ISO 19092: A Standard for Biometric Security Management

By Phillip H. Griffin

Organizations that rely on biometric technology need to protect and manage the security of their biometric assets.

Biometric systems security and the management of biometric information security must become integrated into the organization's overall information security management program. This program should be based on policy defined to meet the business objectives of the organization, and a risk-based approach should be used to select and impose proper controls and monitor their effectiveness.

A Biometric Information Security Management System (ISMS) includes the biometric policy, security practices, operational security procedures, organizational structure, assigned responsibilities, and resources needed to protect biometric assets. Independent reviews of security practices should ensure that they are consistent with the biometric policy, and that adequate and effective controls are in place.

Formal mechanisms should be used to document and report biometric system events, including system malfunctions and other security incidents. Incident management results and metrics gathered from biometric event journals should be used in the review process to cause controls to be re-evaluated over time. One goal of adopting an ongoing, systematic approach is for these activities to cause the Biometric ISMS to be continuously improved.

A standard for Biometric ISMS

An information security management program to protect biometric assets is a prudent business practice that helps an organization identify and manage risk. A new biometric security standard, ISO 19092[1], provides a technology-specific extension to the ISO/IEC 17799 *Code of practice for information security management*[2]. Though developed in the financial services, ISO 19092 is a general-purpose standard that can be used by any industry that employs biometric technology as a policy-based authentication mechanism.

ISO 19092 defines core requirements for managing and securing biometric information for all applications and environments where biometric information is used. These requirements apply to the transmission and storage of biometric information. Validation of a biometric system relies on maintenance of a secure biometric event journal that can be used for legal and regulatory compliance and ISMS audit.

Core requirements can be met using physical protection when all biometric system components reside within the same tamper-resistant unit and there is no transmission of biometric information. Outside of this environment, requirements can be met using cryptographic mechanisms, such as a digital signature and encryption, to protect biometric information.

The standard defines control objectives and security controls that can be augmented or trimmed to meet the specific needs of an organization. Its protocols, security techniques and message syntax can be applied by software applications to automate enforcement of biometric information security policy. By binding the biometric security policy and practices identifiers to the biometric reference template[3], applications using biometrics can transform biometric information into policy-based management action.

For example, ISO 19092 requires that when a template is terminated, the termination request be processed and validated in accordance with the requirements of the Biometric Policy (BP) and Biometric Practice Statement (BPS) identified in the template. The BP and BPS specify who is authorized to terminate a template, the circumstances under which a template may be terminated, and the circumstances

1 ISO 19092 (All parts) Financial Services – Security – Biometrics

2 ISO/IEC 17799:2005 (2nd edition) Information technology – Security techniques – Code of practice for information security management

3 The reference template is biometric measurement data extracted from the biometric sample of an individual enrolling in a biometric system, and stored for later use by the system for comparison against data extracted from subsequently submitted biometric samples.

under which a template shall be terminated. A biometric template termination application can use the template BP and BPS identifiers as inputs that control the termination process.

Biometric Policy

A Biometric Policy (BP) is a set of rules that indicate the applicability of a biometric reference template for use by some community or class of applications that have common security requirements. Each BP is a document identified by a globally unique name, an information object identifier assigned by the organization[4]. BP identifiers can be bound cryptographically to a biometric reference template using a digital signature.

Biometric Policy identifiers can be bound cryptographically to a biometric reference template using a digital signature.

This cryptographic binding makes it possible for software applications to recognize and enforce the biometric security policy appropriate for a given template. A BP identifier may indicate that a template may be used to control access to customer or employee information and assets, or to authenticate a person acting in some role or engaging in some restricted activity. A BP identifier may indicate security requirements and conditions under which a biometric may be used, such as only with a valid pass phrase.

ISO 19092 defines a schema for representing BP information, and specifies cryptographic processing for binding this information to a biometric reference template. The BP information can be carried explicitly in a template by using a biometric policies extension, or implicitly associated with a template as an authenticated attribute that is bound to, but detached from, the template. In either case, a digital signature is used to bind BP information to a biometric reference template.

The BP schema defines a biometric security policy as a series of one or more biometric policy objects. Each object contains the biometric policy identifier assigned to a biometric security policy document by an organization. When more than one BP is carried in a biometric policies extension, it is appropriate to use the associated biometric template according to any of the policies included in the extension.

The biometric security policy object may optionally include the hash of the policy document and a Uniform Resource Identifier (URI) that points to the document or to additional information[5]. Including the hash and URI in the policy object provides using applications with a network policy resource that allows policy information to be made available to relying parties. When bound to biometric reference templates, the BP will be included in biometric event journal entries and available for the incident management and Biometric ISMS reviews.

