

Cryptographic transitions

Jeff Stapleton
Innové LLC
jeff.stapleton@innove-us.com

Ralph Poore
Innové LLC
ralph.poore@innove-us.com

Abstract

A cryptographic transition is defined as managing the passage from one security architecture to another in a methodical approach that is consistent with prudent business practices and security guidelines. This paper addresses the three technology issues that drive the business and security justifications for initiating a transition; the principles guiding policy and practices when conducting a transition; the process to conduct a successful transition; and provides the pros and cons of several actual case studies of cryptographic transitions.

1. Introduction

This paper defines a cryptographic transition as the passage from one security architecture; whose differences can be rather dramatic akin to comparing an ancient wind-driven seagoing clipper ship to a futuristic anti-matter powered starship. These transitions must be managed in a methodical approach; such that the transition is consistent with prudent business practices and security guidelines. The genesis for such transitions stems from increased business risks due to various technology issues. This paper discusses the technology issues; provides principles to manage cryptographic transitions; presents the transitional steps; and affords four actual case studies.

2. Technology Issues

Technology issues are grouped into three categories related to cryptographic vulnerabilities.

- **Key Life Cycle** issues relate to advancements in raw computing power has increased risk to shorter cryptographic keys.
- **Algorithm Life Cycle** issues relate to advancements in mathematical research can increase risk to existing algorithms.

- **Product Life Cycle** issues relate to losing hardware and/or software vendor support such that products are no longer maintainable.

2.1 Key Life Cycle

Gordon Moore made his famous observation in 1965, four years after the first planar integrated circuit was discovered, observing an exponential growth in the number of transistors per integrated circuit and predicted that this trend would continue; 2005 is the 40th anniversary of Moore's Law [16]. The unending advancement of computer capability continues to erode the security of the symmetric key space; increased computing power continues to decrease the time for an exhaustive key search.

In 1977 the National Bureau of Standards (NBS), now the National Institute of Standards and Technology, in cooperation with the National Security Agency (NSA), adapted the International Business Machines' (IBM) encryption algorithm Lucifer as the new Federal Information Processing Standard (FIPS) 40 Data Encryption Standard (DES). DES has a fixed 56-bit key size (actually it's a 64-bit value with 8 parity bits) and a 64-bit data block. Assuming a computer could achieve a million DES calculations per second, it would take approximately 2,285 years to search the 2^{56} key space.

Twenty years later, in 1997 the DES II Challenge sponsored by the RSA Security Corporation was successfully completed. Computer power coupled with the Internet had advanced sufficiently such that employing an estimated 10,000 workstations tested about 90% of the 2^{56} or approximately 72 Quadrillion keys to discover the single DES key used in the challenge in 140 days. This accomplishment was a harbinger to the Financial Services Industry and the Federal government that the DES life cycle was reaching its end [17].

In a mere two more years, in 1999 the DES III Challenge was successfully completed in 22 hours

and 15 minutes. For this challenge, an estimated 100,000 workstations and a specially built computer called Deepcrack built by the Electronic Freedom Frontier (EFF) achieved an estimated 245 billion DES calculations per second. This accomplishment instigated the withdrawal of several DES-based standards. In addition, the Federal Reserve Bank, the National Institute of Standards and Technology (NIST) and the American Bankers Association issued recommendation letters to migrate from single-DES to triple-DES; a cryptographic transition.

Similar challenges continue to demonstrate Moore's law erosion of cryptographic security. In 2002 the RC5-64 Challenge was successfully completed. The organization *distributed.net* discovered the 64-bit key for the RC5 algorithm in 1,757 days. The 5-year project included cooperation amongst 331,252 individuals. A major difference between the DES III and the RC5-64 Challenge was the absence of the Deepcrack specialized hardware. The RC5-72 Challenge began in 2002 and is an ongoing effort [18].

2.2 Algorithm Life Cycle

Cryptographic algorithms are susceptible to advances in mathematics, computer science techniques or cryptanalysis methods. Such advances can shorten their longevity or dismiss their usefulness. The term cryptanalysis was coined by William Friedman in 1920 in his manual "The index of Coincidences and its Application in Cryptography." William and his wife Elizabeth were the federal code breakers assisting the US Coast Guard during the late 1920s Prohibition-era in deciphering radio messages from the Pacific and Atlantic rum runners.

