



SPYRUS®



Audit Framework for Public Key Infrastructure

White Paper

Audit Framework for Public Key Infrastructure

White Paper

Document No. 412-210007-01

June 2002

SPYRUS[®]

< info@spyrus.com >

< <http://www.spyrus.com> >



© Copyright by SPYRUS, Inc. 1998-2002. All Rights Reserved.

This document is provided only for informational purposes and is accurate as of the date of publication. This document may not be distributed for profit. It may be copied subject to the following conditions:

- All text must be copied without modification and all pages must be included.
- All copies must contain the SPYRUS copyright notices and any other notices provided herein.

Trademarks

SPYRUS, the SPYRUS logos, LYNKS Privacy Card, Security In A Box, SPEX/, SPYCOS, Multisession, Hydra Privacy Card, Cryptocalculator, Talisman/DS and WebWallet are registered trademarks of SPYRUS. Rosetta, LYNKS Metering Device, IES, Personal Access Reader, Signet, Talisman/SAM, WEBREG and WEBSAFE are trademarks of SPYRUS.

Terisa Systems is a registered trademark and SecureWeb Toolkit, and SecureWeb Payments are trademarks of Terisa Systems, Inc., a wholly-owned subsidiary of SPYRUS.

All other trademarks are the property of their respective owners.

Contents

| | | |
|----------|---|----------|
| 1 | PKI AUDIT OVERVIEW..... | 1 |
| 2 | AUDIT..... | 2 |
| 2.1 | PURPOSE..... | 2 |
| 2.2 | AUDIT POLICY..... | 2 |
| 2.3 | AUDIT-RELATED PKI POLICY AND PROCEDURES..... | 3 |
| 2.3.1 | Creating Trust: Audit of Root Key Generation..... | 3 |
| 3 | ACCREDITATION..... | 4 |
| 4 | CONCLUSION..... | 5 |

1 PKI Audit Overview

Public Key Infrastructure is much more than software, hardware, tokens and networks. To demonstrate the necessary trust and assurance, a PKI must conform to international standards and attest to this conformance through regular and ongoing audit. Conformance to the pertinent benchmarks of system security may lead to accreditation – externally recognized certification against one or more specific standards or similar trust schemes. The PKI policy framework establishes the parameters within which the organization intends to operate its PKI; the PKI audit framework provides the means to assure users, relying parties and other interested stakeholders that the PKI performs in accordance with its policy framework.

The SPYRUS PKI System was designed not only to conform to the relevant standards but also to demonstrate trust through standards-based audit and accreditation. SPYRUS develops its products on the basis of the appropriate standards, so that certification is achievable. Our policy and audit experts have developed the foundation for trust through audit. The SPYRUS PKI “Chain of Trust” architecture incorporates transaction audit. Audit provides the mechanism to determine whether policy rules have been followed in an effective and efficient manner. A successful audit can lead the way to accreditation, under the varying jurisdictional and legislative mandates being developed, and potentially to system certification against international standards.

This paper explains the fundamental processes that will enable an organization that has implemented a PKI to achieve accreditation and certification. These are increasingly required for global secure electronic business.

2 Audit

2.1 Purpose

Users, relying parties and other interested stakeholders need some evidence of the trust and assurance of a PKI. Throughout the world, different mechanisms are being introduced to provide such evidence, ranging from government regulation to the opposite extreme of self-declaration. In the first case, countries such as the United Kingdom are considering licensing certification service providers, or at least mandating a “trust scheme.” As another example, in the European Union, the electronic signature directive (1999/93/EC) specifies measures for compliance with the directive. Compliance with these measures is not mandatory; however, certification service providers in the European Union will be labelled according to their compliance, which will likely have the effect of making compliance with these measures mandatory. The United States federal government and several of the States are prescribing the parameters of certification service providers, again, with the effect of making compliance mandatory. In Canada and Australia, on the other hand, the federal governments are introducing high-level principles for authentication services, which can be interpreted in a variety of ways; development of these fundamental principles does, however, have the ultimate objective that they be adapted by certification service providers. In addition, in certain vertical markets, either legislation or procedures developed by industry associations are mandating certain ways of operating. One example is the Health Insurance Portability and Accountability Act in the United States, and the ensuing regulations, which are mandatory on any entity operating in the healthcare sector in the United States. Similarly, the trust system established in the North American financial services industry requires all parties to conform to a set of procedures and attest to this conformance through audit.

