PKI NOTE

July 2001

CA Trust

Public Key Infrastructure provides a means for relying parties (i.e., recipients of certificates who act in reliance on digital signatures verified using those certificates) to know that another individual's public key actually belongs to that individual. Certification Authorities are those entities that initially authenticate the public key subscriber and issue the certificate for use by the relying parties. Independent verification that a certification authority operates using industry accepted standards for business disclosures and environmental, key management, and certificate management controls will enhance the TRUST in eCommerce. The PKI Forum endorses the standards embodied in the American National Standard (ANS) X9.79 *PKI Practices and Policy Framework*, and the American Institute of Certified Public Accounts' (AICPA) and Canadian Institute of Chartered Accounts' (CICA) standard *WebTrust*℠/™ *Program for Certification Authorities*. ANS X9.79 is currently under process to become an ISO standard. This endorsement is for the standards as adopted by their respective standards bodies and do not include any proprietary, organizational or other extensions and extrapolations from these standards.

PKI Forum Endorsements

The Business Working Group (BWG) of the PKI Forum established the Best Practices Working Group to propose a set of standards, policies and audit procedures that ensure the overall integrity, effectiveness and interoperability of trusted PKI-enabled implementations. At the Sydney meeting in December 2000, the Best Practices Work Group undertook to prepare its first items. Following that, members learned of the efforts of the ASC X9 and the widespread acceptance of the AICPA/CICA standard and concluded during the San Jose meeting in March 2001, that the professional and international standards that they were seeking already existed. The working group reviewed the parallel development efforts of the X9 Accredited Standards Committee (ASC X9) and the joint American Institute of Certified Public Accounts and the Canadian Institute of Chartered Accounts (AICPA/CICA) and formally endorses ANS X9.79 PKI Practices and Policy Framework and the WebTrust℠/™ Program for Certification Authorities.

The PKI Forum believes that the standards endorsed by the PKI Forum herein represent those policies, procedures and practices which are best used nationally and internationally. Thus, the PKI Forum will focus on these standards[1] and, working through its members, will influence these standards by reviewing documents, promoting comments

[1] The WebTrust standard, the multi-part X9.79 standard, and the anticipated ISO standard.

Acknowledgements

"CA Trust" is a deliverable from the PKI Forum's Best Practices Working Group. Several member organizations and individuals have contributed by providing content, editorial assistance and editorial reviews.

Primary Author:

Jeff Stapleton
KPMG, LLP

Contents

PKI forum

and recommending changes. These documents represent the consensual opinions of a vast number of corporations and governments internationally. Many of the PKI Forum members are X9 members, including AT&T, Baltimore, Certicom, Chrysalis-ITS, Digital Signature Trust Co., Entrust, IBM, KPMG LLP, nCipher, PricewaterhouseCoopers LLP, RSA Security, Securify, Spyrus, VeriSign, Visa International, and Wells Fargo Bank,. Therefore the PKI Forum was engaged in the development and balloting process which resulted in these standards, and thus the PKI Forum has already had some say in their establishment. PKI Forum endorsement will be reviewed as these standards evolve and the Forum will not otherwise endorse policies and practices not justified in these standards.

PKI Forum endorsement will be reviewed as these standards evolve and the Forum will not otherwise endorse policies and practices not justified in these standards.

Accredited Standards Committee X9

ASC X9 is the US standards committee for the financial industry services, whose mission is to develop, establish, publish, maintain, and promote standards for the Financial Services Industry in order to facilitate delivery of financial products and services.[1] X9 is accredited by the American National Standards Institute (ANSI).[2] ANSI is the US national standards body representing the US to the International Standards Organization (ISO). The X9 Secretariat is the American Bankers Association (ABA).[3] X9 is also the US Technical Advisory Group (TAG) to ISO Technical Committee 68 *Banking, securities and other financial services*.[4] The X9F5 working group developed ANS X9.79 *PKI Practices and Policy Framework* in cooperation with the AICPA/CICA Electronic Commerce Assurance Task Force.

