Electronic Authentication Partnership Trust Framework

Version 1.0

January 6, 2005

Electronic Authentication Partnership Trust Framework

Contents

1 BUSINESS RULES

1.1 Scope

Signatories to these business rules agree that these rules govern the use and validation of Electronic Authentication Partnership (EAP) certified credentials, the certification of such credentials and the accreditation of those who assess issuers of such credentials. These business rules are intended to cover use of credentials for purposes of authentication and not specifically for the application of a legal signature, which may be subject to other rules depending upon the parties and transactions involved.

The EAP is responsible for the EAP certification of credentials issued by a credential service provider (CSP). The EAP is responsible for the accreditation of assessors who evaluate CSPs for purposes of EAP certification of credentials. An EAP certified credential issued by any EAP CSP may be used by any EAP-relying party that is a signatory to these business rules and that chooses to accept or otherwise rely upon the credential by agreement with the issuing CSP.

The foregoing does not prohibit use of an EAP credential under a different brand, certification, or set of rules, provided that the credential is clearly being used as a non-EAP credential.

Claimants are not direct signatories to these business rules. Claimants must have contracts with each CSP issuing an EAP credential to the claimant. The claimant can be a person, the electronic agent of a person, or any legal entity, including a corporation.

1.2 Participation and Voluntary Termination

Each relying party and CSP must agree to be bound by these business rules as a precondition to participation in the EAP System. By contractually agreeing to be bound by these business rules, a party becomes a signatory to these rules. Before becoming eligible to become a signatory to these rules, a CSP must successfully complete an assessment by an EAP-accredited assessor, be awarded EAP certification for one or more lines of credentials issued by that CSP and sign a CSP participation agreement. A relying party becomes a signatory to these business rules by contracting with one or more EAP CSPs and assenting to the relying party participation agreement. A person need not be a member of the EAP non-profit corporation in order to become a signatory to these business rules. Execution of the participation agreement must be performed by a person legally authorized to bind the respective relying party or CSP for that purpose. The execution of the relying party or CSP participation agreement may be accomplished by any method of contracting approved for this purpose by the EAP Board of Directors.

A party that has become a signatory to these business rules may terminate signatory status at any time by providing the EAP with written notice of termination that includes the effective date of termination. Such notice must be provided no less than 30 days prior to the effective date of termination. Any signatory that objects to an amendment under Section 3.1.1 may give notice of termination less than 30 days prior to the effective date if necessary to avoid becoming bound to the amendment to which the signatory objects. Termination of signatory status terminates any EAP trademark license and any CSP participation agreement and/or relying party agreement to which the signatory is a party.

1.3 Roles and Obligations

1.3.1 EAP

1.3.1.1 Promulgation and Amendment of Business Rules and Other Documents

The EAP shall formalize and may periodically amend these business rules. The EAP shall also formalize and may periodically amend a set of documents governing the accreditation of assessors of EAP CSPs and the certification of EAP credentials. The EAP reserves the right, at its discretion, to formalize and periodically amend such other materials, including policies or guidelines, participation agreements, handbooks or other documents relevant to the EAP. Notice of all amendments shall be given by EAP by electronic mail to the contact person(s) identified by each signatory for such purpose and by posting to the EAP web site. All amendments shall be effective as of the date specified in such notice. If a signatory objects in writing to an amendment within 30 days after notice of the amendment is given by EAP, such objection shall be deemed to be a notice of termination of such signatory's participation in EAP under Section 1.2.

1.3.1.2 Relying Party, CSP and Assessor Approval

The EAP is responsible for approving participation in the EAP System by relying parties, CSPs and assessors. The EAP shall formalize and may periodically amend requirements for certification of credentials issued by a CSP and the accreditation of assessors of CSPs. The EAP shall formalize, maintain and update as needed an EAP-approved CSP list (EAP CSP list) of certified signatory CSPs. This EAP CSP list shall include, at a minimum, the names of each CSP, the level of assurance for which credentials issued by the CSP have been certified and a URL and other contact information for the CSP.

1.3.1.3 Contact Information

Current contact information for the EAP can be found at http://www.eapartnership.org.

1.3.2 CSP OBLIGATIONS

1.3.2.1 CSP Certification

A CSP is obliged to achieve certification of one or more lines of credentials and be added to the EAP CSP list as a prerequisite to being approved by the EAP for participation in the EAP System.

1.3.2.2 CSP Participation Agreement

A CSP is obliged to execute a CSP participation agreement as a prerequisite to being approved by the EAP for participation in the EAP System.

1.3.2.3 Continued Compliance with Certification Requirements

Each approved and certified CSP must comply with all certification requirements during the period of time for which credentials issued by the CSP are certified.

1.3.2.4 Use of EAP Trademark

A CSP may not use or display the EAP trademark in association with the issuance, validation or other servicing of an EAP credential or otherwise use or display the EAP trademark on or associated with any service, product, literature or other information unless such use has been approved by the EAP and the trademark is used in accordance with the applicable agreement with the EAP.

1.3.2.5 Records of EAP Related Disputes

A CSP is required to investigate any complaint raised to the CSP from a relying party regarding an EAP credential. The CSP is also required to keep auditable records of its investigation and decisions regarding any complaint.

1.3.2.6 Validation

Each CSP must make available a method of validation for each EAP credential it issues or is otherwise responsible for validating. Such method must be accessible and reliable.

1.3.2.7 Privacy Practices

Each CSP must be able to verify that it is complying with applicable privacy practices, as stated in Section 1.3.4.8 of these business rules.

1.3.2.8 Relying Party Agreement With CSP

Each approved CSP shall have in place a contract governing the rights and obligations between it and any relying party using, validating or otherwise relying upon EAP-certified credentials issued by that CSP. The parties to the contract, levels of assurance involved, applicable band of monetary recourse (identified in Section 1.4.2), and effective dates must be reported to the EAP in a timely fashion. At a minimum, such contracts shall inform the relying party that it must agree to abide by these business rules and agree to terms and conditions of use of the EAP System contained in a relying party agreement. Such agreement may contain such additional terms as the parties may agree to.

1.3.3 RELYING PARTY OBLIGATIONS

1.3.3.1 Relying Party Participation Agreement

A relying party is obliged to execute a relying party participation agreement as a prerequisite to (a) approval for participation in the EAP System and (b) seeking to validate and rely upon a credential issued under these rules.

1.3.3.2 Reasonable Reliance and Level of Assurance

A relying party is obliged to determine for itself the appropriate level of assurance of the EAP credential needed for a particular application, transaction or other session. A relying party is obliged to establish that a credential is in fact issued by a listed EAP-approved and accredited CSP in order for the relying party's reliance upon the asserted identity of the claimant to be deemed reasonable under these business rules. A relying party is obliged to successfully validate an EAP credential in order for its reliance upon the asserted identity of the claimant to be deemed reasonable under these business rules. Any use by or validation of an EAP credential by a party that has not entered into a relying party agreement with the CSP that issued the credential shall be at the sole risk of that party, for which the CSP shall have no liability whatsoever.

1.3.3.3 Use of EAP Trademark

A relying party may not use or display the EAP trademark in association with the acceptance, validation or other use of an EAP credential or otherwise use or display the EAP trademark on or associated with any service, product, literature or other information unless such use has been approved by the EAP and the trademark is used in accordance with the applicable agreement with the EAP.

1.3.4 ASSESSOR OBLIGATIONS

1.3.4.1 CSP Accreditation

An assessor is not eligible for approval by the EAP to conduct an assessment for purposes of EAP certification of a CSP or otherwise participate as an assessor in the EAP System unless that assessor has been and remains accredited by the EAP.

1.3.4.2 CSP Participation Agreement

An assessor is obliged to execute an EAP assessor agreement as a prerequisite to being approved by the EAP.

1.3.4.3 Continued Compliance with Accreditation Requirements

In accordance with the requirements of the EAP accreditation and certification rules and any applicable service assessment criteria, approved and accredited assessors must remain in compliance with all accreditation requirements for the period of time for which they are accredited.

1.3.4.4 Use of EAP Trademark

An assessor may not use or display the EAP trademark in association with an assessment or otherwise use or display the EAP trademark on or associated with any service, product, literature or other information unless such use has been approved by the EAP and the trademark is used in accordance with the applicable agreement with the EAP.

1.3.5 GENERAL OBLIGATIONS

1.3.4.5 Record Keeping

Every signatory wishing to avail itself of EAP resolution of disputes under the terms of these business rules is obliged to keep records sufficient to preserve evidence of the facts related to a particular dispute.

1.3.4.6 System Security and Reliability

Every signatory agrees to safeguard the security and reliability of the EAP System. Specifically, every signatory agrees that the EAP reserves the right to suspend use of the EAP System, in whole or in part, and the participation of any party or parties to the system without notice and at the sole discretion of the EAP to protect the integrity and efficacy of the EAP System or the rights or property of any party. Agreement to access, use or rely upon the EAP System is subject to such terms and conditions as the EAP may provide in these business rules, related participation agreements or otherwise.

1.3.4.7 Third Party Processors

Any CSP or relying party that is a signatory to these rules and uses a third-party processor to perform any processing, transactions or other obligations related to participation in the EAP System either must take full responsibility for assuring that actions of the third-party processor are in compliance with all applicable terms of these business rules or assure that the third party itself becomes a direct signatory of these business rules.

1.3.4.8 Claimant Privacy

Every signatory to these business rules must assure that each claimant for which the signatory collects or otherwise uses personally identifiable information has granted informed consent with regard to the sharing of any personally identifiable information about the claimant by the signatory with any other party, whether such information is contained in a credential, other identity assertion or otherwise. The informed consent of the individual must be obtained before personally identifiable information is used for enrollment, authentication or any subsequent uses. Claimants must be provided with a clear statement about the collection and use of personally identifiable information upon which to make informed decisions. Signatories must collect only the information necessary to complete the intended authentication function.

Informed consent, for the purposes of this section, is an agreement made by a claimant with the legal capacity to do so who is so situated as to be able to exercise free power of choice without the intervention of any element of force, fraud, deceit, duress, over-reaching, or other form of constraint or coercion and who is given sufficient information about the subject matter and elements of the transaction involved as to enable him or her to make an informed and enlightened decision.

Nothing in these business rules shall be construed to authorize or permit the sharing of any personally identifiable information about an end user other than the information contained in a certificate or other identity assertion. Such information can be shared only with an approved relying party to whom the end user has presented credentials or attempted to access services with an identity assertion operating under the EAP. If any other personally identifiable information about a claimant is shared with any party operating within the EAP System or any other party, the required consent terms listed in this section of these business rules must be affirmatively assented to by the claimant.

1.4 Enforcement and Recourse

1.4.1 BREACH OF ACCREDITATION OR CERTIFICATION REQUIREMENTS

1.4.1.1 Compliance Determination

Upon receipt by the EAP of credible information that an assessor or CSP is not in compliance with the requirements for accreditation or certification, the EAP Board or staff or a committee at Board discretion shall make a determination on whether the assessor or CSP is in fact in material non-compliance with EAP requirements and shall communicate the determination to the affected parties. The Board of Directors shall establish further criteria, as needed, detailing conduct or circumstances constituting material non-compliance with EAP rules or standards.

1.4.1.2 Period to Cure

An assessor or CSP found to be in material non-compliance shall be afforded an opportunity and period of time to remedy that material non-compliance, provided such period does not unduly jeopardize the integrity of the EAP System or the rights or property of another party.

1.4.2 MONETARY RECOURSE

A CSP may be liable solely under the terms of an applicable relying-party agreement with an EAP-approved relying party for losses suffered by such EAP-approved relying party where the cause is attributable to conduct by the CSP that was carried out in material non-compliance with these business rules or with certification requirements.

A CSP may offer credentials at a band of monetary recourse set independently from levels of assurance. A CSP shall disclose the monetary recourse it will or will not make available with respect to EAP credentials and any applicable terms or limitations governing the recourse according to

Table 1-1:

Table 1-1. Bands and Amounts of Monetary Recourse

Band	Amount
1. No recourse	Zero monetary recourse
2. By agreement	By agreement of the parties

1.4.2.1 Safe Harbors

1.4.2.1.1 Losses Arising From Authorization or Unreasonable Reliance

In no event shall liability or other recourse specified herein be triggered by unreasonable reliance on a credential by a relying party or by losses resulting from authorization errors that have not been caused by errors in authentication of identity of a `claimant by means of an EAP credential.

1.4.2.1.2 Conduct in Accordance with Business Rules

Under these business rules, an approved CSP is not liable for losses suffered by an approved relying party where the cause is attributable to conduct by the CSP that was carried out in accordance with these business rules.

1.4.2.2 Request for Monetary Recourse

If a relying party is eligible to request monetary recourse under these rules, then it may do so by submitting to the relevant CSP an event summary, including at least the following information: The account, the date(s) of incorrect authentication validation(s), the cost of repair and the amount of recourse requested, as constrained by the applicable floor and ceiling at the band of recourse for the EAP credential in question. A relying party may request $0, even if costs are significant.

1.4.2.3 Reporting to the EAP

All requests for monetary recourse and the dispositions of all requests must be reported to the EAP by each relying party and CSP involved.

1.4.3 ADMINISTRATIVE RECOURSE

Based on review of all available data and in light of all relevant circumstances, the EAP Board of Directors may take administrative recourse against any signatory determined to be in material non-compliance with these business rules, to include, as needed, any of the following remedies.

1.4.3.1 Warning

The non-complying party may be given a warning. The warning may be confidential or may be publicized within the EAP or publicized more broadly, at the discretion of the EAP Board of Directors.

1.4.3.2 Credential Revocation

The non-complying party may be required to revoke one or more EAP credentials.