The earliest known documentation of cryptanalysis was over a thousand years ago in the ninth century by the Arabic researcher Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi in his treatise "A Manuscript on Deciphering Cryptographic Messages" addressing frequency analysis.

2.2.1 Differential Cryptanalysis

The discovery of differential cryptanalysis is generally attributed to Eli Biham (currently a professor at the Technion Israeli Institute of Technology Computer Science Department) and Adi Shamir (currently on the faculty of Mathematics and Computer Science of the Weizmann Institute) in the late 1980s, who published a number of attacks against various block ciphers and hash functions,

including a theoretical weakness in the Data Encryption Standard (DES). In fact, one of the controversies with the National Security Agency's (NSA) involvement during the transformation of the IBM Lucifer algorithm to DES in the late 1960s was its undisclosed design process. Don Coppersmith, one of the IBM developers, revealed in 1994 that defending against differential cryptanalysis was a design goal. It appears that the NSA was aware of the technique before its rediscovery at IBM, and did not want the attack to become public knowledge; this was the reason the design process was kept secret.

While researching error-correcting codes in 1990, Mitsuru Matsui was inspired by Biham and Shamir's differential cryptanalysis, and is attributed the discovery of linear cryptanalysis. He first applied the technique to the FEAL cipher in 1992. Subsequently, Matsui published an attack on DES, eventually leading to the first experimental cryptanalysis of the cipher reported in 1993. However, this attack on DES is not considered very practical, as it requires the attacker to have 2^{43} (over 8 trillion) known plaintexts and the corresponding ciphertext examples.

Differential cryptanalysis using side-channel data includes timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other cryptographic algorithms introduced by Paul Kocher in 1996 and his differential power analysis (DPA) in 1999. By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems. DPA is a method of attacking a cryptosystem which exploits the varying power consumption of microprocessors while executing cryptographic program code.

2.2.2 Integer Factorization

Integer factorization is another research area as it is a "hard" mathematical problem on which the RSA algorithm is based. Beyond the brute force approach of dividing by every prime number, Carl Pomerance developed the Quadratic Sieve in 1981. The method is based on discovering congruence of squares ($X^2 \equiv Y^2$) modulo the integer being factored, which often leads to a factor of the integer. It is still the fastest for integers under about 110 decimal digits, and is considerably simpler than the number field sieve.

Another factorization method developed by Hendrik W. Lenstra is the elliptic curve factorization method (ECM) published in 1987 as the paper "Factoring

integers with elliptic curves” in the Annals of Mathematics. This method was the best algorithm for integer factorization until the general number field sieve was developed. It is still best for factoring out divisors of 20 to 25 digits.

Arjen Lenstra and Hendrik Lenstra published the general number field sieve in their 1993 lecture notes “The Development of the Number Field Sieve.” This technique is the most efficient algorithm known for factoring integers larger than 100 digits (in comparison an RSA 1024 key is larger than a 290 digit integer). The number field sieve performs computations and factorizations in number fields. This results in many rather complicated aspects of the algorithm, as compared to the simpler rational sieve

2.2.3 Quantum Computing

The ultimate advancement predicted to date is quantum computing. A quantum computer is a device that makes use of the quantum mechanical phenomena of superposition, enabling data to be represented in qubits. A classical binary computer can only process a 0 or 1 data bit sequentially, whereas a qubit can handle multiple states at the same time. However, research is still in its infancy and the ability to program them is not well understood. Peter Shor developed a quantum algorithm for factoring large integers in relatively quick time, which might render RSA useless. Shor's algorithm was demonstrated in 2001 by a group at IBM, which factored 15 into 3 and 5, using a quantum computer with 7 qubits.

2.3 Product Life Cycle

Like any hardware or software product, cryptographic products are likewise vulnerable to unanticipated market trends, such as companies terminating unprofitable product lines; companies going out of business; or merger and acquisition situations where the new parent company terminates the product due to market conflict.

For example, RSA Security introduced its SecurPC product in 1992 and ended support in 1996. The product provided software encryption capability to protect files stored on disk or attached to an e-mail. It originally ran on Windows, continued to run on Win/98, ran with limited functionality on Win/NT, and no longer operates with Win/XP. Hence encrypted files created on earlier computers and

ported over to current systems can no longer be decrypted.

Another more widespread example is the evolution of web browsers. From the early days of Netscape introducing the Secure Socket Layer (SSL) to Microsoft's Internet Explorer, web browsers and servers have evolved SSL and other web applications such that earlier browser versions can no longer operate.