In short, audit is, first of all, simply sound management practice, to review policies and practices and to refine and adjust them on the basis of audit recommendations. Secondly, and specific to PKI, audit is fast becoming the means to give assurance to all parties involved – and the means to becoming and remaining a player in the field of providing certification services.

2.2 Audit Policy

A PKI Certificate Policy should derive from a corporate Security Policy, which in turn takes its direction from corporate objectives and goals. From both of these, a corporate audit policy can be created. An audit policy is simple and straightforward; its primary purpose is to specify what needs to be audited, how frequently, and by whom.

An audit policy considers the nature of the business, its activities and consequent level of assurance. For some, simply confirming that the most cost-effective procedures and processes are in place is sufficient. For others – such as PKI operations – explicit and demonstrable proof of a strong degree of assurance may be needed. Security has long been considered an activity supported by audit. Regular audit of the effectiveness of policies, administrative procedures and their implementation is essential to ensure accountability and effective management. The audit requirement can be met in various ways, depending on the jurisdiction and any regulatory requirements. For example, a corporate security officer may be authorized to conduct internal audit, on a regularly scheduled basis. Note, however, that audit should never be delegated either

to the person responsible for managing security on a daily basis, or to PKI administrators or operators. It is preferable that an external audit be conducted at least annually by an accredited auditor. For a small company, an objective review of internal audit may be substituted. The reviewer may be internal but must not have a reporting relationship with the person who conducted the audit.

In addition to formal audits, the person assigned can conduct frequent and periodic spot checks in different areas: for example, random checking of recruiting records to ensure that background checks are being carried out in accordance with personnel screening or recruitment policies; visual checking of the secure areas to ensure that logs are kept and unauthorized entry does not take place; review of contracting files to ensure that non-disclosure agreements are in place when warranted. In the case of particularly sensitive operations (e.g., those associated with Intellectual Property), detailed procedures that can be audited should be implemented. The latter may be required by law or government policy, for example, in the case of a company that works with government classified information. These are some examples of the specifics of an audit policy.

2.3 Audit-related PKI Policy and Procedures

SPYRUS has developed a comprehensive set of PKI Policies and Procedures (P&P) to assist customers in developing their own customized P&P documentation. One of the central advantages of the SPYRUS P&P templates is the reduced time it takes for a customer to implement its own auditable policies and procedures, which in turn reduces costs. In this regard, SPYRUS has developed Audit Guidelines for a variety of activities and functions, without which an accredited auditor would normally take several days to develop for each. SPYRUS professional services consultants have worked with clients through the preparation and conduct of PKI audits, and have proven the cost-effectiveness of this approach.

All PKI P&P should be audited for effective implementation. In addition, certain procedural documents are created for audit purposes. These include:

- Audit Procedures for secure root key generation,
- Physical Security Requirements for secure root key generation,
- Audit guidelines (derived from the audit policy).

2.3.1 Creating Trust: Audit of Root Key Generation

The foundation of a PKI is its root key – the private key that ultimately ensures trust in the final end-entity digital certificates, through a chain of trust in the hierarchical PKI. Generation of the root key must take place with maximum security controls. If the root key cannot be trusted, then the consequent activities of the PKI as a whole, as well as the transactions that the PKI purportedly serves to assure, cannot be trusted.

The secure audit process is designed to attest to the integrity of the root key generation as well as to ensure that the root key is maintained through strict adherence to procedural controls. The detailed procedures enable everyone present during root key generation to affirm that only the mandated steps were followed and that no anomalies occurred that might later impugn the integrity of the root key.