American Institute of Certified Public Accountants

The American Institute of Certified Public Accountants is the national, professional organization for all Certified Public Accountants.[5] Its mission is to provide members with the resources, information, and leadership that enable them to provide valuable services in the highest professional manner to benefit the public as well as employers and clients. The joint AICPA / CICA Electronic Commerce Assurance Task Force developed in cooperation with the X9F5 working group the *WebTrust*SM/TM *Program for Certification Authorities.*

Canadian Institute of Chartered Accountants

The Canadian Institute of Chartered Accountants (CICA), together with the provincial and territorial institutes of chartered accountants, represents a membership of more than 66,000 CAs and 8,500 students in Canada and Bermuda. The CICA conducts research into current business issues and sets accounting and assurance standards for business, not-for-profit organizations and government. It issues guidance on control and governance, publishes professional literature, develops continuing education programs and represents the CA profession nationally and internationally.

[1] For more information, visit www.x9.org.

[2] For more information, visit www.ansi.org.

[3] For more information, visit www.aba.com.

[4] For more information, visit www.tc68.org.

[5] For more information, visit www.aicpa.org.

ANS X9.79-2000 PKI Practices and Policy Framework

The ANS X9.79-2000 PKI Practices and Policy Framework is an American National Standard that defines the components of a PKI and sets a framework of practices and policy requirements for the operation of a PKI. The standard draws a distinction between PKI systems used in open, closed and networked environments. It further defines the operational practices relative to industry accepted information systems control objectives. PKI practices implementing this standard can support multiple polices that incorporate the use of digital signature technology. The standard allows for the implementation of operational, baseline PKI practices ("practices") that satisfy industry accepted information systems control objectives.[6]

PKI practices implementing the ANS X9.79-2000 standard can support multiple polices that incorporate the use of digital signature technology.

In §7.2 Certification Practice Statements of X9.79, requirement 4. reads as follows: "Certification practices SHALL comply with the control objectives specified in Annex B: Certification Authority Control Objectives." The contents of Annex B draws heavily from the following documents, listed in alphabetical and numerical order:

- ANS X9.57 *Certificate Management*
- ANS X9.80 (draft), *Prime Number Generation, Primality Testing, and Primality Certificates*
- British Standard (BS) 7799-1999 *Code of Practice for Information Security Management*, also known as ISO/IEC DIS 17799-1999, *Information Security Management*, Part 1: *Code Of Practice For Information Security Management*.
- Federal Information Processing Standard 140-1, *Security Requirements for Cryptographic Modules*
- Internet Engineering Task Force (IETF), RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, also known as PKIX-4.
- ISO 10202-1991, *Financial transaction cards - Security architecture of financial transaction systems using integrated circuit cards*, Part 1: *Card life cycle*
- ISO 11568-1998, *Banking – Key Management (retail)*, Part 4: *Key management techniques using public-key cryptography*, and Part 5: Part 5: *Key life cycle for public key cryptosystems*
- ISO 13491-1 (draft), *Banking – Secure Cryptographic Devices (Retail)*, Part 2: *Security Compliance Checklists for Devices used in Magnetic Stripe Card Systems*
- ISO 15782 *Banking – Certificate Management*, Part 1: *Certificate Management*
- National Automated Clearing House Association (NACHA), Internet Council's *Certification Authority Rating and Trust* (CARAT).

The *Certification Authority Control Objectives* are organized into three sections, B.1 *CA Environmental Controls*, B.2 *Key Management Life Cycle Controls*, and B.3 *Certificate Life Cycle Controls*. Annex B.1 *CA Environmental Controls* contains 11 detailed control objectives, with 165 comprehensive control procedures. Annex B.2 *Key Management Life Cycle Controls* contains 9 detailed control objectives, with 67 comprehensive control procedures. Annex B.3 *Certificate Life Cycle Controls* contains 9 detailed control objectives, with 115 comprehensive control procedures. These control objectives and procedures are suitable for use by a professional audit practitioner to assess a public key infrastructure.

