Akamai
FASTER FORWARD

Commonly Accepted Security Practices and Recommendations (CASPR)

June 2015

Table of Contents

CASPR

CASPR is an open-source project aimed at documenting the information security common body of knowledge through commonly accepted practices and recommendations. This project draws on the experience of volunteer security professionals to develop a comprehensive and freely distributable body of information security standards.

The CASPR web site is http://www.caspr.org

FIPS 140-2: Security Requirements For Cryptographic Modules

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce This United States standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-2 and other cryptography based standards. In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested.

Akamai uses the OpenSSL source code as the basis of the SSL modules. The OpenSSL organization was considering FIPS certification and Akamai has not pursued independent certification of OpenSSL, OpenSSH, and Akamai's internal algorithm implementations.

The NIST web site is http://www.nist.gov

Federal Information Security Management Act (FISMA)

FISMA refers to the Federal Information Security Management Act of 2002 Subchapter III, Chapter 35 of title 44, United States Code). FISMA requires that agencies develop and maintain an "Information Security Program" to ensure the appropriate security level through policies, procedures, periodic assessments, etc. Agencies must also report annually on the adequacy and effectiveness of their information security activities. NIST is task with developing and publishing security related standards and guidelines.

The NIST web site is http://www.nist.gov

Gramm-Leach-Bliley (GLBA)

Gramm-Leach-Bliley (GLBA) is U.S. Law, the Financial Services Modernization Act, created to improve consumer financial services. The law is a series of rules and guidelines were established by several federal agencies for implementation. The rules and guidelines are to assure people that the confidentiality and privacy of financial information electronically collected, maintained, used, or transmitted is secure – especially when financial information can be directly linked to an individual.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 was created to improve the US health care system enabled by the nation’s four million-plus health plans and 1.2 million-plus providers. A series of rules were developed and issued by the Department of Health and Human Services, mandating standards-based implementations of HIPAA by all health care organizations that create, store or transmit electronic protected health information. With Department-specified deadlines are various civil penalties, including fines and/or imprisonment for non-compliance.

The level of appropriate control for HIPAA conformance varies from use case to use case, and Akamai's platform allows for the implementation of specific controls to assist in meeting regulatory requirements.

Akamai works with each of its customers to understand their specific needs and implement the correct and appropriate controls.

IEC 15408:1999 – (Common Criteria) Information Technology – Security Techniques – Evaluation Criteria for IT Technology

An internationally recognized standard, often referred to as the Common Criteria, for defining the criteria to be used as the basis for evaluation of security properties of IT products and systems, e.g., firewalls. Typically, these products are purchased by government agencies in the United States and in other countries.

Evaluation is the process (performed by an authorized laboratory) of comparing the product to the standards and hopefully finding that the product is in compliance. A Certification Board (usually a government body in the country where the evaluation is performed) oversees the reviews the laboratory's work and if everything is in order, certifies the product.

Akamai feels that Common Criteria is not an appropriate standard to measure Akamai's security position or evaluating the security aspects of of a service such as Secure Content Delivery.

The ISO web site is http://www.iso.org

ISO/IEC 27002 – Information Technology Code of Practice for Information Security Management

ISO/IEC 27002 is an internationally recognized standard for information security management, that provides a common basis for developing organizational security standards and effective security management practices.

The standard was originally developed as BS7799, published in the mid-1990's. The British Standard was adopted by ISO/IEC as ISO/IEC 17799:2000, revised in 2005, and renumbered (but otherwise unchanged) in 2007 to align with the other ISO/IEC 27000-series standards.

As with all major standards, ISO 17799 is periodically reviewed and updated. The most recent version of ISO 17799 was released in 2005. It provides for detailed analysis of the following topic areas:

- Security Policy
- Organizing Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

The Akamai Information Security Management System (ISMS) is structured in accordance with the standard and Akamai annually undergoes a readiness assessment to determine compliance by a 'big four' consulting firm or a reputable equivalent thereto (currently PricewaterhouseCoopers).

For additional Q&A information see the InfoSec FAQ

Certification

Certification demonstrates to competent authorities that the organization observes all applicable laws and regulations. In this matter, the ISO 17799 standard complements other existing standards and legislation, for example: HIPAA, the Gramm-Leach-Bliley, Sarbanes-Oxley, and Federal Information Security Management Act.