The Cylink Corporation, founded in 1983, developed cryptographic microchips, however with its 2002 bankruptcy, the companies intellectual property was acquired by SafeNet. In a more dire example, CertifiedTime was founded in 1998 to provide trusted time stamping services; however, its venture capital funds ran dry and the company expired in 2002.

3. Transition Principles

Principles are the core concepts that provide guidance towards orchestrating a successful cryptographic transition; and are grouped into three areas:

- Business Requirements
- Cryptographic Hardware
- Application Management

3.1 Business Requirements

The business requirements principle is a primary element of a cryptographic transition and is an overarching concept that applies equally to the other principles. Any project management methodology promotes a requirements phase for capturing the technical and operational goals. This equally applies to a cryptographic transition, regardless of its size or scope. Clearly understanding and documenting the underlying business objectives will result in more accurate technical and operational requirements and ultimately result in a more successful transition.

3.2 Cryptographic Hardware

The cryptographic hardware principle addresses an algorithm's implementation. Algorithms typically begin life as software; once created, an algorithm can operate in several environments. The algorithm can remain as executable software running on a general purpose computer; however this is a high risk implementation as it is vulnerable to exposing the algorithm and its cryptographic keys to unauthorized or inadvertent tampering. Alternatively, the algorithm can run in a dedicated device whose sole purpose is to provide cryptographic services; and the algorithm can further be converted to programmable

firmware or even hardware implementation. For the alternative choice, the cryptographic hardware principle is organized into four concepts:

- Security Module
- Interoperability
- Reliability
- Certification.

3.2.1 Tamper Resistant Security Module

The tamper resistant security module (TRSM) concept is where the cryptographic product has a high degree of assurance that the product is free from defects or malicious attributes such that its security features and mechanisms resist accidental and malicious attacks, both physical and logical attacks, throughout the product's life cycle. Essentially this means that cryptographic keys cannot be revealed or misused. We use the term "tamper resistant" to recognize the fact that there is no such thing as tamper proof; operating under the presumption that given sufficient time and money, any security control can be circumvented. A manufacturer must include strong security controls throughout the software and product development life cycle.

3.2.2 Interoperability

The interoperability concept is where products comply with industry standards such that for given input parameters and state, the product produces the same output parameters. This applies equally to the algorithm, the cryptographic scheme that employs the algorithm, and the application protocol that implements the scheme. Products from different manufacturers must interoperate, different products from the same manufacturer must interoperate, and even different releases of the same product from the same manufacturer must interoperate.

3.2.3 Reliability

The reliability concept is where manufacturers employ quality assurance standards, trusted engineering techniques and verifiable project management controls across the development life cycle. This concept must be closely aligned with the TRSM concept. The ability of a manufacturer to produce quality products in a reliably repeatable manner can be measured and awarded using industry quality management standards such as the ISO 9000 family of standards [6].

3.2.4 Certification

The certification concept is where products are certified to be compliant to industry standards by an independent and accredited laboratory. The National Institute of Standards and Technology (NIST) [8] and the National Security Agency (NSA) [9] of the United States, and the Communications Security Establishment (CSE) [10] of Canada support several such programs.

The NIST and NSA National Information Assurance Partnership (NIAP) is a collaboration to meet the security testing needs of both information technology consumers and manufacturers [3]. The NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) [4] is a national program for the evaluation of information technology products for conformance to the International Common Criteria for Information Technology Security Evaluation [11].

The NIST and CSE Cryptographic Algorithm Validation Program (CAVP) addresses validation testing for Federal Information Processing Standards (FIPS) cryptographic algorithms [2]. Algorithm validation is a prerequisite to the Cryptographic Module Validation Program (CMVP). All of the tests under the CAVP are handled by laboratories accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP).

The NIST and CSE Cryptographic Module Validation Program (CMVP) encompasses validation testing for cryptographic modules based on the Federal Information Processing Standards (FIPS) 140 Security Requirements for Cryptographic Modules [1]. All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). Vendors interested in validation testing may select any of the twelve accredited labs.

The NIST and CSE National Voluntary Laboratory Accreditation Program (NVLAP) [5] provides accreditation to North American laboratories. NVLAP operates in conformance with ISO [6] and the International Electrotechnical Commission (IEC) [7] standards, including conformity assessment [12] and laboratory requirements [13].