1.4.3.3 Non-compliance Fees

The non-complying party may be subject to a schedule of fees, to be specified by the EAP Board of Directors. The fees may increase according to the length of time before the party comes back into compliance.

1.4.3.4 Suspension

The non-complying party may have its participation in the EAP System suspended, including the suspension of accreditation or certification, pending coming back into compliance.

1.4.3.5 Termination

The non-complying party may have its participation in the EAP System terminated, including the termination of accreditation or certification.

1.5 General Terms

1.5.1 GOVERNING LAW

These business rules and any related materials governing the EAP shall be construed and adjudicated according to the laws of the state of Delaware.

1.5.2 DISCLAIMER

No signatory may disclaim the warranty of merchantability and fitness for a particular purpose with respect to the provision of any service or product to any other signatory under these business rules.

1.5.3 ASSIGNMENT AND SUCCESSION

No signatory may sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in these business rules or the participation agreement executed by that signatory without the express written consent of the EAP.

1.5.4 HOLD HARMLESS

All signatories to these business rules agree to hold the EAP harmless for any losses or other liability arising out of or in relation to the issuance, use, acceptance, validation, or other reliance upon an EAP credential or otherwise arising out of or in relation to participation in the EAP System or other conduct subject to these business rules.

1.5.5 SEVERABILITY

If any provision, set of provisions or part of a provision of these business rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

1.6 Interpretation

The terms of these business rules shall be interpreted by the EAP so as to avoid conflict or inconsistencies between the various provisions and between these business rules, applicable participation agreements and other relevant EAP materials.

2 ASSURANCE LEVELS

2.1 Assurance Level Policy Overview

An assurance level (AL) describes the degree to which a relying party in an electronic business transaction can be confident that the credential being presented actually represents the entity named in it and that it is the represented entity who is actually engaging in the electronic transaction. ALs are based on two factors:

- The extent to which the identity presented in an electronic credential can be trusted to actually belong to the entity represented. This factor is generally handled by identity proofing.
- The extent to which the electronic credential can be trusted to be a proxy for the entity named in it and not someone else (known as identity binding). This factor is directly related to the trustworthiness of the credential technology, the processes by which the credential is secured to a token, the trustworthiness of the system that manages the credential and token, and the system available to validate the credential, including the reliability of the credential service provider responsible for this service.

Managing risk in electronic transactions requires authentication processes that provide an appropriate level of assurance. Because different levels of risk are associated with different electronic transactions, EAP has adopted a multi-level approach to ALs. Each level describes a different degree of certainty in the identity of the claimant.

The EAP defines four levels of assurance. The four EAP ALs are based on the four levels of assurance posited by the U.S. Federal Government and described in OMB M-04-04 and NIST Special Publication 800-63 for use by Federal agencies. The EAP ALs enable subscribers and relying parties to select appropriate electronic trust services. EAP uses the ALs to define the service assessment criteria to be applied to electronic trust service providers when they are demonstrating compliance through the EAP assessment process. Relying parties should use the levels to map risk and determine the type of credential issuing and authentication services they require. Credential service providers (CSPs) should use the levels to determine what types of credentialing electronic trust services to offer.

2.2 Description of the Four Assurance Levels

The four ALs describe the degree of certainty associated with an identity. The levels are identified by both a number and a text label. The levels are defined as shown in **Error! Reference source not found.**:

Table 2-1. Four Assurance Levels

Number	Label	Description
1	Minimal	Little or no confidence in the asserted identity's validity
2	Moderate	Some confidence in the asserted identity's validity

3	Substantial	High confidence in the asserted identity's validity
4	High	Very high confidence in the asserted identity's validity

The choice of AL is based on the degree of authentication required to mitigate risk and the level of authentication provided by the credentialing process. The degree of authentication required is determined by the relying party through risk assessment processes covering the electronic transaction system. By mapping impact levels to ALs, relying parties can then determine what level of authentication they require. (Further information on assessing risk is provided below.)

The level of authentication provided is measured by the strength and rigor of the identity-proofing process, the credential's strength and the management processes the service provider applies to it. The EAP has established service assessment criteria at each AL for electronic trust services providing credential management services. These criteria are described in Section 3.

CSPs can determine the AL at which their services might qualify by evaluating their overall business processes and technical mechanisms against the EAP service assessment criteria. Services can be developed to qualify for a particular AL. The service assessment criteria within each AL are the basis for assessing and approving electronic trust services.

Table 2-2 Potential Impact at Each Assurance Level

Potential Impact of Authentication Errors	**Assurance Level***			
	1	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Min	Mod	Sub	High
Financial loss or agency liability	Min	Mod	Sub	High
Harm to agency programs or public interests	N/A	Min	Mod	High
Unauthorized release of sensitive information	N/A	Min	Sub	High
Personal safety	N/A	N/A	Min	Sub High
Civil or criminal violations	N/A	Min	Sub	High

**Min=Minimum; Mod=Moderate; Sub=Substantial; High=High*

2.2.1 ASSURANCE LEVEL 1 (MINIMAL)

At AL1, there is minimal confidence in the asserted identity. Use of this level is appropriate when no negative consequences result from erroneous authentication and the authentication mechanism used provides some assurance. A wide range of available technologies and any of the token methods associated with higher ALs, including PINS, can satisfy the authentication requirement. This level does not require use of cryptographic methods.

The electronic submission of forms by individuals can be Level 1 transactions when all information flows to the organization from the individual, there is no release of information in return and the criteria for higher assurance levels are not triggered. For example, when an individual uses a web site to pay a parking ticket or tax payment, the transaction can be treated as a Level 1 transaction. Other examples of Level 1 transactions include transactions in which a claimant presents a self-registered user ID or password to a merchant's web page to create a customized page, or transactions involving web sites that require registration for access to materials and documentation such as news or product documentation.

2.2.2 ASSURANCE LEVEL 2 (MODERATE)

At AL2 there is confidence that an asserted identity is accurate. Moderate risk is associated with erroneous authentication. Single-factor remote network authentication is appropriate. Successful authentication requires that the claimant prove control of the token through a secure authentication protocol. Eavesdropper, replay and online guessing attacks are prevented. Although the identity proofing requirements are similar to those for AL1, the authentication mechanisms must be more secure.

For example, a transaction in which a beneficiary changes an address of record through an insurance provider's web site can be a Level 2 transaction. The site needs some authentication to ensure that the address being changed is the entitled person's address. However, this transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status and records of changes are sent to the beneficiary's address of record, the transaction entails moderate risk of unauthorized release of personally sensitive data.

2.2.3 ASSURANCE LEVEL 3 (SUBSTANTIAL)

AL3 is appropriate for transactions requiring high confidence in an asserted identity. Substantial risk is associated with erroneous authentication. This level requires multi-factor remote network authentication. Identity proofing procedures require verification of identifying materials and information. Authentication must be based on proof of possession of a key or password through a cryptographic protocol. Tokens can be “soft,” “hard,” or “one-time password” device tokens. Note that both identity proofing and authentication mechanism requirements are more substantial.

For example, a transaction in which a patent attorney electronically submits confidential patent information to the U.S. Patent and Trademark Office can be a Level 3 transaction. Improper disclosure would give competitors a competitive advantage. Other Level 3 transaction examples include online access to a brokerage account that allows the claimant to trade stock, or use by a contractor of a remote system to access potentially sensitive personal client information.

2.2.4 ASSURANCE LEVEL 4 (HIGH)

AL4 is appropriate for transactions requiring very high confidence in an asserted identity. This level provides the best practical remote-network authentication assurance, based on proof of possession of a key through a cryptographic protocol. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed. High levels of cryptographic assurance are required for all elements of credential and token management. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

For example, access by a law enforcement official to a law enforcement database containing criminal records requires Level 4 protection. Unauthorized access could raise privacy issues and/or compromise investigations. Dispensation by a pharmacist of a controlled drug also requires Level 4 protection. The pharmacist needs full assurance that a qualified doctor prescribed the drug, and the pharmacist is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount. Finally, approval by an executive of a transfer of funds in excess of $1 million out of an organization’s bank accounts would be a Level 4 transaction.

3 SERVICE ASSESSMENT CRITERIA

3.1 Context and Scope

The EAP Service Assessment Criteria (SAC) are prepared and maintained by the Electronic Authentication Partnership (EAP) as part of its Trust Framework. These criteria set out the requirements for services and their providers at all assurance levels within the Framework. These criteria focus on the specific requirements for EAP assessment at each assurance level (AL) for the following:

- The general business and organizational conformity of services and their providers,
- The functional conformity of identity proofing services, and
- The functional conformity of credential management services and their providers.

These criteria (at the applicable level) must be complied with by all services that are assessed for certification under the EAP Trust Framework.

These criteria have been approved under the EAP's governance rules as being suitable for use by EAP-recognized assessors in the performance of their assessments of trust services whose providers are seeking approval by EAP.

In the context of the EAP Trust Framework, the status of this document is normative. An applicant provider's trust service **shall** comply with all applicable criteria within this SAC at their nominated AL.

This document describes the specific criteria that must be met to achieve each of the four ALs supported by the EAP. To be certified under the EAP System, services must comply with all criteria at the appropriate level.

3.2 Readership

This description of Service Assessment Criteria is required reading for all EAP-recognized assessors, since it sets out the requirements with which service functions must comply to obtain EAP approval.

The description of criteria in sections 3.5, 3.6 and 3.7 is required reading for all providers of services that include identity-proofing functions, since providers must be fully aware of the criteria with which their service must comply. It is also recommended reading for those involved in the governance and day-to-day administration of the EAP Trust Framework.

Identity proofing criteria included in section 3.6 is required reading for all Electronic Trust Service Providers whose services include identity-proofing functions, since providers must be fully aware of the criteria with which their service must comply.

This document will also be of interest to those wishing to have a detailed understanding of the operation of the EAP's Trust Framework but who are not actively involved in its operations or in services that may fall within the scope of the Framework.

3.3 Terminology

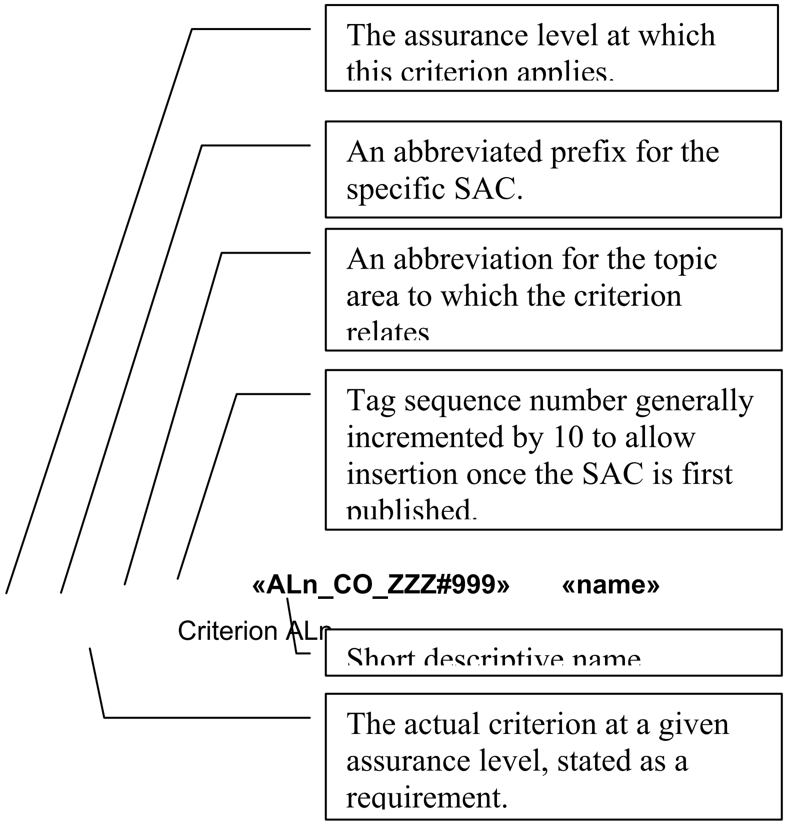
All special terms used in this description are defined in the EAP Glossary.

3.4 Criteria Descriptions

The Service Assessment Criteria are organized by AL. Subsections within each level describe the criteria that apply to specific functions. The subsections are parallel. Subsections describing the requirements for the same function at different levels of assurance have the same title.

Each criterion consists of three components: a unique alphanumeric tag, a short name, and the criterion (or criteria) associated with the tag. The tag provides a unique reference for each criterion that assessors and service providers can use to refer to that criterion. The name identifies the intended scope or purpose of the criterion.

The criteria are described as follows:


The assurance level at which this criterion applies.
An abbreviated prefix for the specific SAC.
An abbreviation for the topic area to which the criterion relates
Tag sequence number generally incremented by 10 to allow insertion once the SAC is first published.
«ALn_CO_ZZZ#999»
«name»
Criterion ALn
Short descriptive name
The actual criterion at a given assurance level, stated as a requirement.

3.5 Common Organizational Service Assessment Criteria

The Service Assessment Criteria in this section establish the general business and organizational requirements for conformity of services and service providers at all ALs defined in Section 2. These criteria are generally referred to elsewhere within EAP documentation as CO-SAC.

These criteria may only be used in an assessment in combination with one or more other SACs that address the technical functionality of specific service offerings.

3.5.1 ASSURANCE LEVEL 1 (MINIMAL)

3.5.1.1 Enterprise and Service Maturity

These criteria apply to the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL1_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the assessment package.

AL1_CO_ESM#020 Established service

Be described in the assessment package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL1_CO_ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be used.

3.5.1.2 Notices & User information

These criteria address the publication of information describing the service and the manner of and any limitations upon its provision.

