Identity Proofing and Authentication Policy

Purpose

The purpose of the Crowley Enterprises Identity Proofing and Authentication Policy is to establish the requirements necessary to ensure that individuals with the authorization to access and use Crowley Enterprises Information Resources are given that access only after their identity has been established and they have provided authentication commensurate to the access they require.

Audience

The Crowley Enterprises Identity Proofing and Authentication Policy applies to individuals who are responsible for managing Crowley Enterprises Information Resource access, and those granted access privileges, including special access privileges, to any Crowley Enterprises Information Resource.

Contents

|  |  |
| --- | --- |
| Identity Proofing  [Authentication](#_Account_Management)  Authenticator Management  Federation | [Definitions](#_Remote_Access)  References  Enforcement |

Policy

Identity Proofing

* A user will be given an Identity Assurance Level based on what level of identity assurance is needed for access to the related resource after they have asserted their PII and those identifying attributes have been verified to belong to a unique individual by a CSP
* Identity Assurance Levels
  + IAL1: The access or service offering does not require that attributes be validated and verified
    - The CSP may request self-asserted attributes of the user
  + IAL2: The access or service offering requires the validation and verification of evidence of the following information about the user: This evidence supports the real-world existence of the claimed identity.
    - Identity proofing may be remote or in-person
    - Two pieces of strong evidence or one piece of strong evidence plus two pieces of fair evidence to prove identity shall be collected
    - Evidence includes home address, photo identification, biometric collection, name, date of birth
    - The collection of this evidence shall be limited to the minimum necessary amount to resolve the identity of the evidence provider
  + IAL3: more rigorous than IAL2, this level requires stronger evidence and requires an in person or supervised remote session to resolve evidence, validate it as correct, and then verify that the claimed identity is associated with the real person supplying the evidence
    - Requires two pieces of superior evidence or one piece of superior evidence plus one piece of strong evidence
    - As in IA2, pieces of evidence may be checked against the records of the authoritative issuer of the documentation provided by the user to validate the evidence is correct
* The strength of identity evidence is determined in accordance with NIST SP 800-63A wherein strength levels range from unacceptable to superior: refer to that document to determine the strength of evidence provided to the CSP
* User applicants are entitled to be given notice of collection of evidence which will be used to maintain a record of the attributes necessary for identity proofing
* CSPs must conduct a privacy risk assessment to determine the likelihood of verification steps to create a problem for the applicant
* See NIST SP 800-63A for details about the resolution, validation, and verification steps taken by the CSP

Authentication

* Authenticators are things that a user applicant controls which act as a key (like a token)
* Authenticators can be any of the following: memorized secret, look-up secret, out-of-band devices, single-factor one-time password (OTP) device, multi-factor (MF) OTP device, single-factor cryptographic software, single-factor cryptographic device, multi-factor cryptographic software, multi-factor cryptographic device
* Memorized secrets are passwords and the following restrictions must be imposed at a minimum to ensure the security of passwords:
  + They must be at least 8 characters in length if chosen by the user subscriber or 6 characters if chosen by the CSP (and may be entirely numeric)
  + If the whole or parts of the memorized secret appear on a blacklist of compromised values (such as dictionary words or repetitive values), the subscriber must choose a different memorized secret
* A subscriber will be assigned an Authenticator Assurance Level commensurate with the type of authenticator or combination of authenticators they have been issued based on the level of authentication they need to access resources or services
* Authenticator Assurance Levels
  + AAL1: requires a single authenticator from the previously listed authenticators
    - Adequate for compliance with Federal Information Processing Standards (FIPS) 140-2 level 1: cryptographic device or cryptography modules are free from various egregious security flaws
  + AAL2: requires a MF OTP device; MF crypto software; a MF crypto device; or memorized secret plus:
    - Look-up secret
    - Out-of-band
    - SF OTP device
    - SF crypto software
    - SF crypto device
  + AAL2 cryptographic devices and cryptography modules must meet standards of FIPS 140-2 level 1
  + AAL3: requires MF crypto device; SF crypto device plus memorized secret; SF OTP device plus MF crypto device or software; SF OTP device plus SF crypto software plus memorized secret
    - Authenticators in this level must have physical tamper-resistance and identity-based authentication as well as role-based authentication
  + Additional details about the types of acceptable authenticators can be found in NIST 800-63B

Authenticator Management

* The events that occur over the lifecycle of authenticators include binding, loss, theft, unauthorized duplication, expiration, and revocation
* Binding is the linking of an authenticator to a subscriber’s account to allow that account to authenticate
  + Binding occurs by 1) issuance by the CSP as part of enrollment or 2) associating an acceptable subscriber-provided authenticator
* Replacement of lost authentication factors
  + In this event, the subscriber must repeat the identity proofing process to confirm that their new authenticator(s) is/are bound to an existing identity
* Loss, theft, damage, and unauthorized duplication
  + Suspension, revocation, or destruction of compromised authenticators should occur as soon as possible following detection
    - The time limit of this process at Crowley Enterprises is 48 hours
  + Subscribers are required to set up a backup authenticator like a memorized secret or physical device to be used for reporting the loss, theft, damage, or unauthorized duplication of primary authenticators to the CSP
* CSPs may issue authenticators that expire
  + After expiration date, the authenticator is not usable for authentication
  + Expired authenticators must be surrendered to the CSP or the CSP can accept proof of destruction of the authenticators
* CSPs shall revoke the binding of authenticators to accounts when:
  + The online identity tied to the account ceases to exist (death, discovery of fraudulent account)
  + Requested by the subscriber
  + The CSP determines that the subscriber no longer meets eligibility
* Surrender of or proof of destruction of physical authenticators which have been revoked is required
* See NIST 800-63B for details about authenticator types and their specific requirements
* Reauthentication of subscriber will be performed at least once every twelve hours when AAL3 status is required to access resources or services

Federation

* Federation is a process which allows the conveyance of identity and authentication information across a set of networked systems
* This process occurs between a CSP (called an identity provider in this case) and an RP for the purpose of the RP providing access to a resource or service to the subscriber
* NIST SP 800-63C encourages the implementation of technical measures to provide disassociability and prevent subscriber tracking and profiling
* Additional details about the privacy and security of the federation process are found in NIST 800-63C and Crowley Enterprises shall follow the practices outlined there
* Assertions of identity information to an RP are categorized into three levels of Federation Assertion Levels (FALs)
  + The technical classifications of these levels are outlined in SP 800-63C, and key management between the IdP and RP is required to be encrypted by a shared key or the RP’s public key

Definitions

* RP – relying party: an entity that verifies or establishes the identity and status of an individual, role, system, device, the integrity of a digitally signed message, or the identity of the creator of a message
* CSP – credential service provider: a trusted entity that issues electronic credentials to a user (also referred to as an IdP – identity provider)

References

* NIST SP 800-63A, NIST SP 800-63B, NIST SP 800-63C
* NIST FIPS-140-2
* FR Security Identity and Access Management Policy Template

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.