79

Cryptographic Transitions

Ralph Spencer Poore

Change is inevitable. As businesses adopted commercial cryptography as an important tool in protecting information, they transitioned from either reliance solely on physical security measures or, more often, reliance on no intentional protection to either a proprietary cryptographic process (e.g., PGP) or the, then newly established, federal cryptographic standard: Data Encryption Standard (DES). Cryptography, however, always includes a balancing of efficient use with effective security. This means that cryptographic techniques that provide computational efficiency sufficient to permit operational use in a commercial setting will degrade in security effectiveness as computational power increases (a corollary to Moore's Law). Cryptographic protocols and algorithms may also fall prey to advances in mathematics and cryptanalysis. Specific implementations believed secure when originally deployed may fail because of technological obsoleses of hardware or software components on which they depended. New technologies may permit previously infeasible attacks. Regardless of the specific reason, organizations will find it necessary to transition from one cryptographic security solution to another at some point in their existence.

Cryptographic transitions is the process by which an organization addresses the problems associated with updating (or initially implementing) cryptographic security measures in response to changes in the environment that require better information security. This chapter addresses a myriad of environmental changes that might motivate a cryptographic transition, including both technological and business events. It will then describe a process for such transitions.

79.1 Technological Obsolescence

Cryptographic implementations become technologically obsolete either when aspects of the cryptography itself cease to provide the appropriate levels of assurance or when the technology (e.g., hardware or software) on which it is based becomes obsolete.

Advanced cryptanalytic capabilities and faster computers have made the Data Encryption Algorithm (also known as the Data Encryption Standard—DES) obsolete. DES has long outlived its effectiveness

AU7495—Chapter79—25/1/2007—20:49—PARTHIBAN—14739—XML MODEL CRC12a – pp. 1029–1037.

except, perhaps, as Triple DES. Although cryptographic advances have produced the Advanced Encryption Standard (AES) that provides better security and higher efficiency than Triple DES when equivalent implementations (i.e., hardware versus hardware or software versus software) are compared, very little of the business infrastructure that previously depended on DES has successfully converted to AES. This occurs despite the many intervening years since published reports widely proclaimed the death of DES.[1]

What information security professionals can do to minimize the potential adverse impact to within their respective organizations will be further discussed throughout this chapter. The following are suggestions that may help information security professionals minimize these impacts:

1. Information security professionals should carefully research potential products. If a good body of experience for a given product cannot be found (vendor marketing material aside), then the business will be better served by letting someone else risk its assets. For example, businesses that jumped on wireless LANs discovered that they were providing free services to unintended parties and opening their LANs to attack outside of their physical control. Where cryptography was an option, they failed to implement it. But even when they learned to implement it, the available protocol was not secure. A transition from 802.11b to 802.11g, although apparently more secure and less subject to interference, was also more expensive and had a shorter range, requiring more units. Early adopters of the 802.11b wireless technology found themselves with equipment that needed years on their books for depreciation but that was, nonetheless, obsolete.

   The irony of bleeding edge technology that depends on security functionality for its business case can be seen. The advantages boasted in marketing material for adoption of the new technology (e.g., efficiency, cost savings) evaporate when the buyer must add to the equation fraud losses, down time, and premature forced replacement of the equipment. A further irony remains: the replacement technology may suffer the same fate as the technology it replaced.
2. Information security professionals should assess the business and legal risks. From the time the industry is officially on notice that an encryption method, protocol, or implementation no longer provides the necessary level of protection until the time an enterprise actually adopts an effective[2] alternative, the enterprise is increasingly at risk of litigation for negligence because it continued to rely on the faulty technology when it knew (or should have known) that it was unsafe. This aggravates the situation by increasing the pressure on the enterprise to buy a replacement product that may prematurely come to market without the benefit of rigorous vetting. To avoid this becoming a vicious circle, balance the risks of the exposures with the costs associated with a transition to the new product. Compensating controls in the existing environment (for example, the use of encryption at a higher level in the ISO stack) may be more cost effective.
3. A cryptographic lifecycle plan should be designed, and appropriate procedures in existing software development and acquisition processes should be integrated.