An enterprise and its specified service must:

AL1_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition for its specified service that includes all applicable Terms, Conditions, Fees and Privacy Policy for the service, including any limitations of its usage.

AL1_CO_NUI#020 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions and Privacy Policy for the specified service.

AL2_CO_NUI#035 User Agreement

Through a user agreement:

a) require the Subscriber to provide full and correct information as required under the terms of their use of the service.
b) obtain a record (hard-copy or electronic) of the Subscriber's Agreement to the Terms and Conditions of service.

3.5.1.3 Information Security Management

No stipulation.

3.5.1.4 Secure Communications

AL1_CO_SCO#020 Protection of secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications which need such access.

b) stored shared secrets are not held in their plaintext form.
c) any plaintext passwords or secrets are not transmitted across any public or unsecured network.

3.5.2 ASSURANCE LEVEL 2 (MODERATE)

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

3.5.2.1 Enterprise and Service Maturity

These criteria apply to the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL2_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the assessment package.

AL2_CO_ESM#020 Established service

Be described in the assessment package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL2_CO_ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered.

AL2_CO_ESM#050 Financial Provisions

Demonstrate that it has adequate financial resources for the continued operation of the service and has in place appropriate provision for the degree of liability exposure being carried.

AL2_CO_ESM#060 Data Retention & Protection

Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention of private (personal and business) information (its secure storage and protection against loss and/or destruction) and the protection of private information (against unlawful or unauthorized access unless permitted by the information owner or required by due process).

3.5.2.2 Notices and User Information/Agreements

These criteria apply to the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL2_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition for its specified service that includes any specific uses or limitations on its use, all applicable Terms, Conditions, Fees and Privacy Policy for the service, including any limitations of its usage and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

AL2_CO_NUI#020 Service Definition sections

Publish a Service Definition for the specified service containing clauses that provide the following information:

a) the legal jurisdiction under which the service is operated.
b) if different from the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into.
c) applicable legislation with which the service complies.
d) obligations incumbent upon the CSP
e) obligations incumbent upon the subscriber.
f) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product.
g) statement of warranties.
h) statement of liabilities.
i) procedures for notification of changes to terms and conditions.
j) steps the ETSP will take in the event that it chooses or is obliged to terminate the service.
k) full contact details for the ETSP (i.e., conventional post, telephone, Internet) including a helpdesk.
l) availability of the specified service per se and of its help desk facility.
m) termination of aspects or all of service.

AL2_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the Service Definition and any applicable Terms, Conditions, Fees and Privacy Policy for the specified service and provides a clear means by which subscribers may indicate that they wish to accept the new terms or terminate their subscription.

AL2_CO_NUI#034 Subscriber Information

Require the Subscriber to provide full and correct information as required under the terms of their use of the service.

AL2_CO_NUI#036 Subscriber Agreement

Obtain a record (hard-copy or electronic) of the Subscriber's Agreement to the Terms & Conditions of service.

AL2_CO_NUI#038 Change of Subscriber Information

Require and provide the mechanisms for the Subscriber to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's identity has been authenticated.

AL2_CO_NUI#040 Helpdesk facility

Ensure that its helpdesk is available for any queries related to the specified service during the regular business hours of its primary operational location, minimally from 9 AM to 5 PM, Monday through Friday, excepting Federal holidays.

3.5.2.3 Information Security Management

These criteria apply to the way in which the enterprise manages security for its business, the specified service and information relating to its user community. These criteria focus on the key components of an effective Information Security Management System (ISMS).

An enterprise and its specified service must:

AL2_CO_ISM#010 Documented policies and procedures

Have documented all security-relevant administrative, management and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards or published references, are adequate for the specified service and are applied in the manner intended.

AL2_CO_ISM#020 Policy Management & Responsibility

Have a clearly defined managerial role, at a senior level, in which full responsibility for the business's security policies is vested and from which promulgation of policy and related procedures is controlled and managed. The policies in place must be properly maintained so as to be effective at all times.

AL2_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community.

AL2_CO_ISM#040 Continuity of Operations Plan

Have and shall keep updated a Continuity of Operations Plan that covers disaster recovery and the resilience of the specified service.

AL2_CO_ISM#050 Configuration Management

Demonstrate a Configuration Management system that at least includes:

a) version control for software system components.
b) timely identification and installation of all applicable patches for any software used in the provisioning of the specified service.

AL2_CO_ISM#060 Quality Management

Demonstrate a Quality Management system that is appropriate for the specified service.

AL2_CO_ISM#065 System Installation & Operation Controls

Apply controls during system development, procurement installation and operation that protect the security and integrity of the system environment, hardware, software and communications.

AL2_CO_ISM#070 Internal Service Audit

Unless it can show that by reason of its size or for other operational reason it is unreasonable, be regularly audited for effective provision of the specified service by internal audit functions independent of the parts of the enterprise responsible for the Specified Service.

AL2_CO_ISM#080 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization’s security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor must have appropriate accreditation or other acceptable experience and qualification**.**

AL2_CO_ISM#090 Audit Records

Retain full records of all audits, both internal and independent, for a period that, at a minimum, fulfills its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a Subscriber. Such records must be held securely and protected against loss, alteration or destruction.

AL2_CO_ISM#100 Termination provisions

Have in place a clear plan for the protection of subscribers’ private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally required records and for the secure destruction and disposal of any such information whose retention is not legally required. Essential details of this plan must be published.

3.5.2.4 Security-relevant Event (Audit) Records

These criteria apply to the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL2_CO_SER#010 Security event logging

Maintain a log of all security-relevant events concerning the operation of the service, together with a precise record of the time at which the event occurred (time-stamp) [AL4 provided by a trusted time-source]and such records must be retained with appropriate protection, accounting for service definition, risk management requirements and applicable legislation.

3.5.2.5 Operational infrastructure

These criteria apply to the infrastructure within which the delivery of the specified service takes place. These criteria emphasize the personnel involved and their selection, training and duties.

An enterprise and its specified service must:

AL2_CO_OPN#010 Technical security

Demonstrate that the technical controls employed will provide the level of security required by the risk assessment plan and the ISMS and that these controls are effectively integrated with the appropriate procedural and physical security measures.

AL2_CO_OPN#020 Defined security roles

Define by means of a job description the roles and responsibilities for every security-relevant task, relating it to specific procedures (which shall be set out in the ISMS) and other job descriptions. Where the role is security critical or where special privileges or shared duties exist, these must be specifically highlighted, including access privileges relating to logical and physical parts of the services operations.

AL2_CO_OPN#030 Personnel recruitment

Demonstrate that it has defined practices for the selection, evaluation and contracting of all personnel, both direct employees and those whose services are provided by third parties.

AL2_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on-the-job training, they must only do so under the guidance of a mentor with established leadership skills.

AL2_CO_OPN#045 Adequacy of Personnel resources

Have sufficient staff to operate the Specified Service according to its policies and procedures**.**

AL2_CO_OPN#050 Physical access control

Apply physical access control mechanisms to ensure that access to sensitive areas is restricted to authorized personnel.

AL2_CO_OPN#060 Logical access control

Employ logical access control mechanisms to ensure that access to sensitive system functions and controls is restricted to authorized personnel.

3.5.2.6 External Services and Components

These criteria apply to the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL2_CO_ESC#010 Contracted policies and procedures

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources that are integrated with its own operations and under its controls, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures and practices that the subcontractor is required to fulfill.

AL2_CO_ESC#020 Visibility of contracted parties

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources that are integrated with its own operations and under its controls, ensure that contractors' compliance with contractually stipulated policies and procedures, and thus with EAP assessment criteria, can be proven and subsequently monitored.

3.5.2.7 Secure Communications

An enterprise and its specified service must:

AL2_CO_SCO#010 Secure remote communications

If the Specific Service components are located remotely from and communicate over a public or unsecured network with other service components or other CSP(s) it services, the communications must be cryptographically authenticated by an authentication method that meets, at a minimum, the requirements of AL2 and encrypted using a Federal Information Processing Standard (FIPS)-approved encryption method or a mechanism of demonstrably equivalent rigor.

AL2_CO_SCO#020 Protection of secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls that permit access to those roles/applications requiring such access.
b) stored shared secrets are not held in their plaintext form.
c) any long-term (i.e., not session) shared secrets are revealed only to the Subscriber and to CSP's direct agents (bearing in mind a, above).

3.5.3 ASSURANCE LEVEL 3 (SUBSTANTIAL)

Achieving AL3 requires meeting all criteria required to achieve AL2. This section includes only requirements additional to those described in Section 3.5.2.

3.5.3.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL3_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the Assessment Package.

AL3_CO_ESM#020 Established service

Be described in the assessment package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL3_CO_ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered.

AL3_CO_ESM#050 Financial Provisions

Demonstrate that it has adequate financial resources for the continued operation of the service and has in place appropriate provision for the degree of liability exposure being carried.

AL3_CO_ESM#060 Data Retention and Protection

Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention of private (personal and business) information (its secure storage and protection against loss and/or destruction) and the protection of private information (against unlawful or unauthorized access unless permitted by the information owner or required by due process).

AL3_CO_ESM#070 Ownership

If the enterprise named as the CSP is a part of a larger entity, the nature of the relationship with its parent organization shall be disclosed to the assessors and, on their request, to customers.

AL3_CO_ESM#080 Independent management and operations

Demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability and function according to separate policies, procedures and controls.

3.5.3.2 Notices and User Information

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL3_CO_NUI#010 General Service Definition

Make available to the intended user community a service definition for its specified service which includes any specific uses or limitations on its use, all applicable terms, conditions, fees and privacy policy for the service, including any limitations of its usage and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

AL3_CO_NUI#020 Service Definition Sections

Publish a service definition for the specified service containing clauses which provide the following information:

a) the legal jurisdiction under which the service is operated;
b) if different to the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into;
c) applicable legislation with which the service complies;
d) obligations incumbent upon the ETSP;
e) obligations incumbent upon the subscriber;
f) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product;
g) statement of warranties;
h) statement of liabilities;
i) procedures for notification of changes to terms and conditions;
j) steps the ETSP will take in the event that it chooses or is obliged to terminate the service;
k) full contact details for the ETSP (i.e. conventional post, telephone, internet) including a helpdesk;
l) availability of the specified service *per se* and of its help desk facility;
m) termination of aspects or all of service.

AL3_CO_NUI#030 Due notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the service definition and any applicable terms, conditions, fees and privacy policy for the specified service and provides a clear means by which subscribers may indicate that they wish to accept the new terms or terminate their subscription.

AL3_CO_NUI#034 Subscriber Information

Require the subscriber to provide full and correct information as required under the terms of their use of the service.

AL3_CO_NUI#036 Subscriber Agreement

Obtain a record (hard-copy or electronic) of the subscriber's agreement to the terms and conditions of service.

AL3_CO_NUI#038 Change of Subscriber Information

Require and provide the mechanisms for the Subscriber to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's identity has been authenticated.

AL3_CO_NUI#040 Helpdesk facility

Ensure that its helpdesk is available for any queries related to the specified service during the regular business hours of its primary operational location, minimally from 9:00 a.m. through 5:00 p.m., Monday to Friday inclusive, excepting Federal holidays.

3.5.3.3 Information Security Management

Criteria in this section address the way in which the enterprise manages the security of its business, the specified service and information it holds relating to its user community. This focuses on the key components which make up a well-established Information Security Management System (ISMS).

An enterprise and its specified service must:

AL3_CO_ISM#010 Documented policies and procedures

Have documented all security relevant administrative management and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards or published references are adequate for the specified service and are applied in the manner intended.

AL3_CO_ISM#020 Policy Management and Responsibility

Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security policies is vested and from which promulgation of policy and related procedures is controlled and managed. The policies in place must be properly maintained so as to be effective at all times.

AL3_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and must show that a risk assessment review is performed at least once every six months.

AL3_CO_ISM#040 Continuity of Operations Plan

Have and shall keep updated a continuity of operations plan that covers disaster recovery and the resilience of the specified service and must show that a review of this plan is performed at least once every six months.

AL3_CO_ISM#050 Configuration Management

Demonstrate a configuration management system that at least includes:

a) version control for software system components;
b) timely identification and installation of all applicable patches for any software used in the provisioning of the specified service;
c) version control and managed distribution for all documentation associated with the specification, management and operation of the system, covering both internal and publicly available materials.

AL3_CO_ISM#060 Quality Management

Demonstrate a quality management system that is appropriate for the specified service.

AL3_CO_ISM#065 System Installation and Operation Controls

Apply controls during system development, procurement, installation and operation that protect the security and integrity of the system environment, hardware, software and communications having particular regard to:
a) the software and hardware development environments, for customized components.
b) the procurement process for commercial off-the-shelf (COTS) components.
c) contracted consultancy/support services.
d) shipment of system components.
e) storage of system components.
f) installation environment security.
g) system configuration.
h) transfer to operational status.

AL3_CO_ISM#070 Internal Service Audit

Unless it can show that by reason of its size or for other arguable operational reason it is unreasonable so to perform, be regularly audited for effective provision of the specified service by internal audit functions independent of the parts of the enterprise responsible for the specified service.

AL3_CO_ISM#080 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization's security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor must have appropriate accreditation or other acceptable experience and qualification.

AL3_CO_ISM#090 Audit Records

Retain full records of all audits, both internal and independent, for a period which, as a minimum, fulfils its legal obligations and otherwise for greater periods either as it may have committed to in its service definition or required by any other obligations it has with/to a subscriber. Such records must be held securely and protected against loss, alteration or destruction.

AL3_CO_ISM#100 Termination provisions

Have in place a clear plan for the protection of subscribers' private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally-required records and for the secure destruction and disposal of any such information whose retention is not legally required. Essential details of this plan must be published.