3 Accreditation

PKI Policies and Procedures provide the foundation for trust and assurance for electronic transactions. As the demand for a secure global economy increases, the need to prove trust in a PKI grows accordingly. To be accredited, a PKI must have standards-based, internationally recognized documentation. Standards and guidelines for PKI accreditation are being developed in several fora, including the American Bar Association Internet Security Committee and the American Institute of Certified Public Accountants; similar development is taking place at the international level, for example, in ISO and IETF sub-committees. As noted above, mandatory requirements for PKI accreditation and audit are being set by national jurisdictions through legislation and regulations. Accreditation is in the process of becoming mandatory for a PKI.

Implementing a PKI with the comprehensive set of P&P ensures that it will be able to meet the developing accreditation regimes. Compliance with mandated accreditation standards lowers the liability risk to an acceptable level, while non-compliance leaves PKI operators highly vulnerable. Certification to ISO or IETF standards is becoming the norm for PKI; foremost amongst these standards is ISO/IEC IS 15408 – Common Criteria for Information Technology Security Evaluation (Common Criteria). The U.S. National Institute of Standards and Technology's (NIST) Security Requirements for Cryptographic Modules – Federal Information Processing Standard # 140-1 (FIPS) defines the security requirements and four levels of assurance for the cryptographic modules that can be associated with a PKI system. FIPS 140-1 has been updated, and, as of May 2002, FIPS 140-2 is the effective standard. FIPS 140-2, the cryptographic module validation program, will be introduced into ISO to become an international standard in the fall of 2002. The Information Technology Security Evaluation Criteria (ITSEC) is still widely used outside of North America, although Common Criteria is expected in time to supersede it.

As legislation and regulations develop in different jurisdictions, a PKI based on a solid set of P&P can readily adjust to meet the most stringent mandatory requirements while at the same time retaining the flexibility to adapt to a variety of regulatory regimes.

Companies that span multiple jurisdictions and therefore need to take into account varying national requirements understand the criticality of establishing a sound and stable foundation from which to grow and adapt. This pertains directly to establishing trust for PKI and the capability of working across national boundaries for a truly global business. The foundation enables consistency through any number of PKI implementations.

The ultimate purpose of a PKI is to mitigate risk. The clear direction toward mandatory accreditation and audit serves this purpose by ensuring that there is evidence of trust and assurance in the PKI. Furthermore, the demand for a secure global economy will drive the resolution of incompatible requirements for PKI, deriving from varying international, national and regional legislative and regulatory regimes. SPYRUS has dedicated considerable resources to participating in standards development. SPYRUS standards specialists play lead roles in ISO Joint Technical Committee, sub-committee on IT security techniques, ISO technical committees on healthcare PKI and financial systems security, and a number of relevant IETF working groups.

4 Conclusion

An audit framework will help to ensure that an organization's PKI can be accredited against the developing international and vertical market systems. The PKI needs policy, and audit frameworks to encapsulate it. This is the total risk management framework within which a business can rely on the technology and on the processes in place that are tailored to its business objectives. This will include preparing the security infrastructure so that absolute trust exists in the root, and ensuring that the entire PKI system can be successfully audited for trust, assurance, and security, and accredited or certified under the relevant international standards or national legislation or regulations. SPYRUS professional services consultants can assist an organization in understanding the pertinent legal and jurisdictional framework, and establishing the appropriate audit environment.

About SPYRUS

SPYRUS, the High Assurance Security Systems Company for Global Business™, builds and deploys Public Key Infrastructure (PKI) system solutions for applications that demand customer-defined policy management, and strong audit, risk, and liability protection. As part of the Systems Solution, SPYRUS also offers the Rosetta line of security certified smart cards, readers and USB tokens for secure storage of digital certificates, personal identity information and security policies. SPYRUS is a privately held company headquartered in San Jose, California, with offices across the United States, Europe, and Australia. We welcome you to visit any of our offices to obtain more information about SPYRUS and its products and solutions, or to visit our Web site at www.spyrus.com.