79.2 Cryptographic Lifecycle

The lifecycle for cryptographic security products is much like the lifecycle for humans. In cryptography, an end happens when an easily exploitable flaw is found in the algorithm, and the underlying cryptosystem is deemed beyond repair. For example, the Fast Data Encipherment Algorithm (FEAL), developed by the Nippon Telephone and Telegraph with the intent that it be an improvement to DES, was found susceptible to a variety of cryptanalytic attacks, some requiring as few as twelve chosen plaintexts, that prematurely ended its life.

[1] See, for example, Ben Rothke's article "DES is Dead! Long Live ????" published in the Spring 1998 edition of the Information Systems Security by which time, this was the general consensus.

[2] At least one currently perceived as effective.

Effectiveness is gradually lost, often a victim of Moore's Law or cumulative breakthroughs in cryptanalysis' drastically reducing the time necessary to ascertain the cryptographic key (or the message directly without the key). Some cryptosystems will have very short lives, and others may span centuries. Predicting the life of any given cryptographic security product, however, is probably about the same as reading a person's lifeline on his or her palm.

A cryptographic system contains many elements with all remaining secure if the overall system is to remain cryptographically effective. If a backdoor to the algorithm is discovered or a cryptanalytic attack efficiently reduces the key space against which a brute-force attack succeeds, the algorithm no longer provides adequate cryptographic strength. If the protocol associated with key management or registration fails to withstand an attack, then the cryptosystem is likely compromised. If the source of random values, e.g., a pseudo-random number generator (PRNG)—also more accurately called a deterministic random number generator (DRNG), is discovered to have a predictable pattern or to generate values within a space significantly smaller than the target key space, a cryptanalyst may exploit this weakness to the detriment of the cryptosystem. In recent years, researchers have found that timing, power consumption, error states, failure modes, and storage utilization all may act as covert channels, leaking information that may permit the solving of the implemented cryptosystem without benefit of the keys.

In addition to the potential for failures related to the cryptographic algorithm, cryptographic security implementations depend on other factors. These factors vary depending on the cryptographic services intended for use. For example, to use cryptography for user authentication, a means of binding an identity with a certificate is necessary. This requires a registration process where an identity is asserted, it is authenticated in some manner, and a cryptographically signed piece of data to represent that identity is created. Weaknesses in the registration process, the signing process, the revocation process, or the chain of trust on which the resulting certificate relies are all potentially exploitable. A National Institute of Standards and Technology (NIST) Special Publication addresses this complex area and its impact to the cryptographic key lifecycle. NIST Special Publication 800-57[3] provides guidance on over a dozen different kinds of cryptographic keys (e.g., Private Signature Key, Public Signature Key, Symmetric Authentication Key, Private Authentication Key, Public Authentication Key, Symmetric Data Encryption Key, Symmetric Key Wrapping Key, Symmetric and Asymmetric Random Number Generator Key, Symmetric Master Key, Private Key Transport Key, Public Key Transport Key, Symmetric Key Agreement Key, Private Static Key Agreement Key, Public Static Key Agreement Key, Private Ephemeral Key Agreement Key, Public Ephemeral Key Agreement Key, Symmetric Authorization Key, Private Authorization Key, and Public Authorization Key). With the many differences in the application of cryptography come differences in the overall cryptographic lifecycle of the products used. Products that encrypt a message, send it, receive it, and decrypt it serve their cryptographic purpose in almost real time. Products that encrypt for archival or sign contracts that must be capable of authentication a decade later will have much longer cryptographic lifecycles.

The services supported by encryption, e.g., confidentiality, authentication, and nonrepudiation, have nearly perpetual lives. Business functions that require such services almost never cease to require them. Nonetheless, a given implementation of these services will have a planned lifecycle associated with the business functions that rely on these services. Secrets rarely require perpetual protection. For most trade secrets, three years of confidentiality might provide sufficient protection for the business to profit from its advantage. Of course, robust cryptographic security measures may have a shelf life far in excess of three years. Selecting the cryptosystem and key length deemed safe for the length of time that management believes is appropriate for a given business function is more art than science. In many applications, however, little difference in acquisition and implementation costs for cryptosystems using are found (for example, 128 bits of active key and 512 bits of active key). But changing from a system based on 128 bits to one of 512 bits might be costly. Here is one place where planning and foresight gives

[3]For a copy of this special publication, refer to http://csrc.nist.gov/publications/nistpubs/

the information security professional an opportunity to control at least some of the cryptographic security product lifecycle parameters.