4 ISO/IEC 9834-8 | ITU-T Rec. X.667, Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: Generation and Registration of Universally Unique Identifiers (UUIDs) and their Use as ASN.1 Object Identifier Components

5 IETF, *RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax*, T. Berners-Lee, R. Fielding, L. Masinter, August 1998. http://www.ietf.org/rfc/rfc2396.txt

Biometric practices

A Biometric Practice Statement (BPS) describes the security practices that an organization follows during the biometric reference template life cycle, including the business, legal, regulatory and technical considerations. Each BPS document is identified by a globally unique name, an information object identifier assigned by the organization. Like BP identifiers, BPS identifiers can be cryptographically bound to a biometric reference template, making it possible for software applications to recognize and enforce the biometric security practices associated with a given template.

While a BP is often a single, public document that consists of only a single page, BPS documents are not public and are less abstract. BPS documents are general-purpose and more technical in nature. They are technology-neutral, but may be applicable to specific biometric technologies or limited to well-bounded systems and applications within the organization.

Biometric ISMS control objectives

ISO 19092 defines Biometric ISMS control objectives that can serve as the criteria for the evaluation and audit of a biometric security system. These criteria represent recommended practices for the operation and technical use of biometric technology within an organization. An existing ISMS may already specify some of the security policies and practices needed to meet these objectives.

Three types of control categories are identified in ISO 19092. These are biometric information life cycle, environmental, and key management life cycle controls. The security of a biometric system implementation that resides within or relies upon an Information and Communication Technology (ICT) infrastructure requires environmental controls. If the security of the implementation depends on cryptographic protection, key management life cycle controls are necessary.

The life cycle of biometric information in a biometric system is analogous to the life cycle for digital identity certificates. Individuals are enrolled in the system by the capture of their biometric data, and this data is used to generate a biometric reference template, which is then distributed, used and eventually terminated and archived.

A biometric information security management program should establish control objectives for the biometric information life cycle. These control objectives should cover the biometric enrollment process, the biometric authentication process, the biometric reference template life cycle, and the biometric device life cycle.

Organizations should establish and maintain controls to ensure that the biometric enrollment process properly identifies enrollees and reliably authenticates their claimed identities. Controls should ensure that only authorized enrollments occur, and that the biometric data of the enrollee is accurate and complete.

The biometric authentication process includes identification of individuals and verification of a claimed identity. Both processes must be performed securely and in accordance with parameters specified by the biometric security policies and practices of the organization.

Throughout their life cycle, controls must be in place to ensure that biometric reference templates are properly handled. They must be securely and properly generated, then validated prior to their distribution and use. Reference templates must be securely transmitted and stored, and properly terminated. These security requirements

must cover any period in which a template may be archived after termination and no longer in active use.

Controls must be in place to ensure that biometric devices are properly handled throughout their life cycle. Only authorized individuals may be allowed access to biometric devices, and operational security procedures must be in place to ensure that biometric devices function properly. The settings of biometric devices should be established by security practices and monitored using metrics from the biometric event journals.

When biometric technology is added to an ICT infrastructure managed by an existing ISMS, sufficient environmental controls to protect the security of biometric systems may already be in place. These can be applied to the protection of biometric assets. For environmental controls, a given implementation may require control objectives and control criteria for:

- The information security policy and infrastructure
- Biometric asset classification and management
- Personnel security management
- Physical security
- Operations and systems access management
- Systems development and maintenance
- Business continuity management
- Legal and regulatory monitoring and compliance
- Journaling of significant environment events

Some biometric technology must be protected by cryptography. If this technology is added to an infrastructure reliant on cryptographic techniques and managed by an existing ISMS, sufficient key management life cycle controls may already be in place, and these can be applied to the protection of biometric assets. For key management life cycle controls, a given implementation should consider control objectives and control criteria for:

- Cryptographic key generation
- Storage
- Backup
- Recovery
- Distribution and usage
- Destruction and archival
- The life cycle of cryptographic devices

Biometric event journal

A biometric event journal is a series of biometric system event records, each containing a single journal entry. Journal entries provide an audit trail containing evidence of the consistency and accuracy of the authentication system. To be of value in an information security management program, journal entries must be protected by physical or cryptographic means. Each journal entry may be digitally signed so that intentional and unintentional tampering can be detected, and the source of the journal entry can be authenticated.

Maintaining a biometric event journal for compliance and audit purposes is a core security requirement of ISO 19092. The standard promotes the management of biometric information as part of an overall information security management program. Compliance with the standard can be demonstrated by the periodic validation of the biometric system against the Biometric ISMS policy, practices and procedures of the organization.

When ISO 19092 is used as a technology-specific extension of ISO/IEC 17799, biometric system validation becomes part of the "Check" function activity in a Plan–Do–Check–Act (PDCA) model. Metrics gathered from event journal entries and event journal summary records can be used to improve the Biometric ISMS, and to measure the effectiveness of the policy, practices and procedures of the organization over time.