3.3 Application Management

The application management principle addresses the operational issues of current and future cryptographic transitions. The application management principle is focused towards a more scalable, extensible and flexible model; and is organized into four concepts:

- Algorithm Independence
- Security Architecture
- Enterprise Management
- Security Guidelines

3.3.1 Algorithm Independence

The algorithm independence concept is where the system security is independent of the cryptographic algorithm. This provides an architecture whereby the algorithm is easily changeable and requires that the system has the ability to identify, recognize and authorize which algorithms are in use. This capability can occur at the application layer, built within the infrastructure or provided within the TRSM itself. This concept must therefore be aligned with the business requirements principle.

3.3.2 Security Architecture

The security architecture concept is where the system cryptographic and security controls operate within a framework that is consistent and manageable across the enterprise. The architecture must address the business and security requirements by providing the appropriate security and technical solutions. At the same time, the solution set must be manageable and fit within a consistent framework. For example, if a business requirement is to operate in a multi-national environment, then the background check process must be consistent with the disparate privacy laws in different countries. Another example is the selection of cryptographic algorithms that are driven by various industry standards and governmental policies.

3.3.3 Enterprise Management

The enterprise management concept is an extension of the security architecture providing the ability to securely administer enterprise resources. Application devices ranging from automated teller machines and point of sale terminals used in the financial industry to common information technology (IT) network routers, printers and servers are becoming more sophisticated and offer increased functionality, they are becoming more vulnerable to attack. Enterprise management is the capability to securely manage such a wide variety of application devices across disparate management systems. These management

capabilities include key management, inventory management, configuration management, policy and audit controls. Newer industry standards provide a common message format and protocol [14].

3.3.4 Security Guidelines

The security guidelines concept is addresses the necessary and appropriate security policies, practices and procedures for access controls, mutual authentication, and overall support of the enterprise management principle. Policies state the goals of what is to be achieved and are often public. Practices state the performance of how the policy goals will be fulfilled and are typically considered to be sensitive. Procedures are the detailed operational instructions on executing the practices.

The goal of most organizations is to meet or exceed industry standard practices when using technology in a responsible manner by imposing proper controls. Compliance to policies, standards, practices and procedures can only be assured by verification of the controls via a security review or audit. Such reviews and audits must be performed by a qualified professional practitioner and should be conducted by an independent third party.

4. Transition Process

The necessary process to conduct a successful cryptographic transition can be summarized in the following phases:

- Vulnerability Assessment
- Impact Analysis
- Implementation
- Reconciliation

4.1 Vulnerability Assessment

The objective of the vulnerability assessment phase is to collect relevant data to perform a risk assessment.

The first task is to ascertain legacy system requirements. Current security requirements must be confirmed. This is typically accomplished by reviewing legacy documentation and current operating procedures. However, all too often legacy systems are not fully documented or specifications identity what was planned but necessarily implemented. Further, operating procedures are often stale or simply not followed. Thus, interviews can play an important role in determining 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 reviewing strategic business plans. Since many cryptographic systems can remain in use for 10, 15 or even 20 years or more, 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, conducting interviews is the best approach. One important group that should be interviewed is the operations staff who supports the production applications and rely on documented and execute procedures. Another group is the IT staff who addresses the gap between the production systems and the users. Other groups include other systems support staff such as 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 risk assessment of systems and infrastructures to ascertain the potential threats, realistic vulnerabilities, business and technical risks and derive the appropriate security requirements.

4.2 Impact Analysis

The objective of the impact analysis phase is to determine the effect that cryptography has and will have on the business systems.

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.

The second task is to perform a dependency analysis to determine where systems share an interdependency and whether applications, infrastructure and/or devices are and/or can be algorithm independent.

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

The fourth task is to address migration issues to determine availability of cryptographic products to buy solution, 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.

4.3 Implementation

The implementation phase is the basic project management life cycle 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. Cold cut-over should be avoided at all costs. Deployment planning includes documenting roll out schedules with incremental modifications, and the ability to roll-back in the case of unforeseen problems.

4.4 Reconciliation

Reconciliation is the final and fourth phase whose objective is to determine the successfulness of the cryptographic transition. A post mortem should be conducted to review the project successes and failure and document future improvements. The team should learn from their mistakes and convey that wisdom to future project teams. In addition to the post mortem, a monitor program should be put into affect to measure system results to expected results. Any unexpected events should be investigated, documented, and resolved. Initial monitoring should be rather frequent (e.g. hourly, daily, weekly) and eventually reduced to normal operational status reports (e.g. monthly, quarterly).