The speed at which new implementations of cryptographic protocols issue from RFC and proprietary development efforts leaves implementers in the dust. Vetting (i.e., formally testing and proving) an implementation requires time and great skill. The great commercial pressure to bring new products to market rarely admits to the necessity for such vetting. The wireless protocol 802.11b was a good example. Implementations were in the field before the protocol weaknesses were fully understood. The tools for freely exploiting its weaknesses were available well before a newer, more secure standard. The new standard, 802.11g, was not compatible with the equipment already in the field. Manufacturers had to productize this standard before companies could acquire the new devices. For the purchasers of the previous technology, nothing short of replacing the equipment would avail to correct the deficiency (a host of products to compensate for the protocol weakness not withstanding).

Cryptographic transitions pose special challenges with similarities to forced system or hardware conversions. The change is rarely limited to a single application or platform. Similar to data transmission or data storage strategies, cryptographic security is infrastructural. In current commerce applications, a company relies on cryptographic security measures whether it knows it or not. The default use of cryptography rarely reflects the needs of a specific business (other than, perhaps, the vendor's business).

79.3 Lifecycles for Encryption Products

Cryptographic security products may have features or specific implementation factors that may provide a better clue to its lifecycle. Just as certain life-style factors may increase or decrease a person's health and longevity, so too do aspects of product implementations. For example, a hardware implementation for a specific speed, latency, and physical layer protocol may fall victim to rapid changes in telecommunication technology. Here, obsolescence is unrelated to merits of the cryptosystem. The product ends its lifecycle just as tubes gave way to transistors that gave way to integrated circuits, etc. An additional source of obsolescence is the vendor's planning for its product. The vendor simply decides not to support the product. RSA Security's SecurPC, introduced in 1992, is an example of this for RSA ended support for it in 1996. Archived files or e-mail protected by this product would require a Windows 98 software platform for decryption because the product does not run on Windows 2000 or Windows XP. Clearly, factors beyond the efficacy of the algorithm will limit the life expectancy of a cryptographic security product.

Perhaps, just as strangely, it may be found that the birth of a new cryptographic security product is premature. Such a product might die if a market for it does not develop quickly. Or if the sponsoring company has sufficient staying power, the premature product may live long and prosper.

Because breakthroughs like RSA's public key technology may have come to market before the industry even understood what problems it might solve, businesses have struggled with public key infrastructure (PKI) projects and other attempts at implementing cryptographic products. Many organizations have dozens of cryptographic products—often where a single, well-chosen product would have sufficed. The efficacy of these products remains generally unknowable by the people who buy and implement them. Few information technology professionals (or information security administrators) follow the cryptographic research literature or have access to a cryptographic laboratory for testing.

Since the early works on public key cryptography, e.g., Whitfield Diffie's and Martin Hellman's work in 1975, cryptographers have devised many asymmetric key schemes based on an almost limitless array of algorithms. Current work includes advances in elliptic curves cryptography (ECC),[4] hyper-elliptic cryptosystems,[5] RSA variants and optimizations,[6] multivariate quadratic equations over a finite field

[4]For example, work by Katsuyuki Okeya and Tsuyoshi Takagi or work by Kristen Eisenträger, Kristen Lauter, and Peter L. Montgomery. V. Miller and N. Koblitz introduced ECC in mid-1980.

[5]Hyper-elliptic cryptosystems, a generalization of ECC, was introduced by N. Koblitz ca.1989.

[6]For example, work by Adi Shamir (the "S" in "RSA").

(the MQ problem),[7] and lattices.[8] Future advances in quantum cryptographic key management and biological computing (i.e., using genetic structures to form living computers) may drastically change cryptographic products. Unfortunately for most information security practitioners, a Ph.D. in mathematics seems to be only a good starting point for research in cryptosystems.

To a greater extent, professionals depend on the vendors of cryptographic products to educate them on the products' merits. Without casting aspersions on the sales forces for these products, few will have the motivation or objectivity or the academic background sufficient to evaluate their own product. Fewer will have sufficient access to fairly compare and contrast the technical merits of competitors' products. And few, if any, will have the ability to assess the current state of cryptanalysis versus their and their competitors' products. But if such salespeople existed, would information security professionals understand the assessments?

To protect from ignorance, information security professionals should rely on products evaluated through nationally accredited laboratories, e.g., the National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP).[9] However, this may lead to another potential end-of-life situation for a cryptographic product, i.e., the loss of accreditation. Once a previously approved product loses accreditation, any continued use of the product places an organization at risk. Having a transition plan for accredited products is the best defense.