ISO 19092 specifies record format and cryptographic processing requirements for the capture of validation materials. The event journal schema is extensible, and defined as an abstract syntax that supports a compact, efficient binary format and verbose, human-readable XML markup[6].

Supporting two journal representations allows the capture of biometric events in resource-constrained and high-volume transaction environments. Since every binary value has an equivalent XML markup representation, binary journal entries are easily converted to their XML counterparts for display or subsequent processing and analysis.

Any organization with a need can define new journal event records, and each of the event journal record types defined in ISO 19092 can be extended to include additional information. The standard specifies the following thirteen types of event records:

- Enrollment event records document each successful enrollment in a biometric system. These journal entries should be signed by an authorized enroller to ensure the integrity of enrollment information, and to authenticate the origin of the enrollment event.
- Enrollment failure event records document each failure to enroll in a biometric system. These journal entries should be signed by an authorized enroller to ensure the integrity of enrollment failure information, and to authenticate the origin of the enrollment failure event.
- Identification event records document each successful identification in a database of biometric reference templates, and may provide evidence for non-repudiation. These journal entries should be signed to ensure the integrity of identification information, and to authenticate the origin of the identification event.
- Identification failure event records document each failed attempt to identify an individual in a database of biometric reference templates. These journal entries should be signed to ensure the integrity of identification failure information, and to authenticate the origin of the identification failure event.
- Verification event records document each successful verification of a claimed identity, and may provide evidence for non-repudiation. These journal entries should be signed to ensure the integrity of verification information, and to authenticate the origin of the verification event.
- Verification failure event records document each failed verification of a claimed identity. These journal entries should be signed to ensure the integrity of verification failure information, and to authenticate the origin of the verification failure event.

6 Extensible Markup Language (XML) 1.0 (Third Edition), 1994-2003. World Wide Web Consortium (W3C®) (Massachusetts Institute of Technology, European Research Consortium for Informatics and Mathematics, Keio University) W3C Recommendation 04 February 2004. http://www.w3.org/TR/2004/REC-xml-20040204/

- Termination event records document the termination of biometric reference templates. These journal entries should be signed to ensure the integrity of termination information, and to authenticate the origin of the entity requesting template termination.
- Addition event records document every addition of biometric information to a biometric reference template storage system. These journal entries should be signed by the entity authorized to perform the operation.
- Deletion event records document every deletion of biometric information from a biometric reference template storage system. These journal entries should be signed by the entity authorized to perform the operation.
- Modification event records document modifications made to information in a biometric reference template storage system. These journal entries should be signed by the entity authorized to perform the operation.
- Injection event records document the injection of biometric reference templates into secure tokens, when tokens are issued for distribution to enrollees. These journal entries should be signed by an authorized enroller to ensure the integrity of injection information, and to authenticate the origin of the injection event.
- Summary event records contain totals of event journal entry types over time, and can be used to monitor operation of a biometric system. These records should be produced daily and checked for unexpected or unusual activity.
- Archive event records are added to biometric event journals when they are deactivated. The archive event information should identify the preceding archive and the current active journal.

Conclusion

A policy-based biometric information security management program should be integrated into the organization's overall ISMS to protect and manage the security of their biometric assets. Proper controls should be established for biometric systems and the management of biometric information. Systematic security reviews should be performed on a regular basis to monitor the effectiveness of the program and ensure compliance to the organization's security policies, practices and procedures. A secure biometric event journal should be used to improve the Biometric ISMS, and to measure the effectiveness of the organization's policy, practices and procedures over time.

About the Author

Phillip H. Griffin is principal of GRIFFIN Consulting, *an information security services company located in Raleigh, North Carolina, USA, and specializing in secure software design, development and project management, national and international security standards committee representation, and the management and development of information security standards. He currently serves as liaison from ISO/IEC JTC 1/SC 27* IT Security Techniques *to the biometrics working group of ISO TC 68/SC 2* Financial Services Security, *and as editor of the ISO 19092 biometric information management and security standard and the ISO 22895 cryptographic message syntax standard. He can be reached at phil@phillipgriffin.com.*

Join ISSA Now!
Visit www.issa.org
or email issa_membership@issa.org

Information security awareness and training for all your audience groups...

Easy i offers a complete range of customizable solutions available in multiple languages for:

- General Awareness
- New Hires/Contractors
- Managers/Executives
- IT/IS Specialists

Visit our website and view a FLASH DEMO or contact us:

North America
310-414-0731
email: info@easyi.com

Europe
+44 (0)1926 854111
email: info@easyi.co.uk

Asia Pacific
+61 2 8206 6357
email: info@easyi.com.au

Easy *i*
An SAI Global Company

www.easyi.com/is
from information to understanding