In the commercial marketplace Certification can helps set the company apart from its competitors by providing credibility and confidence to partners and customers. Akamai already has contracts that require annual assessment for confromance to ISO 17799.

ISO/IEC 17799:2005 (Part 1) is the standard code of practice derived from British Standard BS7799 Part 1. ISO 17799 is not yet a certification standard.

BS7799-2: 1999 (Part 2) is a standard specification for how to implement and maintain an Information Security Management Systems (ISMS). BS7799-2 basically explains how to apply and implement BS7799- 1 and ISO 17799.

Note that BS7799-2:1999 has been withdrawn and certification will be for ISO 27001:2005.

The ISO web site is http://www.iso.org

ISO/IEC 27001:2005 – PCI PAYMENT CARD INDUSTRY SECURITY REQUIREMENTS

Formerly was the Visa U.S.A. Cardholder Information Security Program (CISP). The PCI Data Security Requirements applies "to all Members, merchants, and service providers that store, process, or transmit cardholder data." Additionally, these security requirements apply to all "system components" which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including both internal and external (web) applications.

Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. The account number is the critical component that makes PCI applicable. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data, however, PCI applies even if the only data stored, processed, or transmitted is account numbers.

The PCI web site is www.visa.com

SAS 70

The Statement on Auditing Standards No. 70, Service Organizations, or SAS 70, is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA). The primary purpose of this standard is to allow organizations to disclose information regarding their control activities and processes to customers (and customer auditors) in a uniform format. SAS 70 does not require any particular controls or practices, but involves a review of the existing

controls utilizing industry standards for audit. At the conclusion of the examination, a "Service Auditor's Report" is issued wherein the independent auditor will offer an opinion regarding the effectiveness of existing controls.

While customers have requested an SAS70 report for the Sarbanes-Oxley compliance Akamai is principally an intermediary service provider for businesses, acting as a conduit for the transmission of data. As such, Akamai itself does not perform financial service transaction processing for its customers. Therefore, while Akamai does retain external firms to perform audits of our financial statements, we do not retain auditors to perform SAS 70 reports of our services, systems, and network infrastructure.

For additional Q&A information see the InfoSec FAQ

The AICPA web site is http://www.aicpa.org

SB-1386, CA 1798 – Personal Information: Privacy

California Senate Bill No. 1386 added Sections 1798.29, 1798.82 and 1798.84 to the California Code of Civil Procedure. The California state law, often referred to as either SB-1386 or CA 1798, was created to combat identity theft and to ensure that California residents are promptly notified in the event that their personal information is accessed improperly through a security breach. The law applies to any company doing business in California that maintains certain information about California residents in computerized form, even if the computer or servers on which the information is stored are not located in California or if the computers or servers belong to an independent third party.

For additional Q&A information see the InfoSec FAQ

SOX – Sarbanes-Oxley

Sarbanes-Oxley is a complex set of regulations covering multiple areas of corporate governance, including corporate responsibility, executive compensation, board composition, audit, and internal controls.

As a publicly traded company, Akamai is required to meet Sarbanes-Oxley requirements, and our auditor's statements are a matter of public record.

Akamai's SEC Filings area available on Akamai's website: https://www.akamai.com/.

Alternatively, any investor could go to the SEC's web page and query Edgar report filings made by Akamai.

Akamai does not, at this time, have separate customer-facing Sarbanes-Oxley statements.

BS25999 Standard for Business Continuity Management (BCM)

The British Standard for Business Continuity (BS25999) was published by BSI at the end of 2006. The standard is intended to support business continuity requirements of ISO 17799 and ISO 27001.

BS 25999 will be published in two parts:

BS 25999-1:2006 is a code of practice that takes the form of guidance and recommendations. It establishes the process, principles and terminology of business continuity management (BCM).

BS 25999-2:2007 will specify the process for achieving certification that business continuity capability is appropriate to the size and complexity of an organization.

The contents of the code of practice (BS 25999-1) are as follows:

- Scope and applicability
- Terms and definitions
- Overview of business continuity management
- The business continuity management policy
- BCM programme management
- Understanding the organization
- Determining business continuity strategy
- Developing and implementing a BCM response
- Exercising, maintaining, and reviewing BCM arrangements
- Embedding BCM in the organization's culture

.

As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move *faster forward*, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.