Certificate Life Cycle Controls *contains 9 detailed control objectives, with 115 comprehensive control procedures. These control objectives and procedures are suitable for use by a professional audit practitioner to assess a public key infrastructure.*

[6] ANS X9.79-2000, §1. Scope

WebTrust[SM/TM] Program for Certification Authorities

The WebTrust[SM/TM] Program for Certification Authorities provides a framework for licensed WebTrust practitioners to assess the adequacy and effectiveness of the controls employed by Certification Authorities (CAs). The public accounting profession has developed and is promoting a set of principles and criteria for CAs. Public accounting firms and practitioners, who are specifically licensed by the AICPA/CICA can provide assurance services to evaluate and test whether the services provided by a particular Certification Authority meet these principles and criteria. The posting of the WebTrust seal of assurance for Certification Authorities is a symbolic representation of a practitioner's unqualified report certifying the conformance of that CA to the WebTrust requirements. In addition, any interested party and in particular those who rely on the digital certificates (and certificate status information) issued by the Certification Authority can click on the WebTrust seal to view the practitioner's report.

The Certification Authority criteria is organized into three principles:

- CA Business Practices Disclosure

  The Certification Authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.

  This principle has 4 disclosure criteria addressing general disclosures, key life cycle management disclosures, certificate life cycle disclosures, and CA environmental disclosures with 45 illustrative disclosures that are harmonized with the ANS X9.79 standard.

- Service Integrity

  The Certification Authority maintains effective controls to provide reasonable assurance that;
  - Subscriber information was properly authenticated (for the registration activities performed by a certification authority).
  - The integrity of keys and certificates it manages is established and protected throughout their life cycles.

  This principle has 9 key management life cycle criteria, with 67 illustrative controls, and 9 certificate life cycle criteria, with 121 illustrative controls, that are harmonized with the ANS X9.79 standard.

- CA Environmental Controls

  The Certification Authority maintains effective controls to provide reasonable assurance that:
  - Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure.
  - The continuity of key and certificate life cycle management operations is maintained.

The posting of the WebTrust seal of assurance for Certification Authorities is a symbolic representation of a practitioner's unqualified report certifying the conformance of that CA to the WebTrust requirements.

- CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.

This principle has 11 CA environmental criteria with 165 illustrative controls that are harmonized with the ANS X9.79 standard.

The WebTrust standard also includes a complete set of example practitioner reports for use in the United States and Canada. This standard has also been adopted by the public accounting profession of other countries, including Australia, Austria, Argentina, Denmark, England, Hong Kong, Ireland, Japan, Netherlands, Scotland, Spain, Germany, and France. Furthermore, the Microsoft Corporation is working with the AICPA/CICA task force to develop the Microsoft Program for Certification Authority Qualification, based on the WebTrust criteria.

Prior to the existence of the WebTrust standard, the Statement on Auditing Standards (SAS) 70 has been used as the reporting vehicle for an audit of a Certification Authority, and is still required by some state legislature today. However, the purpose of the SAS 70 is auditor-to-auditor communication, whereas the WebTrust standard is an auditor to interested parties communication based on the Statements on Standards for Attestation Engagements (SSAE, U.S.) and Standards for Assurance Engagements (SAE, Canada). A table highlighting the differences between a WebTrust for Certification Authorities and SAS NO. 70 and Section 5900 engagements is provided in Appendix E of the WebTrust standard.

Copyright Statement

This Note and all other materials printed by the PKI Forum are property of the PKI Forum and may not be copied without express consent from the PKI Forum. © 2001 PKI Forum, Inc.

About PKI Forum

The PKI Forum is an international, not-for-profit, multi-vendor and end-user alliance whose purpose is to accelerate the adoption and use of Public-Key Infrastructure (PKI).

The PKI Forum advocates industry cooperation and market awareness to enable organizations to under-stand and exploit the value of PKI in their e-business applications.

Web: http://www.pkiforum.org
e-Mail: info@pkiforum.org
Phone: +1 781 876 8810