5. Case Studies

5.1 Healthcare Industry Study

The healthcare industry received a security wakeup call with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its associated privacy and security regulations. While not explicitly mandating cryptographic security measures, the regulations explicitly identified encryption as an acceptable technique and, as a

practical matter, left no viable alternative for protecting information in transit. For many affected organizations this meant a transition from no cryptographic security measures to what most felt to be an oppressive level of control. For a minority that already had some cryptographic security measures, the transition required a unification of disjointed enclaves generally among incompatible software solutions.

Our case study discusses a Fortune 400 pharmaceutical and health management company that had grown rapidly through acquisitions resulting in disunity of policy, procedure, culture, systems, and management. During an 18-month transition period, information systems management succeeded in arguing to executive management that HIPAA compliance for privacy and for security was simply a paperwork exercise that required no changes to applications, hardware, or system software. During that same period, the information systems departments spent in excess of \$25 million to change applications to comply with HIPAA transaction formatting requirements.

Information security measures work best when integrated into application design. Transitioning to stronger controls is, therefore, best accomplished when a major revision to applications is otherwise necessitated. The changes required by HIPAA had provided the opportunity for integrating security and privacy measures into their applications. Having decided not to do so, the organization attempted to implement cryptographic security measures on an *ad hoc* basis. This required them to implement independent products and procedures for FTP, e-mail, web, and mainframe applications. Since they supported many clients and millions of consumers, they soon learned how difficult a piecemeal solution would be. Not having a unified offering and having failed to incorporate contract terms that permitted them to enforce one, they faced a serious hurdle with large clients who wanted tailored solutions (and who could argue that compliance with HIPAA privacy and security rules was implicit—if not explicit—in their existing contracts, so no additional charges would be acceptable).

As a case study, this organization shows us largely what an organization should avoid. As described in section 4, an orderly transition process is needed that is based on proper assessments and that is integrated into normal operations. By attempting the transition

in isolation from the overall application changes, the business spent more, obtained less, and left itself facing future, complex transitions for which they were no better prepared.

5.2 Financial Industry Study

The automated teller machine (ATM) networks, including the use of personal identification numbers (PIN) with debit transactions at the point of sale (POS), transitioned from no encryption, to pseudo encryption, to the Data Encryption Standard (DES) in its early years. By the early 1990's the cryptographic security community was publishing papers warning of the need for a follow on to DES. However, by the time key-space exhaustion attacks on DES were a commercial fact, as discussed in section 2.1, the financial industry had yet to commit to a transition away from DES. Instead it had doggedly continued to invest in DES implementations. With the risk of compromise of entire bank's card bases becoming a reality, the transition to Triple DES (TDES) began in earnest. Part of the problem was the absence of a viable alternative, as the search for the Advanced Encryption Standard (AES) did not begin until 1997.

Triple DES, however, had at least one advantage as a transition from DES. An organization could phase its implementation since using a single key three times in Triple DES produces the same cryptographic result as using the single key in DES. They could update hardware and implement Triple DES on critical links while legacy equipment remained operational.

The banks did face a downside, however. The new ATM, POS, and host cryptographic equipment that supported the new Triple DES would have to remain in service for many years in order to amortize their costs. The timeline in Figure 5.1, however, shows you what they faced. TDES had lost its standing to AES before most financial institutions had implemented it. Yet, most of the financial services industry had not mandated compliance with TDES until 2005. Much of the newly upgraded TDES equipment, however, could not be upgraded to AES without expensive hardware replacement.

Since Triple DES was only an interim solution, they will face a larger, not backward-compatible, transition.

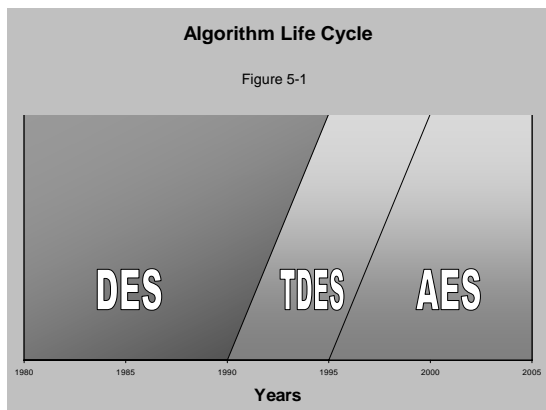


Figure 5-1

5.3 Government SBU Study

For information the government deemed “sensitive but unclassified” (SBU), which included data covered by the Privacy Act, for example, the Data Encryption Standard (DES) was originally the algorithm of choice. Prior to DES [19], the government used cryptographic hardware provided for classified programs, used commercially available proprietary products, or went without. While some elements within the government may have used Triple DES as a replacement for DES, it was the official follow-on for only a few years [20]. The government waited for the Advanced Encryption Standard (AES).