AL3_CO_ISM#110 Best Practice Security Management

Have in place an Information Security Management System (ISMS) that follows best practices as accepted by the information security industry and that applies and is appropriate to the CSP in question. All requirements defined by preceding criteria in this section must fall wholly within the scope of this ISMS.

3.5.3.4 Security-Relevant Event (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events which are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL3_CO_SER#010 Security Event Logging

Maintain a log of all security-relevant events concerning the operation of the service, together with a precise record of the time at which the event occurred (time-stamp).

3.5.3.5 Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training and duties.

An enterprise and its specified service must:

AL3_CO_OPN#010 Technical security

Demonstrate that the technical controls employed will provide the level of security required by the risk assessment plan and the ISMS, and that these controls are effectively integrated with the appropriate procedural and physical security measures.

AL3_CO_OPN#020 Defined security roles

Define by means of a job description the roles and responsibilities for every security-relevant task, relating it to specific procedures (which shall be set out in the ISMS) and other job descriptions. Where the role is security critical or where special privileges or shared duties exist these must be specifically highlighted, including access privileges relating to logical and physical parts of the services operations.

AL3_CO_OPN#030 Personnel recruitment

Demonstrate that is has defined practices for the selection, vetting and contracting of all personnel, both direct employees and those whose services are provided by third parties. Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual’s employment plus the longest lifespan of any credential issued under the service policy.

AL3_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on the job training they must only do so under the guidance of a mentor with established leadership skills.

AL3_CO_OPN#045 Adequacy of Personnel resources

Have sufficient staff to operate the specified service according to its policies and procedures**.**

AL3_CO_OPN#050 Physical access control

Apply physical access control mechanisms to ensure access to sensitive areas is restricted to authorized personnel.

AL3_CO_OPN#060 Logical access control

Employ logical access control mechanisms to ensure access to sensitive system functions and controls is restricted to authorized personnel.

3.5.3.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL3_CO_ESC#010 Contracted policies and procedures

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures and practices that the sub-contractor is required to fulfill.

AL3_CO_ESC#020 Visibility of contracted parties

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that contractors' compliance with contractually stipulated policies and procedures, and thus with the EAP's assessment criteria, can be proven and subsequently monitored.

3.5.3.7 Secure Communications

An enterprise and its specified service must:

AL3_CO_SCO#010 Secure remote communications

If the Specific Service components are located remotely from and communicate over a public or unsecured network with other service components or other CSPs it services, the communications must be cryptographically authenticated by an authentication protocol that meets, at a minimum, the requirements of AL3] and encrypted using an Approved Encryption method.

AL3_CO_SCO#020 Protection of secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls that permit access to those roles/applications requiring such access.

b) stored shared secrets are encrypted such that

   i the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 (or higher) validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation.

   ii they are protected as a key within the boundary of a FIPS 140-2 Level 2 (or higher) validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported in plaintext from the module.

   iii they are split by an '*n from m*' cryptographic secret-sharing method.

c) any long-term (i.e., not session) shared secrets are revealed only to the Subscriber and CSP direct agents (bearing in mind a, above).

3.5.4 ASSURANCE LEVEL 4 (HIGH)

Achieving AL4 requires meeting all criteria required to achieve AL3. This section includes only requirements additional to those described in Section 3.5.3.

3.5.4.1 Enterprise and Service Maturity

Criteria in this section address the establishment of the enterprise offering the service and its basic standing as a legal and operational business entity.

An enterprise and its specified service must:

AL4_CO_ESM#010 Established enterprise

Be a valid legal entity and a person with legal authority to commit the enterprise must submit the Assessment Package.

AL4_CO_ESM#020 Established service

Be described in the Assessment Package as it stands at the time of submission for assessment and must be assessed strictly against that description.

AL4_CO_ESM#040 Legal compliance

Set out and demonstrate that it understands and complies with any legal requirements incumbent on it in connection with operation and delivery of the specified service, accounting for all jurisdictions within which its services may be offered.

AL4_CO_ESM#050 Financial Provisions

Demonstrate that it has adequate financial resources for the continued operation of the service and has in place appropriate provision for the degree of liability exposure being carried.

AL4_CO_ESM#060 Data Retention and Protection

Specifically set out and demonstrate that it understands and complies with those legal and regulatory requirements incumbent upon it concerning the retention of private (personal and business) information (its secure storage and protection against loss and/or destruction) and the protection of private information (against unlawful or unauthorized access unless permitted by the information owner or required by due process).

AL4_CO_ESM#070 Ownership

If the enterprise named as the ETSP is a part of a larger entity, the nature of the relationship with its parent organization, shall be disclosed to the assessors and, on their request, to customers.

AL4_CO_ESM#080 Independent Management and Operations

Demonstrate that, for the purposes of providing the specified service, its management and operational structures are distinct, autonomous, have discrete legal accountability and function according to separate policies, procedures and controls.

3.5.4.2 Notices and User Information/Agreements

Criteria in this section address the publication of information describing the service and the manner of and any limitations upon its provision, and how users are required to accept those terms.

An enterprise and its specified service must:

AL4_CO_NUI#010 General Service Definition

Make available to the intended user community a Service Definition for its specified service which includes any specific uses or limitations on its use, all applicable Terms, Conditions, Fees and Privacy Policy for the service, including any limitations of its usage and definitions of any terms having specific intention or interpretation. Specific provisions are stated in further criteria in this section.

AL4_CO_NUI#020 Service Definition Sections

Publish a Service Definition for the specified service containing clauses which provide the following information:
a) the legal jurisdiction under which the service is operated;

b) if different to the above, the legal jurisdiction under which subscriber and any relying party agreements are entered into;
c) applicable legislation with which the service complies;
d) obligations incumbent upon the ETSP;
e) obligations incumbent upon the subscriber;
f) notifications and guidance for relying parties, especially in respect of actions they are expected to take should they choose to rely upon the service's product;
g) statement of warranties;
h) statement of liabilities;
i) procedures for notification of changes to terms and conditions;
j) steps the ETSP will take in the event that it chooses or is obliged to terminate the service;
k) full contact details for the ETSP (i.e. conventional post, telephone, internet) including a helpdesk;
l) availability of the specified service *per se* and of its help desk facility;
m) termination of aspects or all of service.

AL4_CO_NUI#030 Due Notification

Have in place and follow appropriate policy and procedures to ensure that it notifies subscribers in a timely and reliable fashion of any changes to the service definition and any applicable terms, conditions, fees and privacy policy for the specified service and provides a clear means by which subscribers may indicate that they wish to accept the new terms or terminate their subscription.

AL4_CO_NUI#034 Subscriber Information

Require the Subscriber to provide full and correct information as required under the terms of their use of the service.

AL4_CO_NUI#036 Subscriber Agreement

Obtain a record (hard-copy or electronic) of the Subscriber's Agreement to the Terms and Conditions of service.

AL4_CO_NUI#038 Change of Subscriber Information

Require and provide the mechanisms for the Subscriber to provide in a timely manner full and correct amendments should any of their recorded information change, as required under the terms of their use of the service, and only after the subscriber's identity has been authenticated.

AL4_CO_NUI#040 Helpdesk facility

Ensure that its helpdesk is available for any queries related to the specified service during the regular business hours of its primary operational location, minimally from 9:00 a.m. to 5;00 p.m., Monday to Friday inclusive, excepting Federal holidays.

3.5.4.3 Information Security Management

Criteria in this section address the way in which the enterprise manages the security of its business, the specified service and information it holds relating to its user community. This focuses on the key components which make up a well-established Information Security Management System (ISMS).

An enterprise and its specified service must:

AL4_CO_ISM#010 Documented policies and procedures

Have documented all security-relevant administrative, management and technical policies and procedures. The enterprise must ensure that these are based upon recognized standards or published references, are adequate for the specified service and are applied in the manner intended.

AL4_CO_ISM#020 Policy Management and Responsibility

Have a clearly defined managerial role, at a senior level, where full responsibility for the business' security policies is vested and from which promulgation of policy and related procedures is controlled and managed. The policies in place must be properly maintained so as to be effective at all times.

AL4_CO_ISM#030 Risk Management

Demonstrate a risk management methodology that adequately identifies and mitigates risks related to the specified service and its user community and must show that on-going risk assessment review is conducted as a part of the business' procedures.

AL4_CO_ISM#040 Continuity of Operations Plan

Have and shall keep updated a continuity of operations plan that covers disaster recovery and the resilience of the specified service and must show that on-going review of this plan is conducted as a part of the business' procedures.

AL4_CO_ISM#050 Configuration Management

Demonstrate a Configuration Management system that at least includes:

a) version control for software system components;

b) timely identification and installation of all applicable patches for any software used in the provisioning of the specified service;

c) version control and managed distribution for all documentation associated with the specification, management and operation of the system, covering both internal and publicly available materials.

AL4_CO_ISM#060 Quality Management

Demonstrate a Quality Management system that is appropriate for the specified service.

AL4_CO_ISM#065 System Installation and Operation Controls

Apply controls during system development, procurement installation and operation which protect the security and integrity of the system environment, hardware, software and communications having particular regard to:

a) the software and hardware development environments, for customized components;

b) the procurement process for COTS components;
c) contracted consultancy/support services;
d) shipment of system components;
e) storage of system components;
f) installation environment security;
g) system configuration;
h) transfer to operational status.

AL4_CO_ISM#070 Internal Service Audit

Unless it can show that by reason of its size or for other arguable operational reason it is unreasonable so to perform, be regularly audited for effective provision of the specified service by internal audit functions independent of the parts of the enterprise responsible for the Specified Service.

AL4_CO_ISM#080 Independent Audit

Be audited by an independent auditor at least every 24 months to ensure the organization’s security-related practices are consistent with the policies and procedures for the specified service and the appointed auditor must have appropriate accreditation or other acceptable experience and qualification.

AL4_CO_ISM#090 Audit Records

Retain full records of all audits, both internal and independent, for a period which, as a minimum, fulfils its legal obligations and otherwise for greater periods either as it may have committed to in its Service Definition or required by any other obligations it has with/to a Subscriber. Such records must be held securely and protected against loss, alteration or destruction.

AL4_CO_ISM#100 Termination provisions

Have in place a clear plan for the protection of subscribers’ private and secret information related to their use of the service which must ensure the ongoing secure preservation and protection of legally-required records and for the secure destruction and disposal of any such information whose retention is not legally required. Essential details of this plan must be published.

AL4_CO_ISM#110 Best Practice Security Management

Have in place a certified Information Security Management System (ISMS) which has been assessed and found to be in compliance with the code of practice ISO/IEC 17799 through application of practices defined in BS 7799 Part 2 and which applies and is appropriate to the ETPS in question. All requirements expressed in preceding criteria in this ‘ISM’ section must *inter alia* fall wholly within the scope of this ISMS.

3.5.4.4 Security-Related (Audit) Records

The criteria in this section are concerned with the need to provide an auditable log of all events which are pertinent to the correct and secure operation of the service.

An enterprise and its specified service must:

AL4_CO_SER#010 Security Event Logging

Maintain a log of all security-relevant events concerning the operation of the service, together with a precise record of the time at which the event occurred (time-stamp) provided by a trusted time-source and such records must be retained with appropriate protection, accounting for service definition, risk management requirements and applicable legislation.

3.5.4.5 Operational Infrastructure

The criteria in this section address the infrastructure within which the delivery of the specified service takes place. It puts particular emphasis upon the personnel involved, and their selection, training and duties.

An enterprise and its specified service must:

AL4_CO_OPN#010 Technical Security

Demonstrate that the technical controls employed will provide the level of security required by the risk assessment plan and the ISMS, and that these controls are effectively integrated with the appropriate procedural and physical security measures.

AL4_CO_OPN#020 Defined Security Roles

Define by means of a job description the roles and responsibilities for every security-relevant task, relating it to specific procedures (which shall be set out in the ISMS) and other job descriptions. Where the role is security critical or where special privileges or shared duties exist these must be specifically highlighted, including access privileges relating to logical and physical parts of the services operations.

AL4_CO_OPN#030 Personnel Recruitment

Demonstrate that is has defined practices for the selection, vetting and contracting of all personnel, both direct employees and those whose services are provided by third parties. Full records of all searches and supporting evidence of qualifications and past employment must be kept for the duration of the individual's employment plus the longest lifespan of any credential issued under the service policy.

AL4_CO_OPN#040 Personnel skills

Ensure that employees are sufficiently trained, qualified, experienced and current for the roles they fulfill. Such measures must be accomplished either by recruitment practices or through a specific training program. Where employees are undergoing on the job training they must only do so under the guidance of a mentor with established leadership skills.

AL4_CO_OPN#045 Adequacy of Personnel resources

Have sufficient staff to operate the Specified Service according to its policies and procedures.

AL4_CO_OPN#050 Physical access control

Apply physical access control mechanisms to ensure access to sensitive areas is restricted to authorized personnel.

AL4_CO_OPN#060 Logical access control

Employ logical access control mechanisms to ensure access to sensitive system functions and controls is restricted to authorized personnel.

3.5.4.6 External Services and Components

This section addresses the relationships and obligations upon contracted parties both to apply the policies and procedures of the enterprise and also to be available for assessment as critical parts of the overall service provision.

An enterprise and its specified service must:

AL4_CO_ESC#010 Contracted Policies and Procedures

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that those parties are engaged through reliable and appropriate contractual arrangements which stipulate critical policies, procedures and practices that the sub-contractor is required to fulfill.

