

STATE OF ALABAMA

Information Technology Standard

STANDARD 623S2-00: AUTHENTICATION - BIOMETRICS

A biometric system is an automated system capable of capturing a biometric sample from an end user, extracting biometric data from the sample, comparing the biometric data with that contained in one or more reference templates, deciding how well they match, and indicating whether or not verification of identity has been achieved. Depending upon the biometric technology and the risk environment, using biometrics to supplement other authentication factors will very likely enhance security.

OBJECTIVE:

This standard supports State IT Policy 623: Authentication, and provides the minimum requirements for biometric authentication implementation.

SCOPE:

These requirements apply to all Executive Branch agencies, boards, and commissions except those exempt under The Code of Alabama 1975 (Title 41 Chapter 4 Article 11).

REQUIREMENTS:

A biometric may not be used for identification or to verify an identity in single factor authentication. A biometric may be used for authentication only as a component of two or three factor authentication.

Where biometric authentication is used, the following security controls shall be implemented:

MANAGEMENT CONTROLS

IT Managers shall ensure that individuals are assigned to the following administrative roles:

- Enrollment Administrator – the individual who verifies the identity of new users and guides them through the creation of their associated biometric reference templates using the biometric capture device.
- Security Administrator – the individual who establishes and modifies the values of configuration parameters in the biometric software.
- Audit Administrator – the individual who reviews audit logs for security violations and related suspicious behavior.

IT Managers shall maintain lists of individuals authorized to perform each of the following functions: enroll or re-enroll users; modify the security configuration; and review and manage audit logs.

IT Managers shall ensure that the following functions are restricted to authorized Administrators:

- Creation or modification of authentication rules
- Creation, installation, modification or revocation of cryptographic keys
- Startup and shutdown of the biometric service

IT Managers shall ensure that only authorized Enrollment Administrators are permitted to create user biometric templates.

IT Managers shall ensure that only authorized Audit Administrators can clear the audit log or modify any of its entries.

IT Managers shall ensure that all Administrators must authenticate to the biometric system to perform administrative functions and that this authentication must include a factor outside of the biometric verification the system supports for other users.

ENROLLMENT CONTROLS

In no case shall the strength of the authentication required in the enrollment process be less than the strength of authentication required during the verification process because this begs for an attack on the enrollment process.

IT Managers shall ensure that the enrollment process is conducted by an authorized Enrollment Administrator who will at a minimum check that the enrollee has submitted all required documentation used to authorize access to the system for which the biometric system supports authentication, and ensure the enrollee presents a valid photo ID.

IT Managers shall ensure that users cannot self-enroll biometric information (i.e., enroll outside of the presence of an authorized Enrollment Administrator).

Potential enrollees who do not have the physical characteristics needed to provide the intended biometric sample shall be offered an authentication alternative that does not pose an undue burden on the enrollee, nor creates an inherent weakness in the authentication process that could be easily impersonated or exploited.

To protect against the threat of a poor biometric template, there must be some form of quality control during the initial capture process. Good biometric software will prohibit the creation of clearly inadequately specified templates, however, there is a possibility of a marginal template entering the system (i.e., just good enough to pass quality criteria, but still noisy enough to be susceptible to a sophisticated attack).

IT Managers shall ensure that Enrollment Administrators receive appropriate training that covers, at a minimum:

- The user identification and authorization requirements
- How to use the biometric software and capture device to obtain an acceptable user template
- How to identify when a template is unacceptable and needs to be recreated

Enrollment Administrators shall re-create templates when there is an indication that a template has not been properly captured.

The Security Administrator shall configure the system to search for matches between the enrolled template and previously existing templates and reject enrollment when a match is discovered. If this process cannot be automated, the Enrollment Administrator shall enforce this requirement manually.

VERIFICATION CONTROLS

Verification is the process that supports routine user authentication. A user seeking physical or logical entry presents a live biometric sample to a capture device, which extracts a digital representation of the sample and transfers it to a comparator.

False Acceptance and False Rejection:

The central risk of the verification process is that the technology will mistakenly verify a user's identity when that person is actually someone else – known as *false acceptance*. Human beings are constantly changing (we age, gain and lose weight, sustain injuries, modify behavior, etc.) therefore biometric systems must have some tolerance for error or common everyday changes in individuals would lead to *false rejection*.