Thus, the cryptographic transitions faced within the government varied: from none migrating to DES and then to AES; from classified equipment to commercial-off-the-shelf (COTS) DES equipment and then to AES; from none to COTS proprietary, to DES, to Triple DES and now to AES; and variations of these paths. From the mid-70s until the late 90s, transitions were complicated by internal struggles over cryptographic policy. Should algorithms be secret or publicly disclosed? Should cryptographic keys be escrowed or unrecoverable? How strong should cryptographic implementations be for SBU applications? With DES, the questions were answered with a published standard that was probably better than the intelligence community would have liked, but not as strong as originally proposed. As previously described, DES was effective for SBU for over 20 years. TDES, many times stronger, was good for less than 10 years before it was replaced by AES—an algorithm strong enough

when properly implemented to protect even Top Secret data.

5.4 DoD Crypto Modernization

The protection of military and national security secrets has long been the arena for cryptography. This is also the area in which the most cryptanalysis, i.e., the process of breaking cryptographic systems, has historically occurred [21]. One might imagine, then that superseding one cryptographic system with another would have evolved into a routine process. Several factors, however, militated against this. First, early systems were specific to the technology they protected. A teletype, a telephone, and a radio for examples operated in such dissimilar manners that each required special approaches to cryptographic protection. Second, the development of early systems was often “stove piped.” Partly this was an issue of security and partly bureaucracy. Third, technology was changing rapidly with each new system or major application attempting to take advantage of cryptographic security improvements. A fourth factor was budgetary. Government systems were often forced to remain in use well beyond the originally designed life, so the cryptographic systems designed to support them had to remain as well.

As analog systems gave way to digital systems and as standalone systems gave way to networked systems, the need for an orderly modernization process increased. The Department of Defense (DoD) Cryptographic Modernization program (Crypto Mod) provides such a transitional process [15].

6. Summary

This paper discussed the eventful life cycle of keys, algorithms, and products, providing a brief history of past events and future considerations. The three transition principles, business requirements, cryptographic hardware and application management were described. The transition process was reviewed and several real-world case studies were provided.

It is important to keep in mind that cryptographic transitions are cyclic. Keys, algorithms and products all have life cycles, any of which can trigger a cryptographic transition, so one successful transition does not imply that another transition will never be necessary. Along with taxes and death, it is a certainty that future mathematical, technical or marketing events will initiate another cryptographic transition.

7. References

- [1] <http://csrc.nist.gov/cryptval>
- [2] <http://csrc.nist.gov/cryptval>
- [3] <http://niap.nist.gov/>
- [4] <http://niap.nist.gov/cc-scheme/index.html>
- [5] <http://ts.nist.gov/ts/htdocs/210/214/214.htm>
- [6] www.iso.org
- [7] www.iec.org
- [8] www.nist.gov
- [9] www.nsa.gov
- [10] <http://www.cse-cst.gc.ca/>
- [11] ISO/IEC 15408:2005, Information technology -- Security techniques -- Evaluation criteria for IT security
- [12] ISO/IEC 17011:2004, Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies
- [13] ISO/IEC 17025:2005, General requirements for the competence of testing and calibration laboratories
- [14] American National Standards X9.113-draft, Enterprise Management and Security
- [15] www.cryptomod.org
- [16] www.intel.com
- [17] www.distributed.net/des/
- [18] www.distributed.net
- [19] FIPS PUB 46, Data Encryption Standard, officially established DES on January 15, 1977. FIPS PUB 46-3, which specified the use of Triple DES, was withdrawn May 19, 2005
- [20] FIPS PUB 46-3 permitted DES for “legacy” systems until it was withdrawn in 2005, and AES was in development during the six-years since 1999 when 46-3 became official
- [21] David Kahn’s *The Codebreakers* is an excellent treatment of this subject