AL4_CO_ESC#020 Visibility of Contracted Parties

Where the enterprise uses the services of external suppliers for specific packaged components of the service or for resources which are integrated with its own operations and under its controls, ensure that contractors' compliance with contractually stipulated policies and procedures, and thus with the EAP's assessment criteria, can be proven and subsequently monitored.

3.5.4.7 Secure Communications

An enterprise and its specified service must:

AL4_CO_SCO#010 Secure remote communications

If the specific service components are located remotely from and communicate over a public or unsecured network with other service components or other ETSP(s) it services, the communications must be cryptographically authenticated by an authentication protocol that meets, as a minimum, the requirements of AL4 and encrypted using an approved encryption method.

AL4_CO_SCO#020 Protection of secrets

Ensure that:

a) access to shared secrets shall be subject to discretionary controls which permit access to those roles/applications which need such access;
b) stored shared secrets are encrypted such that:
c) the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2[1] Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and decrypted only as immediately required for an authentication operation;
d) they are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and is not exported in plaintext from the module;
e) they are split by an '*n from m*' cryptographic secret-sharing method.
f) any long-term (i.e. not session) shared secrets are revealed only to the Subscriber and the ETSP's direct agents (bearing in mind (a) above).

3.6 Identity Proofing Service Assessment Criteria

The Service Assessment Criteria in this section establish the requirements for the technical conformity of identity-proofing services at all ALs defined in Section 2. These criteria apply to a particular kind of electronic trust service (ETS) recognized by the EAP and to the related electronic trust service provider (ETSP)—an identity proofing service. (For definitions of terms used in this section, see Section 5). These criteria are generally referred to elsewhere within EAP documentation as ID-SAC.

These criteria do not address the delivery of a credential to the applicant/subscriber, which is dealt with by the Credential Management SAC (CM-SAC), described in Section 3.7.

These criteria may only be used in an assessment in one of the following circumstances:

- In conjunction with the Common Organizational SAC (CO-SAC), described in Section 3.5, for a standalone identity proofing service.
- In combination with one or more other SACs that must include the CO-SAC and where the identity proofing functions that these criteria address form part of a larger service offering.

3.6.1 ASSURANCE LEVEL 1 (MINIMAL)

3.6.1.1 Policy

An enterprise or specified service must:

[1] FIPS PUB 140-2 Security Requirements for Cryptographic Modules

AL1_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL1_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

3.6.1.2 Identity Verification

3.6.1.2.1 In-Person Public Verification

An enterprise or specified service must:

AL1_ID_IPV#010 Required evidence

Ensure that the Applicant possesses any one of the following forms of evidence:

a) one form of Federal or state-issued identity.
b) one signed bank or credit card.
c) two utility statements.
d) any other equivalent form of proof.

AL1_ID_IPV#020 Evidence checks

Ensure that the name on the evidence offered bears the name the Applicant claims and in addition establish, according to the form of evidence provided, any one of the following:

a) the Applicant appears to be the person named.
b) the Applicant can reproduce any signatures shown on bank cards.
c) addresses provided are consistent.
d) any other checks that establish an equivalent degree of certitude.

3.6.1.2.2 Remote Public Verification

If the specific service offers remote identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

An enterprise or specified service must::

AL1_ID_RPV#010 Required evidence

Require the Applicant to provide a contact telephone number or email address.

AL1_ID_RPV#020 Evidence checks

Verify the provided information by either:

a) confirming the request by calling the number.
b) successfully sending a confirmatory email and receiving a positive acknowledgement.

3.6.1.2.3 Secondary Verification

In each of the above cases an enterprise or specified service must:

AL1_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.1.3 Verification Records

No criteria.

3.6.2 ASSURANCE LEVEL 2 (MODERATE)

3.6.2.1 Policy

The specific service must show that it applies identity proofing policies and procedures and that it retains appropriate records of identity proofing activities and evidence.

The enterprise or specified service must:

AL2_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL2_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL2_ID_POL#030 Published Proofing Policy

Publish the Identity Proofing Policy under which it verifies the identity of applicants[2] in form, language and media accessible to the declared community of users.

AL2_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, through application of the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.2.2 Identity Verification

The specific service must offer at least one of the following classes of identity proofing service and may offer any additional sets it chooses, subject to the nature and the entitlement of the CSP concerned.

[2] For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

3.6.2.2.1 In-Person Public Verification

If the specific service offers in-person identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

The enterprise or specified service must:

AL2_ID_IPV#010 Required evidence

Ensure that the Applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.

AL2_ID_IPV#020 Evidence checks

Ensure that the presented document:
a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
b) bears a photographic image of the holder that matches that of the Applicant;
c) states an address at which the Applicant can be contacted.

3.6.2.2.2 Remote Public Verification

If the specific service offers remote identity proofing to applicants with whom it has no previous relationship, then it must comply with the criteria in this section.

An enterprise or specified service must:

AL2_ID_RPV#010 Required evidence

Ensure that the Applicant submits the references of and attests to current possession of a primary Government Picture ID document, and provides additional verifiable personal information that at a minimum must include:
a) a name that matches the referenced photo-ID.
b) date of birth.
c) current address or personal telephone number.
d) the issuer, account number and expiration date of a current credit card.

Additional information may be requested so as to ensure a unique identity, and alternative information may be sought where the enterprise can show that it leads to at least the same degree of certitude when verified.

AL2_ID_RPV#020 Evidence checks

Electronically verify by a record check against the provided identity references with the specified issuing authorities/institutions or through similar databases:
a) the existence of such records with matching name and reference numbers;
b) corroboration of date of birth, current address of record and other personal information sufficient to ensure a unique identity.

Additional checks may be performed so as to establish the uniqueness of the claimed identity, and alternative checks may be performed where the enterprise can show that they lead to at least the same degree of certitude.

3.6.2.2.3 Current Relationship Verification

If the specific service offers identity proofing to applicants with whom it has a current relationship, then it must comply with the criteria in this section.

The enterprise or specified service must:

AL2_ID_CRV#010 Required evidence

Ensure that it has previously exchanged a shared secret (e.g., a PIN or password) with the applicant.

AL2_ID_CRV#010 Evidence checks

Ensure that it has:

a) only issued the shared secret after originally establishing the applicant's identity with a degree of rigor equivalent to that required under either the AL2 (or higher) requirements for in-person or remote public verification
b) an ongoing business relationship sufficient to satisfy the enterprise of the applicant's continued personal possession of the shared secret.

3.6.2.2.4 Affiliation Verification

If the specific service offers identity proofing to applicants on the basis of some form of affiliation, then it must comply with the criteria in this section for the purposes of establishing that affiliation, in addition to the previously stated requirements for the verification of the individual's identity.

The enterprise or specified service must:

AL2_ID_AFV#010 Required evidence

Ensure that the Applicant possesses:

a) identification from the organization with which it is claiming Affiliation.
b) agreement from the organization that the Applicant may be issued a credential indicating that an affiliation exists.

AL2_ID_AFV#020 Evidence checks

Ensure that the presented documents:

a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application.
b) refer to an existing organization, with a contact address.
c) indicate that the Applicant has some form of recognizable affiliation with the organization.
d) appear to grant the Applicant an entitlement to obtain a credential indicating its affiliation with the organization.

3.6.2.2.5 Secondary Verification

In each of the above cases the enterprise or specified service must:

AL2_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can be reasonably anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.2.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes.

An enterprise or specified service must:

AL2_ID_VRC#010 Verification Records for Personal Applicants

Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process. At a minimum, records of identity information must include:

a) the Applicant's full legal name.
b) the Applicant's date of birth.
c) the Applicant's current address of record.
d) the Subscriber's current telephone or email address of record.
e) type, issuing authority and reference number(s) of all documents checked in the identity proofing process.
f) where required, a telephone or email address for related contact and/or delivery of credentials/notifications.
g) any pseudonym used by the Applicant in lieu of the verified identity.
h) date and time of verification.

AL2_ID_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process. At a minimum, records of identity information must include:

a) the Subscriber's full legal name.
b) the Subscriber's current address of record.
c) the Subscriber's current telephone or email address of record.
d) the Subscriber's acknowledgement for issuing the Subject with a credential.
e) type, issuing authority and reference number(s) of all documents checked in the identity proofing process.

AL2_ID_VRC#040 Record Retention

Either retain securely the record of the verification process for the duration of the subscriber account plus 7.5 years, or submit same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.3 ASSURANCE LEVEL 3 (SUBSTANTIAL)

3.6.3.1 Policy

The specific service must show that it applies identity-proofing policies and procedures and that it retains appropriate records of identity-proofing activities and evidence.

The enterprise or specified service must:

AL3_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL3_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL3_ID_POL#030 Published Proofing Policy

Publish the Identity Proofing Policy under which it verifies the identity of applicants[3] in form, language and media accessible to the declared community of Users.

AL3_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, applying the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.3.2 Identity Verification

The specific service must offer at least one of the following classes of identity proofing services and may offer any additional services it chooses, subject to the nature and the entitlement of the CSP concerned.

3.6.3.2.1 In-Person Public Verification

A specific service that offers identity proofing to applicants with whom it has no previous relationship must comply with the criteria in this section.

The enterprise or specified service must:

AL3_ID_IPV#010 Required evidence

Ensure that the Applicant is in possession of a primary Government Picture ID document that bears a photographic image of the holder.

AL3_ID_IPV#020 Evidence checks

Ensure that the presented document:

a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
b) bears a photographic image of the holder that matches that of the Applicant.
c) states an address at which the Applicant can be contacted.

[3] For an identity proofing service that is within the management scope of a Credential Management service provider, this should be the Credential Management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client who has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

d) is electronically verified by a record check with the specified issuing authority or through similar databases that:
   i) establishes the existence of such records with matching name and reference numbers.
   ii) corroborates date of birth, current address of record and other personal information sufficient to ensure a unique identity.

3.6.3.2.2 Remote Public Verification

A specific service that offers remote identity proofing to applicants with whom it has no previous relationship must comply with the criteria in this section.

The enterprise or specified service must:

AL3_ID_RPV#010 Required evidence

Ensure that the Applicant submits details of and attests to current possession of:

a) a primary Government Picture ID document, and either
   i) an account number issued by a regulated financial institution.
   ii) a source of personal information relating to the applicant.

AL3_ID_RPV#020 Evidence checks

Electronically verify by a record check against the provided identity references with the specified issuing authorities/institutions or through similar databases:

a) the existence of such records with matching name and reference numbers.
b) corroboration of date of birth, current address of record or personal telephone number, and other personal information sufficient to ensure a unique identity.
c) dynamic verification of personal information previously provided by or likely to be known only by the applicant.

3.6.3.2.3 Affiliation Verification

A specific service that offers identity proofing to applicants on the basis of some form of affiliation must comply with the criteria in this section to establish that affiliation and with the previously stated requirements to verify the individual's identity.

The enterprise or specified service must:

AL3_ID_AFV#010 Required evidence

Ensure that the Applicant possesses:

a) identification from the organization with which it is claiming Affiliation.
b) agreement from the organization that the Applicant may be issued a credential indicating that an affiliation exists.

AL3_ID_AFV#020 Evidence checks

Ensure that the presented documents:

a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application.
b) refer to an existing organization, with a contact address.

c) indicate that the Applicant has some form of recognizable affiliation with the organization.
d) appear to grant the Applicant an entitlement to obtain a credential indicating an affiliation with the organization.

3.6.3.2.4 Secondary Verification

In each of the above cases, the enterprise or specified service must also meet the following criteria:

AL3_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstance that can reasonably be anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.3.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes.

The enterprise or specified service must:

AL3_ID_VRC#010 Verification Records

Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process. At a minimum, records of identity information must include:
a) the Applicant's full legal name.
b) the Applicant's date and place of birth (as declared, but not necessarily verified).
c) the Applicant's current address of record.
d) the Subscriber's current telephone or email address of record.
e) type, issuing authority and reference number(s) of all documents checked in the identity proofing process.
f) any pseudonym used by the Applicant in lieu of the verified identity**.**
g) date and time of verification.
h) where the identity proofing is conducted in person, the signature of the Applicant.
i) identity of the registrar.
j) identity of the CSP providing the verification service or the location at which the (in-house) verification was performed.

AL3_ID_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process. At a minimum, records of identity information must include:
a) the Subscriber's full legal name.
b) the Subscriber's current address of record.
c) the Subscriber's current telephone or email address of record.
d) the Subscriber's acknowledgement of issuing the subject with a credential.
e) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process.

f) where required, a telephone or email address for related contact and/or delivery of credentials/notifications.

AL3_ID_VRC#040 Record Retention

Either retain securely the record of the verification/revocation process for the duration of the Subscriber account plus 7.5 years, or submit the same record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.4 ASSURANCE LEVEL 4 (HIGH)

Identity proofing at Assurance Level 4 requires the physical presence of the applicant in front of the registration officer with photo ID or other readily verifiable biometric identity information, as well as the requirements set out by the following criteria.

3.6.4.1 Policy

The specific service must show that it applies identity-proofing policies and procedures and that it retains appropriate records of identity-proofing activities and evidence.

The enterprise or specified service must:

AL4_ID_POL#010 Unique service identity

Ensure that a unique identity is attributed to the specific service, such that credentials issued by it can be distinguishable from those issued by other services, including services operated by the same enterprise.

AL4_ID_POL#020 Unique subject identity

Ensure that each Applicant's identity is unique within the service's community of subjects and uniquely associable with tokens and/or credentials issued to that identity.

AL4_ID_POL#030 Published Proofing Policy

Publish the Identity Proofing Policy under which it verifies the identity of applicants[4] in form, language and media accessible to the declared community of users.

AL4_ID_POL#040 Adherence to Proofing Policy

Perform all identity proofing strictly in accordance with its published Identity Proofing Policy, applying the procedures and processes set out in its Identity Proofing Practice Statement.