There is a tradeoff between the *false acceptance rate* (FAR) and *false rejection rate* (FRR). A high FAR means that security may be unacceptably weak; a high FRR means that the technology is likely to be a significant nuisance to falsely rejected users.

- The Security Administrator shall set the FAR to be no greater than 1 in 100,000.
- The Security Administrator shall set the FRR to be no greater than 5 in 100.

Inevitably, there will be some false rejections that require intervention to allow proper access (e.g., the recently injured user). IT Managers shall designate personnel who have the authority to override false rejections and ensure that they receive proper training in how to implement the fallback protocol and verify a user's identity.

Liveness Checks:

Most leading biometric solutions have "liveness" checks that take some action to validate that the sample is coming from a live human being and not a facsimile.

- The Security Administrator shall activate at least one of the available "liveness" checks.
- IT Managers shall document alternative identification and authentication procedures for users that are unable to present the required live biometric sample (such as when a user has a disability or injury).

Failure to Match:

The Security Administrator shall configure the biometric system to:

- Lock out for 15 minutes any user upon the third unsuccessful authentication attempt within a 15-minute period
- Prohibit the identical biometric sample from being used in consecutive authentication attempts
- Not reveal to a user any information related to how close the live sample he or she supplies is to the corresponding biometric template

Exact Matches:

An "exact match" occurs when the digital representation of the live sample extracted from the capture device is identical to the stored biometric template to which it is compared. In most applications, an exact match is a good thing, but in biometrics, it is cause for suspicion. There is inherent variability in the sample capture process that makes exact matches unlikely for many biometric technologies. When one occurs, it may be indicative that someone has improperly obtained the biometric template and is staging a replay attack.

To mitigate the risk of bypass and replay, IT Managers shall ensure that there is adequate physical security, encryption of transmitted data, monitoring, and rejection of "exact matches".

IT Managers shall ensure that the physical connections between the following biometric system components are adequately secured:

- The connection between the capture device and the comparator.
- The connection between the comparator and the biometric-supported access control system.

FALLBACK CONTROLS

Fallback is the condition that occurs when the biometric system is not in use. In some cases, the biometric technology provides partial fallback mechanisms within the system itself. These approaches should be employed whenever feasible.

IT Managers shall ensure that any override of the biometric system is accompanied by a photo ID check of the user and documentation of the following:

- The name of the user who was granted entry with the override
- The time the override occurred

- The reason for the false rejection

IT Managers shall establish adequate identification and authentication procedures that must be followed whenever the biometric system is unavailable.

TECHNICAL CONTROLS

The Security Administrator shall ensure biometric templates are protected by operating system permissions.

The Security Administrator shall ensure that no user ID has access to the files other than those required for running the biometric application software.

Encryption:

The Security Administrator shall:

- Ensure that the biometric system is encrypted in accordance with State standards.
- Ensure that only the process running biometric software is able to read relevant private or shared secret keys (with the exception of key super-session events during which the Security Administrator may temporarily have the ability to replace the key [e.g., to modify the key file]).

The Security Administrator shall configure the biometric system to:

- Encrypt and digitally sign all biometric data before it is transmitted from one physical device to another.
- Encrypt all biometric data resident on non-volatile memory or storage media.

Monitoring and Auditing:

IT Managers shall ensure that the file permissions and storage scheme for biometric audit logs is no less secure than the scheme for the system audit logs of the operating system on which the biometric software resides.

The Security Administrator shall configure the biometric system to audit the following transactions:

- All "exact match" verification transactions
- All failed identification or authentication attempts
- All start and stop events for the biometric service

ADDITIONAL INFORMATION:

Information Technology Policy 623: Authentication

http://cybersecurity.alabama.gov/documents/Policy_623_Authentication.pdf

Information Technology Standard 623S2: Authentication – Biometrics

http://cybersecurity.alabama.gov/documents/Standard_623S1_Authentication-Passwords.pdf

Information Technology Dictionary

http://cybersecurity.alabama.gov/documents/IT_Dictionary.pdf

By Authority of the Office of IT Planning, Standards, and Compliance

DOCUMENT HISTORY:

Version	Release Date	Comments
620-03	1/12/2007	Original document
620-03_A	10/28/2008	Added biometric requirement from Authentication policy (Section 4; first paragraph)
623S2-00	09/01/2011	New number and format