information outside of the standard operating procedures must be strict and equally enforced.

The overhead of using encryption technology includes the additional computer processing power to encrypt and decrypt the data, supporting more computer hardware and software, training the users and administrators, increasing cycle time by adding the encrypting and decrypting processes, and providing key administration services. New policies and standards need to be crafted to ensure that encryption is used to properly benefit the company. A solid encryption key recovery strategy, well-documented plans and procedures need to be crafted, regularly audited and tested to ensure that secure and usable back up and recovery procedures are practiced.

If critical data is encrypted with keys that are now archived it may even be prudent to store these archived keys in multiple physical locations [3]. These locations should meet the disaster recovery best practices such as distance from the data center, to ensure the encryption keys are properly protected in the case of a disaster scenario such as a fire, earthquake, hurricane, etcetera, based upon geographic location of the data center and a completed risk management analysis.

A great deal of effort will need to be completed prior to rolling out any encryption tool to the enterprise, this effort consists of creating and communicating policy and standards around this discipline, educating and training users, help desk personnel and administrators on proper use of the technology. This process must begin with a solid corporate policy. This policy should be supported and enforced through normal corporate policy program to ensure it is treated with the same vigor as other corporate policies.

This policy should include no less than the following components: [3]

1. Keying material that should be recoverable by application
2. How and where the keying material will be saved
3. Who is responsible for the keying material, this could be an individual, a department, or even a trusted vendor
4. Who can request the recovery of a key
5. What decisive factors will allow or disallow a key recovery
6. Who owns the final decision if the decisive factors are not met
7. Audit procedure for the recovery process
8. Proper handling and destruction of recovered keying material
9. Identification of anyone that should be notified of recovered keying material
10. Procedures to follow if the Key Recovery System has been compromised

Security is very important to the validity of the system. Guarding private keys requires a great deal of planning and effort. If it is possible for more than one user to have a copy of the private key, the integrity of the system must be questioned [4]. Responsibility is addressed in number 3 above, but it is extremely important to make sure accountability is addressed as well.

Once the policy has been agreed to by all of the entities that determine policy within your organization such as Human Resources, and Law & Regulation, you can begin the process of developing standards to assist your corporation in meeting the established policies. These standards need to address things such as potential encryption tools that can be used, this may consist of only one enterprise tool that will be supported; when to use cryptography and when not to use it, this could be based upon the corporate data classification scheme; proper policy and standards must be wrapped around this process to ensure that the key recovery process does not increase exposure to the encrypted data over and above the inherent exposure of creating copies of these keys.

Encrypted communication and files require information regarding the location of the encryption key; this information provides an attacker with assistance on where to focus their attention. One method of decreasing the risk this creates is to maintain a split key system by storing portions of the key in multiple locations [2]. This does add to the complexity of the recovery system, however this is true with most security solutions. Remember that security is only as strong as the

weakest link.

To limit exposure of an individual that has administrative capabilities over these keys you need to consider: [4]
The trustworthiness of the individual(s) selected to administer this recovery service.
Two factor authentication such as a smart card, something you have and something you know.
The m of n authentication scheme, which requires a subset of the total encryption key administrators to authenticate to the system before it can be enabled, or keys accessed, this will reduce the threat of a single individual being able to recover a key or keys for the wrong reason(s).

Trustworthiness, accountability and audit controls are key elements in addressing the need of security assurances around the proper use of any process or technology. The selection of trustworthy employees to handle this role is only one step in the course of appropriately securing a key management system. Segregation of duties, as indicated in the m of n authentication scheme listed above helps to enhance the security around many processes by reducing the opportunity and temptation of a single employee to use the system in a non-trustworthy manner. The sensitivity involved in encryption key recovery certainly deserves strong consideration for a segregation of duties methodology. The individuals selected to support this function need to completely understand the importance of the role, the accountability of the role and the disciplinary action that will occur in the event of a security violation. A third party, such as an internal or external auditor, should also review the processes on a regular basis to ensure compliance to policy and standards.

Conclusion

This paper has addresses many of the benefits and risks associated with encryption technology, with an emphasis on key recovery. The decision to use or not use key recovery could be critical to the success of your business since it would likely be your most critical and/or sensitive data that would be encrypted. If these encryption keys not are usable for whatever reason you could potentially have your competitive advantage severely weakened or destroyed, be subject to legal and regulatory ramifications, and/or go out of business. Obviously, key recovery is not a decision that should be taken lightly. It is important to note that this is a business leadership decision and not one that can or should be made by the information technology leadership. This is a decision that has to be made by the leader(s) of the business unit that would be impacted by the loss of unencrypted data that slipped into the wrong hands. If the decision is made to encrypt the data, then a major portion of this risk transfers to the Information Technology area, which will need to ensure that the proper encryption tools are selected, the technology is correctly implemented and managed, and the appropriate controls are in place to safeguard this data.

Glossary [4]

Authentication – The action of verifying information such as identity, ownership, or authorization.

Cryptography – The art and science of using mathematics to secure information and create a high degree of trust in the electronic realm

Encryption – The transformation of plaintext into an apparently less readable form (called ciphertext) through a mathematical process. The ciphertext may be read by anyone who has the key that decrypts (undoes the encryption) the ciphertext.

Encryption Algorithm – The mathematical formula used to encrypt information.

Non-repudiation – The inability to deny actions.

Two-factor authentication – A form of authentication that requires two distinct items to ensure user authenticity. An example is something you have and something you know such as a bank issued ATM card, something you have is the card and something you know is the personal identification number (PIN).

List of References

1 – National Institute of Standards and Technology, “Key Management Guideline, Part 2: Best Practices for Key Management Organization”, URL: http://csrc.nist.gov/CryptoToolkit/kms/guideline-2-Jan03.pdf

2 – Center for Democracy and Technology, “The Risks of Key Recovery, Key Escrow, & Trusted Third Party Encryption”, URL: http://www.cdt.org/crypto/risks98/

3 - National Institute of Standards and Technology, “Special Publication 800-57, Recommendation for Key Management Part 1: General Guideline”, URL: http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf

4 – Nash, Andrew, Duane, William, Joseph, Celia, and Brink, Derek, PKI Implementing and Managing E-Security. Berkley, CA: Osborne/ McGraw –Hill, 2001. Pages 147-154.

5 – Planning for Data Recovery and Key Recovery, Microsoft, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dssch_pki_ugye.asp

6 – RSA Keon, Key Recovery Module, “The Importance of PKI Key Recovery”, URL: http://www.rsasecurity.com/products/keon/whitepapers/kca/IPKR_WP_0702.pdf#xml=http://www.rsasecurity.com/programs/texis.exe/webinator/search/xml.txt?query=key+recovery&pr=default&order=r&cq=&id=3fdd86ba50

7 - National Institute of Standards and Technology, “Key Management Guideline, Workshop Document, November 1-2, 2001” URL: http://www.csrc.nist.gov/CryptoToolkit/kms/key-management-guideline-(workshop).pdf

8 – National Institute of Standards and Technology, Key Management Guidelines, URL: http://csrc.nist.gov/CryptoToolkit/kms/guideline%20overview%20notes%20(b-w).pdf

10 – Disaster Recovery Journal, Volume 13, issue 2, spring 2000, URL: http://www.drj.com/articles/spring00/1302-05.html, (user name and password can be located in the contents of any paper copy of the Disaster Recovery Journal)

11 – SANS Security Essentials Course Material