3.6.4.2 Identity Verification

The specific service may offer only face-to-face identity proofing service. Remote verification is not allowed at this level.

[4] For an identity proofing service that is within the management scope of a credential management service provider, this should be the credential management service's definitive policy; for a stand-alone identity proofing service, the policy may be either that of a client which has defined one through contract, the ID service's own policy or a separate policy that explains how the client's policies will be complied with.

The enterprise or specified service must:

3.6.4.2.1 In-Person Public Verification

AL4_ID_IPV#010 Required evidence

Ensure that the Applicant is in possession of:

a) a primary Government Picture ID document that bears a photographic image of the holder and either
   - i) secondary Government Picture ID or an account number issued by a regulated financial institution.
   - ii) two items confirming name, and address or telephone number, such as: utility bill, professional license or membership, or other evidence of equivalent standing.

AL4_ID_IPV#020 Evidence checks – primary ID

Ensure that the presented document:

a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
b) bears a photographic image of the holder which matches that of the Applicant.
c) states an address at which the Applicant can be contacted.
d) is electronically verified by a record check with the specified issuing authority or through similar databases that:
   - i) establishes the existence of such records with matching name and reference numbers.
   - ii) corroborates date of birth, current address of record and other personal information sufficient to ensure a unique identity.

AL4_ID_IPV#030 Evidence checks – secondary ID

Ensure that the presented document meets the following conditions:

1) If it is secondary Government Picture ID,
   - a) appears to be a genuine document properly issued by the claimed issuing authority and valid at the time of application.
   - b) bears a photographic image of the holder which matches that of the applicant.
   - c) states an address at which the Applicant can be contacted.
2) If it is a financial institution account number,
   - a) is verified by a record check with the specified issuing authority or through similar databases that :
     - i) establishes the existence of such records with matching name and reference numbers.
     - ii) corroborates date of birth, current address of record and other personal information sufficient to ensure a unique identity.
3) If it is two utility bills or equivalent documents,
   - a) each appears to be a genuine document properly issued by the claimed issuing authority.
   - b) corroborates current address of record or telephone number sufficient to ensure a unique identity.

AL4_ID_IPV#050 Applicant knowledge checks

Where the Applicant is unable to satisfy any of the above requirements, that the applicant can provide a Social Security Number (SSN) that matches the claimed identity.

3.6.4.2.2 Affiliation Verification

A specific service that offers identity proofing to applicants on the basis of some form of affiliation must comply with the criteria in this section to establish that affiliation, in addition to complying with the previously stated requirements for verifying the individual's identity.

The enterprise or specified service must:

AL4_ID_AFV#010 Required evidence

Ensure that the Applicant possesses:

a) identification from the organization with which the Applicant is claiming Affiliation.
b) agreement from the organization that the Applicant may be issued a credential indicating that an affiliation exists.

AL4_ID_AFV#020 Evidence checks

Ensure that the presented documents:

a) each appear to be a genuine document properly issued by the claimed issuing authorities and valid at the time of application.
b) refer to an existing organization, with a contact address.
c) indicate that the Applicant has some form of recognizable affiliation with the organization.
d) appear to grant the Applicant an entitlement to obtain a credential indicating an affiliation with the organization.

3.6.4.2.3 Secondary Verification

In each of the above cases, the enterprise or specified service must also meet the following criteria:

AL4_ID_SCV#010 Secondary checks

Have in place additional measures (e.g., require additional documentary evidence, delay completion while out-of-band checks are undertaken) to deal with any anomalous circumstances that can reasonably be anticipated (e.g., a legitimate and recent change of address that has yet to be established as the address of record).

3.6.4.3 Verification Records

The specific service must retain records of the identity proofing (verification) that it undertakes.

The enterprise or specified service must:

AL4_ID_VRC#010 Verification Records

Log, taking account of all applicable legislative and policy obligations, a record of the facts of the verification process. At a minimum, records of identity information must include:

a) the Applicant's full legal name.
b) the Applicant's date and place of birth (as declared, but not necessarily verified).
c) the Applicant's current address of record.
d) the type, issuing authority and reference number(s) of all documents checked in the identity-proofing process.

e) a telephone or email address for related contact and/or delivery of credentials/notifications.
f) any pseudonym used by the Applicant in lieu of the verified identity.
g) a biometric record of the Applicant (e.g., a photograph, fingerprint, voice recording).
h) date and time of verification, issued by a trusted time-source.
i) the signature of the Applicant.
j) identity of the registrar.
k) identity of the CSP providing the verification service or the location at which the (in-house) verification was performed.

AL4_ID_VRC#020 Verification Records for Affiliated Applicants

In addition to the foregoing, log, taking account of all applicable legislative and policy obligations, a record of the additional facts of the verification process. At a minimum, records of identity information must include:
a) the Subscriber's full legal name.
b) the Subscriber's current address of record.
c) the Subscriber's current telephone or email address of record.
d) the Subscriber's authorization for issuing the Subject a credential.
e) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process.
f) a biometric record of each required representative of the affiliating organization (e.g., a photograph, fingerprint, voice recording), as determined by that organization's governance rules/charter.

AL4_ID_VRC#040 Record Retention

Either retain securely the record of the verification/revocation process for the duration of the Subscriber account plus 10.5 years, or submit the record to a client CSP that has undertaken to retain the record for the requisite period or longer.

3.6.5 COMPLIANCE TABLES

Use the following tables to correlate criteria for a particular AL and the evidence offered to support compliance.

CSPs preparing for an assessment can use the table appropriate to the level at which they are seeking approval to correlate evidence with criteria or to justify nonapplicability (e.g., "specific service types not offered"). Assessors can use the tables to record assessment steps and their determination of compliance or failure. (

(THESE TABLES, AND OTHER BLANK TABLES IN PART 3, WILL BE COOMPLETED PRIOR TO PUBLIC EXPOSURE OF THE FRAMEWORK IN JANUARY 2005.)

Table 3-1. ID-SAC - AL1 Compliance

Clause	Description	Compliance
AL1_ID_POL#010	Unique service identity	
AL1_ID_POL#020	Unique subject identity	
AL1_ID_IPV#010	Required evidence	
AL1_ID_IPV#020	Evidence checks	
AL1_ID_RPV#010	Required evidence	
AL1_ID_RPV#020	Evidence checks	
AL1_ID_SCV#010	Secondary checks	

Table 3-2. ID-SAC - AL2 Compliance

Clause	Description	Compliance

Table 3-3. ID-SAC - AL31 compliance

Clause	Description	Compliance

Table 3-4. ID-SAC - AL4 compliance

Clause	Description	Compliance

3.7 Credential Management Service Assessment Criteria

The Service Assessment Criteria in this section establish requirements for the functional conformity of credential management services and their providers at all ALs defined in Section 2. These criteria are generally referred to elsewhere within EAP documentation as CM-SAC.

The criteria are divided into five parts. Each part deals with a specific functional aspect of the overall credential management process.

This SAC must be used in conjunction with the Common Organizational SAC (CO-SAC), described in Section 3.5, and in addition must either:

- Explicitly include the criteria of the Identity Proofing SAC (ID-SAC) described in Section 3.6, or
- Rely upon the criteria of the ID-SAC being fulfilled by the use of an EAP-approved ID-proofing service.

3.7.1 PART A--CREDENTIAL OPERATING ENVIRONMENT

The criteria in this part deal with the overall operational environment in which the credential life-cycle management is conducted. The credential management service assessment criteria must be used in conjunction with the common organizational criteria described in Section 3.5. In addition, they must either explicitly include the identify-proofing service assessment criteria described in Section 3.6 or rely upon those criteria being fulfilled by the use of an EAP-approved identity-proofing service.

These criteria describe requirements for the overall operational environment in which credential life-cycle management is conducted. The common organizational criteria describe broad requirements. The criteria in this section describe implementation specifics. Implementation depends on the AL. The procedures and processes required to create a secure environment for management of credentials and the particular technologies that are considered strong enough to meet the assurance requirements differ considerably from level to level.

3.7.1.1 Assurance Level 1 (Minimal)

These criteria apply to PINs and passwords.

3.7.1.1.1 Credential Policy and Practices

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL1_CM_CPP#010 Credential Policy and Practice Statement

No stipulation.

3.7.1.1.2 Security Controls

An enterprise and its specified service must:

AL1_CM_CTR#010 Secret revelation

No stipulation.

AL1_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats and apply appropriate controls:

a) password guessing.
b) message replay.

AL1_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats and apply appropriate controls:

a) the introduction of malicious code.
b) compromised authentication arising from insider action.
c) out-of-band attacks by other users and system operators (e.g., shoulder-surfing).
d) spoofing of system elements/applications.
e) malfeasance on the part of subscribers and subjects.

3.7.1.1.3 Storage of Long-term Secrets

An enterprise and its specified service must:

AL1_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and apply discretionary access controls that limit access to administrators and those applications that require access.

3.7.1.1.4 Security-relevant Event (Audit) Records

No stipulation.

3.7.1.1.5 Subject Options

An enterprise and its specified service must:

AL1_CM_OPN#010 Changeable PIN/Password

Permit subjects to change their PINs/passwords.

3.7.1.2 Assurance Level 2 (Moderate)

These criteria apply to passwords.

3.7.1.2.1 Credential Policy & Practices

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL2_CM_CPP#010 Credential Policy and Practice Statement

Include in its Service Definition a description of the Policy against which it issues credentials and the corresponding Practices it applies in their management. At a minimum the Policy and Practice Statement must specify:

a) if applicable, any OIDs related to the Practice & Policy Statement;
b) how users may subscribe to the service/apply for credentials and how users' credentials will be delivered to them.
c) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in credential status directories).
d) how credentials may be renewed, modified, revoked and suspended, including how requestors are authenticated or their identity re-proven.
e) what actions a subscriber must take to terminate a subscription.

AL2_CM_CPP#020 Management Authority

Have a nominated management body with authority and responsibility for approving the Credential Policy & Practice Statement and for its implementation.

3.7.1.2.2 Security Controls

An enterprise and its specified service must:

AL2_CM_CTR#010 Secret revelation

Use communication and authentication protocols that minimize the duration of any clear-text disclosure of long-term secrets, even when disclosed to trusted parties.

AL2_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:
a) password guessing.
b) message replay.
c) eavesdropping.

AL2_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats in its risk assessment and apply controls that reduce them to acceptable risk levels:
a) the introduction of malicious code.
b) compromised authentication arising from insider action.
c) out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing).
d) spoofing of system elements/applications.
e) malfeasance on the part of subscribers and subjects.
f) intrusions leading to information theft.

AL2_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage and destruction of its own cryptographic keys used for securing the Specific Service's assertions and other publicized information. At a minimum these should address:
a) the physical security of the environment.
b) access control procedures limiting access to the minimum number of authorized personnel.
c) public-key publication mechanisms.
d) application of controls deemed necessary as a result of the service's risk assessment.
e) destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner that prohibits their reuse.

3.7.1.2.3 Storage of Long-term Secrets

An enterprise and its specified service must:

AL2_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and apply discretionary access controls that limit access to administrators and to those applications requiring access.

3.7.1.2.4 Security-Relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria applying to provision of an auditable log of all events pertinent to the correct and secure operation of the service must also be considered carefully. These criteria carry implications for credential management operations.

3.7.1.2.5 Subject Options

An enterprise and its specified service must:

AL2_CM_OPN#010 Changeable PIN/Password

Permit Subjects to change their passwords.

3.7.1.3 Assurance Level 3 (Substantial)

These criteria apply to one-time password devices and soft crypto applications protected by passwords or biometric controls.

3.7.1.3.1 Credential Policy & Practices

These criteria apply to the policy and practices under which credentials are managed.

An enterprise and its specified service must:

AL3_CM_CPP#010 Credential Policy & Practice Statement

Include in its Service Definition a full description of the Policy against which it issues credentials and the corresponding Practices it applies in their issuance. At a minimum the Practice and Policy Statement must specify:

a) if applicable, any OIDs related to the Practice & Policy Statement.
b) how users may subscribe to the service/apply for credentials and how the users' credentials will be delivered to them.
c) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in credential status directories).
d) how credentials may be renewed, modified, revoked and suspended, including how requestors are authenticated or their identity -proven.
e) what actions a subscriber must take to terminate a subscription.

AL3_CM_CPP#020 Management Authority

Have a nominated management body with authority and responsibility for approving the Credential Policy & Practice Statement, and for its implementation.

3.7.1.3.2 Security Controls

AL3_CM_CTR#010 Secret revelation

Use communication and authentication protocols that minimize the duration of any clear-text disclosure of long-term secrets, even when disclosed to ostensibly trusted parties.

AL3_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

a) password guessing.
b) message replay.
c) eavesdropping.
d) relying party (verifier) impersonation.
e) man-in-the-middle attack.

AL3_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats in its risk assessment and apply controls that reduce them to acceptable risk levels:

a) the introduction of malicious code.
b) compromised authentication arising from insider action.
c) out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing).
d) spoofing of system elements/applications.
e) malfeasance on the part of subscribers and subjects.
f) intrusions leading to information theft.

AL3_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage and destruction of its own cryptographic keys used for securing the Specific Service's assertions and other publicized information. At a minimum, these should address:

a) the physical security of the environment.
b) access control procedures limiting access to the minimum number of authorized personnel.
c) public-key publication mechanisms.
d) application of controls deemed necessary as a result of the service's risk assessment.
e) destruction of expired or compromised private keys in a manner that prohibits their retrieval **or** their archival in a manner that prohibits their reuse.