Beyond technical reasons for cryptographic technology lifecycles' running out prematurely, political factors may also lead to the stillbirth of a cryptographic technology. NSA's Skipjack is a good example of this. It had two embodiments: Clipper Chip for voice communications and Capstone for data. Whatever the merits of the Skipjack algorithm, the concept of cryptographic key escrow by the federal government created such political backlash that few commercial implementations resulted.[10]

79.4 Business Implications of Lifecycle

Most business functions have a financial justification as does the basis for investments in the technologies that support them. To replace (or physically upgrade where feasible) a hundred billion dollars of automated teller machines (ATM) and point of sale (POS) equipment in order to support a replacement for DES, for example, cannot (and did not) happen quickly. The United States' financial services industry, however, expected a long life for its rollout of ATM. The need for the long life was partly based on the large investment it had to make in equipment and systems, but it also reflected the risk inherent in a change of business model. Very early adopters had the opportunity to upgrade or replace equipment several times before the forced migration from DES to Triple-DES. Exhibit 79.1 gives a timeline of Triple-DES in the financial services industry. (AES came out too late and would have required a more massive revolution instead of evolution of existing systems.) Weaknesses in PIN-block format, setup protocols, and nonstandard messages required changes as the networks became more interdependent and attacks against the systems became more sophisticated. The replacement of equipment well before its scheduled and booked depreciation date creates a financial hardship for the business as it may invalidate planning assumptions used to justify the original implementation. Far worse, however, is the potential harm if the resulting business model is made null and void. Privacy concerns, in large measure because of inadequate security and to public perception that this inadequacy was wide spread, probably hastened the demise of many already stressed dotcoms whose business models assumed privacy as a given.

[7]Examples of public key cryptosystems based on the MQ problem include Hidden Fields Default (HFE), Quartz, and Sflash. For more information, see www.nicolascourtois.net.

[8]For more information, see //www.tcs.hut.fi/~helger/crypto/link/lattice/

[9]The Directory of Accredited Laboratories maintained by NIST is available at http://ts.nist.gov/ts/htdocs/210/214/scopes/programs.htm.

[10]For more information, see http://www.epic.org/crypto/clipper/

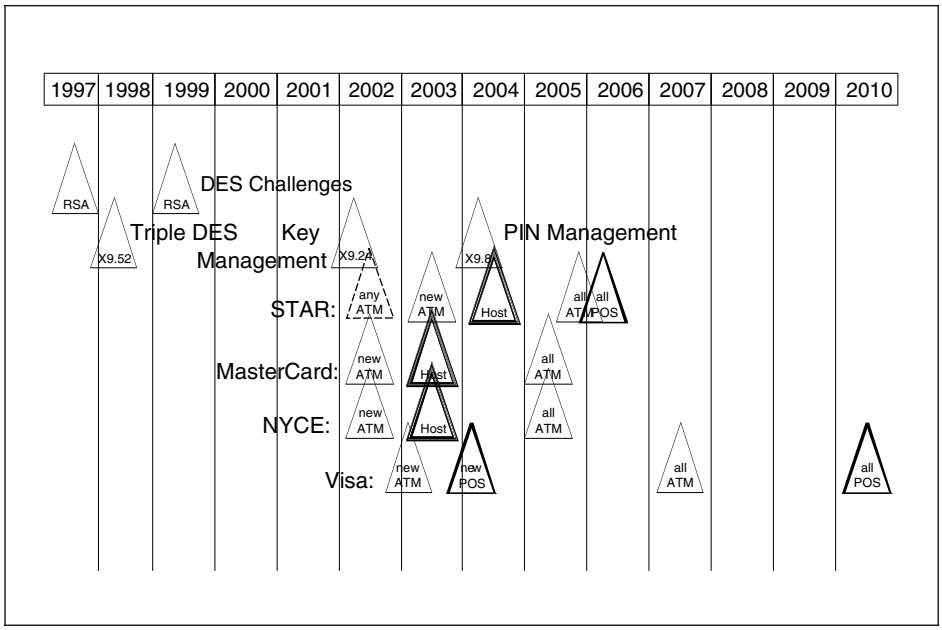

EXHIBIT 79.1 Triple DES time line.

Businesses already feel the pain of near constant desktop system upgrades. Here, vendors try to make the transition smooth with as much backward compatibility as possible. With advances in cryptography, entire classes of algorithms may become obsolete in a single breakthrough. Transitions from a newly broken cryptosystem to a cryptosystem believed to be safe, at least for the moment, are unlikely to be simple migrations.

Business planning for cryptographic security measures needs to include planning for cryptographic lifecycle contingencies. Just as businesses need business continuity planning against adverse events (e.g., natural disasters, fire, sabotage, and human error), businesses need to plan for the inevitable transition from one cryptographic technology to the next. This includes contingency funding and planning for catastrophic cryptographic failure where a rapid transition must occur and for more gradual evolution to more advanced technologies as existing ones approach obsolesce.

79.5 Principles for Cryptographic Transitions

The following four principles prescribe the process for a successful cryptographic transition: vulnerability assessment, impact analysis, implementation, and reconciliation.

79.5.1 Vulnerability Assessment

The principle of the vulnerability assessment addresses the need to understand the applications or infrastructural elements that cryptography will protect or support. With an understanding of the business issues and of the technical vulnerabilities to be addressed by cryptographic measures, a foundation is created on which cryptographic transitions must be based.

The first task is to ascertain legacy system requirements. The current security requirements must then be confirmed. Typically, this is accomplished by reviewing legacy documentation and current operating procedures. However, legacy systems may not be fully documented or specifications identify what was planned but not necessarily implemented. Further, operating procedures may be obsolete or

simply not followed. It may be necessary to augment documentation with interviews to determine legacy system requirements.

The second task is to determine new system requirements. This can be accomplished by reviewing projects currently in progress and—even more importantly—by reviewing strategic business plans. Because many cryptographic systems can remain in use for 10 or more years, transitioning to a security architecture and an enterprise management system that can support short-term and long-term business strategies is an important aspect of determining new system requirements.

The third task is to determine the infrastructure requirements. Unless the business strategies have previously identified and documented such requirements, it will be necessary to conduct interviews. One important group that should be interviewed is the operations staff because it supports the production applications and relies on documented procedures. Another group that should be interviewed is the information technology staff because it addresses the gap between the production systems and the users. Other important groups include database administrators, security officers, and general counsel. The collective knowledge of these groups is critical in determining the infrastructure requirements.

The fourth task is to perform a formal vulnerability assessment of systems and infrastructures to ascertain the potential threats, realistic vulnerabilities, and business and technical risks and to derive the appropriate security requirements.

79.5.2 Impact Analysis

The principle of the impact analysis addresses the effect that cryptography has and will have on the business systems. The impact analysis also translates technical issues into financial or business terms important to internal communication.

The first task is to perform an inventory assessment to determine where cryptography is used, how it is used, and why it is used versus other controls. In this inventory, information should be gathered about the algorithms, protocols, and devices or products currently in use.

The second task is to perform a dependency analysis to determine where systems have interdependencies and whether applications, infrastructural elements, or devices are or can be algorithm independent. If specific functions can be identified that might be common, e.g., key generation, digital signature, message encryption, or file encryption, the potential for isolating these functions into an abstraction layer that would reduce the future impact of cryptographic transitions should be documented.

The third task is to address jurisdictional issues to determine current and future needs for cryptography in multi-national, national, and regional locations. Different nations have different rules and laws that may affect the overall security architecture.[11]

The fourth task is to address migration issues to determine availability of cryptographic products to buy solutions or cryptographic tools to build solutions where products are insufficient or unavailable. In some cases, further analysis is necessary to determine alternatives to cryptography solutions.

79.5.3 Implementation

The implementation principle is the basic project management lifecycle that has been summarized here into development, testing, quality assurance, and deployment planning tasks. Development planning is documenting the manpower, resources, time tables, reporting, and auditing for the modification or replacement of the application, infrastructure, or equipment. Test planning includes documenting test cases and test results approved by management for unit testing, integration testing, system testing, and parallel testing. Quality assurance planning includes documenting final acceptance with roll-back plans that have been reviewed, approved, and signed off by management. Careful planning avoids any

[11]For more information, see Poore, R.S. 2000. Jurisdictional issues in global transmissions. In *Information Security Management Handbook*, M. Krause and H.F. Tipton, eds., *4th Ed*., *Vol. 1*. Boca Raton: CRC Press.

cold cut-over. Further, deployment planning must include documented roll-out schedules with incremental modifications and the ability to roll-back in the case of unforeseen problems.