3.7.1.3.3 Storage of Long-term Secrets

An enterprise and its specified service must:

AL3_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and apply discretionary access controls that limit access to administrators and to those applications that require access.

AL3_CM_STS#020 Stored Secret Encryption

Encrypt such shared secret files so that:

a) the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module.
b) the shared secret file is decrypted only as immediately required for an authentication operation.
c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported from the module in plain text.
d) shared secrets are split by an *n from m* cryptographic secret sharing method.

3.7.1.3.4 Security-relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria applying to the recording of all security-related events must also be considered carefully. These criteria carry implications for credential management operations.

In the specific context of a certificate management service, an enterprise and its specified service must:

AL3_CM_SER#010 Security event logging

Ensure that such audit records include:
a) the identity of the point of Registration (irrespective of whether internal or outsourced).
b) generation of the subscriber's keys or the evidence that the subscriber was in possession of both parts of their own key-pair.
c) generation of the subscriber's certificate.
d) dissemination of the subscriber's certificate.
e) any revocation or suspension associated with the subscriber's certificate.

3.7.1.3.5 Subject options

An enterprise and its specified service must:

AL3_CM_OPN#010 Changeable PIN/Password

Permit Subjects to change the password used to activate their credentials.

3.7.1.4 Assurance Level 4 (High)

These criteria apply exclusively to cryptographic technology deployed through a Public Key Infrastructure. This technology requires hardware tokens protected by password or biometric controls. No other forms of credential are permitted at AL4.

3.7.1.4.1 Certification Policy and Practices

These criteria apply to the policy and practices under which certificates are managed.

An enterprise and its specified service must:

AL4_CM_CPP#010 Certificate Policy/Certification Practice Statement

Include in its Service Definition its full Certificate Policy and the corresponding Certification Practice Statement. The Certificate Policy and Certification Practice Statement must conform to IETF RFC 3647 (2003-11) in their content and scope or be demonstrably consistent with the content or scope of that RFC. At a minimum, the Certificate Policy must specify:
a) applicable OIDs for each certificate type issued.
b) how users may subscribe to the service/apply for certificates, and how certificates will be issued to them.
c) if users present their own keys, how they will be required to demonstrate possession of the private key;.
d) if users' keys are generated for them, how the private keys will be delivered to them.
e) how subscribers acknowledge receipt of tokens and credentials and what obligations they accept in so doing (including whether they consent to publication of their details in certificate status directories).

f) how certificates may be renewed, re-keyed, modified, revoked and suspended, including how requestors are authenticated or their identity proven.
g) what actions a subscriber must take to terminate their subscription.

AL4_CM_CPP#020 Management Authority

Have a nominated high-level management body with authority and responsibility for approving the Certificate Policy and Certification Practice Statement, including ultimate responsibility for its proper implementation.

3.7.1.4.2 Security Controls

An enterprise and its specified service must:

AL4_CM_CTR#010 Secret revelation

Use communication and authentication protocols that minimize the duration of any clear-text disclosure of long-term secrets, even when disclosed to ostensibly trusted parties, which must themselves be authenticated prior to being granted access to any sensitive information.

AL4_CM_CTR#020 Protocol threat risk assessment and controls

Account for the following protocol threats in its risk assessment and apply controls that reduce them to acceptable risk levels:
a) password guessing.
b) message replay.
c) eavesdropping.
d) relying party (verifier) impersonation.
e) man-in-the-middle attack.
f) session hijacking.

AL4_CM_CTR#030 System threat risk assessment and controls

Account for the following system threats in its risk assessment and apply controls that reduce them to acceptable risk levels:
a) the introduction of malicious code.
b) compromised authentication arising from insider action.
c) out-of-band attacks by both users and system operators (e.g., the ubiquitous shoulder-surfing).
d) spoofing of system elements/applications.
e) malfeasance on the part of subscribers and subjects.
f) intrusions leading to information theft.

AL4_CM_CTR#040 Specified Service's Key Management

Specify and observe procedures and processes for the generation, storage and destruction of its own cryptographic keys used for securing the Specific Service's assertions and other publicized information. At a minimum, these should address:
a) the physical security of the environment.
b) access control procedures limiting access to the minimum number of authorized personnel.
c) public-key publication mechanisms.
d) application of controls deemed necessary as a result of the service's risk assessment.

e) destruction of expired or compromised private keys in a manner that prohibits their retrieval, or their archival in a manner which prohibits their reuse;

3.7.1.4.3 Storage of Long-term Secrets

The enterprise and its specified service must meet the following criteria:

AL4_CM_STS#010 Stored Secrets

Not store secrets (such as passwords) as plain text and must apply discretionary access controls that limit access to administrators and to those applications that require access.

AL4_CM_STS#020 Stored Secret Encryption

Encrypt such shared secret files so that:

a) the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module.
b) the shared secret file is decrypted only as immediately required for an authentication operation.
c) shared secrets are protected as a key within the boundary of a FIPS 140-2 Level 2 or higher validated hardware cryptographic module or any FIPS 140-2 Level 3 or 4 cryptographic module and are not exported from the module in plaintext.
d) shared secrets are split by an *n from m* cryptographic secret sharing method.

3.7.1.4.4 Security-relevant Event (Audit) Records

These criteria describe the need to provide an auditable log of all events that are pertinent to the correct and secure operation of the service. The common organizational criteria relating to the recording of all security-related events must also be considered carefully. These criteria carry implications for credential management operations.

An enterprise and its specified service must:

AL4_CM_SER#010 Security event logging

Ensure that such audit records include:

a) the identity of the point of Registration (whether internal or outsourced).
b) generation of the subscriber’s keys or evidence that the subscriber was in possession of both parts of the key-pair.
c) generation of the subscriber’s certificate.
d) dissemination of the subscriber’s certificate.
e) any revocation or suspension associated with the subscriber’s certificate.

3.7.1.4.5 Subject Options

An enterprise and its specified service must:

AL4_CM_OPN#010 Changeable PIN/Password

Permit Subjects to change the passwords used to activate their credentials.

3.7.2 PART B--CREDENTIAL ISSUING

These criteria apply to the verification of the identity of the subject of a credential and with token strength and credential delivery mechanisms. They address requirements levied by the use of various technologies to achieve the appropriate AL.[5] These criteria include by reference all applicable criteria in Section 3.6.

3.7.2.1 Assurance Level 1 (Minimal)

3.7.2.1.1 Identity Proofing

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity proofing functions.

The enterprise and its specified service must:

AL1_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity-proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria[6,7] for AL1 or higher.

AL1_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL1 or higher.

AL1_CM_IDP#030 Non EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions, ensure that each provider of such a service demonstrates compliance with all applicable identity-proofing service assessment criteria[4] for AL1 or higher, and that the enterprise itself has in place controls to ensure the continued fulfillment of those criteria by the provider to which the functions have been outsourced.

AL1_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to amend their stored information after registration.

3.7.2.1.2 Credential Creation

These criteria address the requirements for creation of credentials that can only be used at AL1. Any

[5] Largely driven by the guidance in NIST SP 800-63.

[6] Formal reference of this document is *EAP CSAC 04011, "ID-SAC"*

[7] Not all criteria may be applicable – the precise scope (definition) of the identity proofing performed by a particular service may exclude certain functionality and therefore certain criteria.

credentials/tokens that comply with the criteria stipulated for AL2 and higher are acceptable at AL1.

An enterprise and its specified service must:

AL1_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL1 or higher.

AL1_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community.

AL1_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

3.7.2.2 Assurance Level 2 (Moderate)

3.7.2.2.1 Identity Proofing

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity-proofing functions.

The enterprise and its specified service must:

AL2_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity-proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria for AL2 or higher.

AL2_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL2 or higher and that its approval has at least 6 months of remaining validity.

AL2_CM_IDP#030 Non EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions, ensure that each provider of such a service demonstrates compliance with all applicable identity-proofing service assessment criteria [3,4] for AL2 or higher, and that the enterprise itself has in place controls to ensure the continued fulfillment of those criteria by the provider to which the functions have been outsourced.

AL2_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision.

3.7.2.2.2 Credential Creation

These criteria define the requirements for creation of credentials whose highest use is at AL2. Credentials/tokens that comply with the criteria stipulated at AL3 and higher are also acceptable at AL2 and below.

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL2_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL2 or higher.

AL2_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community.

AL2_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

AL2_CM_CRN_#040 Password strength

Only allow passwords that, over the life of the password, have resistance to an on-line guessing attack against a selected user/password of at least 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies.

AL2_CM_CRN_#050 One-time password strength

Only allow password tokens that, over the life of the password, have a resistance to guessing of 1 in 2^{14} (16,384), accounting for state-of-the-art attack strategies.

AL2_CM_CRN_#060 Software cryptographic token strength

Refer to Section 3.7.2.3.

AL2_CM_CRN_#070 Hardware token strength

Refer to Section 3.7.2.3.

AL2_CM_CRN_#080 Binding of key

No stipulation.

AL2_CM_CRN_#090 Nature of subject

Record the nature of the subject of the credential (which must correspond to the manner of identity proofing performed), i.e., private person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.

3.7.2.2.3 Credential Delivery

An enterprise and its specified service must:

AL2_CM_CRD_#010 Confirm subject's details

Confirm the subject's contact details and notify the subject of the credential's issuance by:

a) sending notice to the address of record confirmed during Identity proofing or

b) issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during Identity proofing or

c) issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a telephone number or email at an email address supplied by the applicant during Identity proofing.

3.7.2.3 Assurance Level 3 (Substantial)

3.7.2.3.1 Identity Proofing

These criteria in this section determine how the enterprise shows compliance with the criteria for fulfilling identity-proofing functions.

The enterprise and its specified service must:

AL3_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria for AL3 or AL4.

AL3_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL3 or AL4 and that its approval has at least 6 months of remaining validity.

AL3_CM_IDP#030 Non EAP-approved outsourced service

Not use any non-EAP-approved outsourced services for identity proofing.

AL3_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision. Successful revision must, where necessary, instigate the re-issuance of the credential.

3.7.2.3.2 Credential Creation

These criteria define the requirements for creation of credentials whose highest use is AL3. Any credentials/tokens that comply with the criteria stipulated at AL4 are also acceptable at AL3 and below.

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL3_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL3 or higher.

AL3_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community, accounting fully for identities previously used and that are now cancelled.

AL3_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

AL3_CM_CRN_#040 PIN/Password strength

Not use PIN/password tokens.

AL3_CM_CRN_#050 One-time password strength

Only allow one-time password tokens that:

a) depend on a symmetric key stored on a personal hardware device evaluated against FIPS 140-2 Level 1 or higher.
b) permit at least 10^6 possible password values.
c) require password or biometric activation by the subscriber.

AL3_CM_CRN_#060 Software cryptographic token strength

Ensure that software cryptographic keys stored on general-purpose devices:

a) are protected by a key and cryptographic protocol that are evaluated against FIPS 140-2 Level 2.
b) require password or biometric activation by the subscriber or employ a password protocol when being used for authentication.

AL3_CM_CRN_#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

a) employ a cryptographic module that is evaluated against FIPS 140-2 Level 1 or higher.

b) require password or biometric activation by the subscriber or also employ a password when being used for authentication.

AL3_CM_CRN_#080 Binding of key

If the Specified Service generates the subject's key pair, that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the secrecy of the private key, until it is accepted by the subject.

AL3_CM_CRN_#090 Nature of subject

Record the nature of the subject of the credential (which must correspond to the manner of identity proofing performed), i.e., private person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.

3.7.2.3.3 Subject Key Pair Generation

An enterprise and its specified service must:

AL3_CM_SKP_#010 Key generation by Specified Service

If the Specified Service generates the Subject's keys:

a) use a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.
b) only create keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.
c) generate and store the keys securely until delivery to and acceptance by the Subject.
d) deliver the Subject's private key in a manner that ensures that the privacy of the key is not compromised and only the Subject has access to the private key.

AL3_CM_SKP_#020 Key generation by Subject

If the Subject generates and presents its own keys, obtain the Subject's written confirmation that it has:

a) used a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.
b) created keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.

3.7.2.3.4 Credential Delivery

An enterprise and its specified service must:

AL3_CM_CRD_#010 Confirm subject's details

Confirm the subject's contact details and notify the subject of the credential's issuance by:

a) sending notice to the address of record confirmed during Identity proofing, and either
   i) issuing the credential(s) in a manner that confirms the address of record supplied by the applicant during Identity proofing; or

ii) issuing the credential(s) in a manner that confirms the ability of the applicant to receive telephone communications at a phone number supplied by the applicant during Identity proofing while recording the applicant's voice.

AL3_CM_CRD_#020 Subject's acknowledgement

Receive acknowledgement of receipt of the credential before it is activated and its directory status record is published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).

3.7.2.4 Assurance Level 4 (High)

3.7.2.4.1 Identity Proofing

These criteria determine how the enterprise shows compliance with the criteria for fulfilling identity-proofing functions.

An enterprise and its specified service must:

AL4_CM_IDP#010 Self-managed Identity Proofing

If the enterprise assumes direct responsibility for identity-proofing functions, show, by direct inclusion, compliance with all applicable identity-proofing service assessment criteria for AL4.

AL4_CM_IDP#020 EAP-approved outsourced service

If the enterprise outsources responsibility for identity-proofing functions and uses a service already operating under an EAP Identity-proofing Approval, show that the service in question has been approved at AL4 and that its approval has at least 12 months of remaining validity.

AL4_CM_IDP#030 Non EAP-approved outsourced service

Not use any non-EAP-approved outsourced services for identity proofing unless they can be demonstrated to have satisfied equivalently rigorous requirements established by another scheme recognized by EAP.