79.5.4 Reconciliation

The fourth and final principle's, reconciliation, objective is to determine the cryptographic transition's successfulness. A post mortem should be conducted to review the project's successes and failures and to document these for future improvements. The team should learn from its mistakes and convey that wisdom to future project teams. In addition to the post mortem, a monitor program should be implemented to measure system results against expected results. Any unexpected events should be investigated, documented, and resolved. The initial monitoring should be frequent (e.g., hourly, daily, weekly) and eventually reduced to normal operational status reports (e.g., monthly, quarterly).

Because external factors, many that have been previously addressed, may force the organization to initiate a cryptographic transition sooner than planned, these principles should be formalized into its business planning and the organization should be informed of changes in cryptography.

79.6 Prudent Measures

In closing, here are eight considerations to incorporate in cryptographic transition planning for an organization:

1. Do not ask the company to invest in products that depend on "bleeding edge" cryptosystems. The best safeguard against a poor cryptosystem is time. Let researchers have the time to properly vet the new cryptosystem, and let competitors debug their own implementations.
2. Require independent certification or vetting of cryptosystems, where possible, utilizing recognized standards (e.g., Common Criteria—for additional information in the U.S.A., see NIST Special Publication 800-37, Guidelines for the Security Certification, and Accreditation of Federal Information Technology Systems).
3. Use cryptosystems based on recognized national or international standards. Beware of proprietary algorithms, protocols, or embodiments.
4. Understand the target environment for a vendor's product, including any explicit limitations; ensure the appropriateness of the product for the environment where the organization will run it. For example, some cryptographic security products assume the existence of a physically secure environment or they will run on a trusted workstation. If the plan is to roll one of these products out to remote users whose environments are unknown, the product should be expected to fail.
5. To the degree possible, negotiate assurances into the contract that share the risk of cryptographic failure with the vendor. Always believe a vendor's risk judgment when the vendor is unwilling to take any responsibility for its product. If the vendor does not trust its product, neither should a company.
6. Seek qualified experts' opinions and colleagues' experiences. Learning from the experience of others is almost always preferable to experiencing the learning. If no one in the organization has had an experience with this vendor or product, then refer back to the first measure listed here.
7. Incorporate cryptographic life-cycle considerations into business continuity planning. A cryptographic security failure can pose a serious threat to business operations both by potentially exceeding acceptable business risks for normal operations (a threshold that management may potentially waive to permit a period of operations while a transition to a new product occurs) and by exposing network or database operations to attacks that prevent operations.
8. Create (or follow) an architecture that isolates cryptographic services to an abstraction layer that is independently invoked. This permits replacement or upgrade with minimal impact to the overall application. As discussed in regards to lifecycles, they can be depended on for their uncertainty.

Use as a design assumption that the cryptographic security product will require changes or replacement sooner than the application depending on it will go away.

This last item is perhaps the most important. The field of cryptography is rapidly advancing with cryptanalysis' finding more rapid introduction to general use than more advanced cryptosystems. These advances increase the risk that a given cryptographic implementation will provide effective security for a shorter life than predicted at the time of implementation. Although issues such as Y2K could easily have been anticipated well in advance, programming languages and practices in the 1960–1980 decades generally failed to consider the pending obsolescence, believing instead that the applications they were creating would not live until then. Enough of these applications did survive to cost businesses billions of dollars to address the oversight. Waiting until a business is forced to change cryptographic implementations increases costs and places information assets at risk. Cryptographic transitions are inevitable. Companies should plan for it now.

Note

Poore, R.S. 2003. Advances in Cryptography. *Information Systems Security*, Vol. 12, Issue 4. Auerbach Publications, New York.

References

1. Poore, R.S. 2002. The new standard—a triple play: 3DES. *PULSATIONS* (January).
2. Stapleton, J. and Poore, R.S. 2005. Cryptographic Transitions. Presented at ECC Conference 2005.
3. Poore, R. S. 2005. Cryptographic key management concepts. H. F. Tipton and M. Krause, eds., In *Information Security Management Handbook*, *5th Ed., Vol. 2.* CRC Press, Boca Raton.
4. Special Publication 800-57, *Recommendation for Key Management, Part 1: General*, August, 2005. National Institute of Standards and Technology, Washington, DC.