AL4_CM_IDP#040 Revision to subscriber information

Provide a means for subscribers to securely amend their stored information after registration, either by re-proving their identity as in the initial registration process or by using their credentials to authenticate their revision. Successful revision must, where necessary, instigate the re-issuance of the credential.

3.7.2.4.2 Credential Creation

These criteria define the requirements for creation of credentials whose highest use is AL4.

Note, however, that a token and credential created according to these criteria may not necessarily provide that level of assurance for the claimed identity of the subscriber. Authentication can only be provided at the assurance level at which the identity is proven.

An enterprise and its specified service must:

AL4_CM_CRN_#010 Authenticated Request

Only accept a request to generate a credential and bind it to an identity if the source of the request can be authenticated as being authorized to perform Identity proofing at AL4.

AL4_CM_CRN_#020 Unique identity

Ensure that the identity (e.g., UserID) to which a credential is to be bound is unique within the Specified Service's intended community.

AL4_CM_CRN_#030 Token uniqueness

Allow the subscriber to select a unique token (e.g., UserID combined with PIN/password) that must be validated to be unique within the Specified Service's intended community and assigned uniquely to a single identity.

AL4_CM_CRN_#040 PIN/Password strength

Not use PIN/password tokens.

AL4_CM_CRN_#050 One-time password strength

Not use one-time password tokens.

AL4_CM_CRN_#060 Software cryptographic token strength

Not use software cryptographic tokens.

AL4_CM_CRN_#070 Hardware token strength

Ensure that hardware tokens used to store cryptographic keys:

a) employ a cryptographic module that is evaluated against FIPS 140-2 Level 2 or higher.
b) are evaluated against FIPS 140-2 Level 3 or higher for their physical security.
c) require password or biometric activation by the subscriber.

AL4_CM_CRN_#080 Binding of key

If the Specified Service generates the subject's key pair, that the key generation process securely and uniquely binds that process to the certificate generation and maintains at all times the secrecy of the private key, until it is accepted by the subject.

AL3_CM_CRN_#090 Nature of subject

Record the nature of the subject of the credential, i.e., private person, a named person acting on behalf of a corporation or other legal entity, corporation or legal entity, or corporate machine entity, in a manner that can be unequivocally associated with the credential and the identity that it asserts.

3.7.2.4.3 Subject Key Pair Generation

An enterprise and its specified service must:

AL4_CM_SKP_#010 Key generation by Specified Service

If the Specified Service generates the Subject's keys:

a) use a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.

b) only create keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.

c) generate and store the keys securely until delivery to and acceptance by the Subject;

d) deliver the Subject's private key in a manner that ensures that the privacy of the key is not compromised and only the Subject has access to the private key.

AL4_CM_SKP_#020 Key generation by Subject

If the Subject generates and presents its own keys, obtain the Subject's written confirmation that it has:

a) used a FIPS-approved algorithm that is recognized as being fit for the purposes of the service.

b) created keys of a key length and for use with a FIPS-approved public key algorithm recognized as being fit for the purposes of the service.

3.7.2.4.4 Credential Delivery

An enterprise and its specified service must:

AL4_CM_CRD_#010 Confirm subject's details

Confirm the subject's contact details and notify the subject of the credential's issuance by:

a) sending notice to the address of record confirmed during Identity proofing.

b) unless the subject presented with a private key, issuing the hardware token to the subject in a manner that confirms the address of record supplied by the applicant during Identity proofing.

c) issuing the certificate to the subject over a separate channel in a manner that confirms either the address of record or the email address supplied by the applicant during Identity proofing.

AL4_CM_CRD_#020 Subject's acknowledgement

Receive acknowledgement of receipt of the hardware token before it is activated and the corresponding certificate and its directory status record are published (and thereby the subscription becomes active or re-activated, depending upon the circumstances of issue).

3.7.3 PART C--CREDENTIAL REVOCATION

These criteria deal with credential revocation and the determination of the legitimacy of a revocation request.

3.7.3.1 Assurance Level 1 (Minimal)

An enterprise and its specified service must:

3.7.3.1.1 Not used

3.7.3.1.2 Not used

3.7.3.1.3 Secure Revocation Request

This criterion applies when revocation requests between remote components of a service are made over a secured communication.

An enterprise and its specified service must:

AL1_ID_SRR#010 Submit Request

Submit a request for revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.3.2 Assurance Level 2 (Moderate)

3.7.3.2.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL2_CM_RVP#010 Revocation procedures

State the conditions under which revocation of an issued credential may occur, the processes by which a revocation request may be submitted, the persons and organizations from which a revocation request will be accepted, the validation steps that will be applied to ensure the validity (identity) of the revocant, and the response time between a revocation request being accepted and the publication of revised certificate status.

AL2_CM_ RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL2_CM_ RVP#030 Revocation publication

Ensure that published credential status notification is revised within 72 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful.

AL2_ID_RVP#040 Verify revocation identity

Establish that the identity for which a revocation request is received is one that was issued by the Specified Service.

AL2_ID_RVP#050 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:
a) the Revocant’s full legal name.
b) the Revocant’s current address.

c) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process for the Revocant.
d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement or other legal due process).
e) the Subscriber's full legal name and, where applicable, unique service reference (e.g., certificate serial number, IP address).
f) the Subscriber's date of birth.
g) the Subscriber's current address of record.
h) the Credential Issuer's identity (if not directly responsible for the Identity Proofing service).
i) the identity associated with the credential (whether the Subscriber's name or a pseudonym).
j) the reason for revocation.

AL2_ID_PNR#060 Record Retention

Retain securely the record of the revocation process for the duration of the Subscriber's account plus 7.5 years.

3.7.3.2.2 Verify Revocant's Identity

The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not itself determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL3_ID_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received was one that was issued by the Specified Service.

AL2_ID_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well-founded, in combination with verification of the Revocant, according to AL2_ID_RVR#030, AL2_ID_RVR#040 or AL2_ID_RVR#050.

AL2_ID_RVR#030 Verify Subscriber as Revocant

When the Subscriber seeks revocation of the Subscriber's own credential, the enterprise must:
a) if in person, require presentation of a primary Government Picture ID document that must be electronically verified by a record check against the provided identity with the specified issuing authority's records, or
b) if remote:
   i. electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or
   ii. authenticate an electronic request as being from the same Subscriber, supported by a credential at Assurance Level 2 or higher.

AL2_ID_RVR#040 ETSP as Revocant

Where an CSP seeks revocation of a Subscriber's credential, the enterprise must establish that the request is either:

a) from the Specified Service itself, with authorization as determined by established procedures, or
b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL2_ID_RVR#050 Verify Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document, the enterprise must:
a) if in person, verify the identity of the person presenting the request, or
b) if remote:
   i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or
   ii. authenticate an electronic request as being from a recognized legal office, supported by a credential at Assurance Level 3 or higher.

3.7.3.2.3 Secure Revocation Request

This criterion requires that revocation requests between remote components of the service be made with secured communications.

An enterprise and its specified service must:

AL2_ID_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.3.3 Assurance Level 3 (Substantial)

3.7.3.3.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL3_CM_RVP#010 Revocation procedures

State the conditions under which revocation of an issued credential may occur, the processes by which a revocation request may be submitted, the persons and organizations from which a revocation request will be accepted, the validation steps that will be applied to ensure the validity (identity) of the revocant, and the response time between a revocation request being accepted and the publication of revised certificate status.

AL3_CM_ RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL3_CM_ RVP#030 Revocation publication

Ensure that published credential status notification is revised within 24 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful. The nature of the revocation mechanism shall be in accord with the technologies supported by the service.

AL3_ID_RVP#040 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:
a) the Revocant's full legal name.
b) the Revocant's current address.
c) type, issuing authority and reference number(s) of all documents checked in the identity proofing process for the Revocant.
d) the Revocant's authority to revoke (e.g., subscriber themselves, someone acting with the subscriber's power of attorney, the credential issuer, law enforcement or other legal due process).
e) the Subscriber's full legal name and, where applicable, unique service reference (e.g., certificate serial number, IP address).
f) the Subscriber's date of birth.
g) the Subscriber's current address of record.
h) the Credential Issuer's identity (if not directly responsible for the Identity Proofing service).
i) the identity associated with the credential (whether the Subscriber's name or a pseudonym).
j) the reason for revocation.

AL3_ID_RVP#050 Record Retention

Retain securely the record of the revocation process for the duration of the Subscriber's account plus 7.5 years.

3.7.3.3.2 Verify Revocant's Identity

Revocation of a credential requires that the requestor and the nature of the request be verified as rigorously as the original identity proofing. The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not itself determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL3_ID_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received is one that was initially issued by the Specified Service, applying the same process and criteria as would be applied to an original identity proofing.

AL3_ID_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well-founded, in combination with verification of the Revocant, according to AL3_ID_RVR#030, AL3_ID_RVR#040 or AL3_ID_RVR#050.

AL3_ID_RVR#030 Verify Subscriber as Revocant

When the Subscriber seeks revocation of the Subscriber's own credential:

a) if in-person, require presentation of a primary Government Picture ID document that must be electronically verified by a record check against the provided identity with the specified issuing authority's records, or
b) if remote:
   i. electronically verify a signature against records (if available), confirmed with a call to a telephone number of record, or
   ii. authenticate an electronic request as being from the same Subscriber, supported by a credential at Assurance Level 3 or higher.

AL3_ID_RVR#040 Verify ETSP as Revocant

Where an CSP seeks revocation of a Subscriber's credential, establish that the request is either:
a) from the Specified Service itself, with authorization as determined by established procedures, or
b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL3_ID_RVR#050 Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document:
a) if in person, verify the identity of the person presenting the request, or
b) if remote:
   i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or
   ii. authenticate an electronic request as being from a recognized legal office, supported by a credential at Assurance Level 3 or higher.

3.7.3.3.3 Secure Revocation Request

This criterion requires that revocation requests between remote components of the service be made with secured communications.

An enterprise and its specified service must:

AL3_ID_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.3.4 Assurance Level 4 (High)

3.7.3.4.1 Revocation Procedures

These criteria address general revocation functions, such as the processes involved and the basic requirements for publication.

An enterprise and its specified service must:

AL4_CM_RVP#010 Revocation procedures

State the conditions under which revocation of an issued certificate may occur, the processes by which a revocation request may be submitted, the persons and organizations from which a revocation request will be accepted, the validation steps that will be applied to ensure the validity (identity) of the revocant, and the response time between a revocation request being accepted and the publication of revised certificate status.

AL4_CM_ RVP#020 Secure status notification

Ensure that published credential status notification information can be relied upon in terms of the enterprise being its origin (i.e., its authenticity) and its correctness (i.e., its integrity).

AL4_CM_ RVP#030 Revocation publication

Ensure that published credential status notification is revised within 24 hours of the receipt of a valid revocation request, such that any subsequent attempts to use that credential in an authentication shall be unsuccessful. The nature of the revocation mechanism shall be in accord with the technologies supported by the service.

AL4_ID_RVP#040 Revocation Records

Retain a record of any revocation of a credential that is related to a specific identity previously verified, solely in connection to the stated credential. At a minimum, records of revocation must include:

a) the Revocant’s full legal name.
b) the Revocant’s current address.
c) type, issuing authority and reference number(s) of all documents checked in the identity-proofing process for the Revocant.
d) the Revocant’s authority to revoke (e.g., subscriber themselves, someone acting with the subscriber’s power of attorney, the credential issuer, law enforcement or other legal due process).
e) the Subscriber’s full legal name and, where applicable, unique service reference (e.g., certificate serial number, IP address).
f) the Subscriber’s date of birth.
g) the Subscriber’s current address of record.
h) the Credential Issuer’s identity (if not directly responsible for the Identity Proofing service).
i) the identity associated with the credential (whether the Subscriber’s name or a pseudonym).
j) the reason for revocation.

AL4_ID_RVP#050 Record Retention

Retain securely the record of the revocation process for the duration of the Subscriber’s account plus 7.5 years.

3.7.3.4.2 Revocation and Re-key

Revocation of a credential requires that the requestor and the nature of the request be verified as rigorously as the original identity proofing. The enterprise should not act on a request for revocation without first establishing the validity of the request (if it does not itself determine the need for revocation).

In order to do so, the enterprise and its specified service must:

AL3_ID_RVR#010 Verify revocation identity

Establish that the credential for which a revocation request is received is one that was initially issued by the Specified Service, applying the same process and criteria as would apply to an original identity proofing.

AL3_ID_RVR#020 Revocation reason

Establish the reason for the revocation request as being sound and well-founded, in combination with verification of the Revocant, according to AL4_CM_RVR#030, AL4_CM_RVR#040 or AL4_CM_RVR#050.

AL4_CM_RVR#030 Verify Subscriber as Revocant

Where the Subscriber seeks revocation of the Subscriber's own credential:

a) if in person, require presentation of a primary Government Picture ID document that shall be verified by a record check against the provided identity with the specified issuing authority's records, or
b) if remote:
    i. verify a signature against records (if available), confirmed with a call to a telephone number of record, or
    ii. authenticate an electronic request as being from the same Subscriber, supported by a different credential at Assurance Level 4.

AL4_CM_RVR#040 Verify ETSP as Revocant

Where an CSP seeks revocation of a Subscriber's credential, establish that the request is either:

a) from the Specified Service itself, with authorization as determined by established procedures, or
b) from the client Credential Issuer, by authentication of a formalized request over the established secure communications network.

AL4_CM_RVR#050 Legal Representative as Revocant

Where the request for revocation is made by a law enforcement officer or presentation of a legal document:

a) if in person, verify the identity of the person presenting the request, or
b) if remote:
    i. in paper/facsimile form, verify the origin of the legal document by a database check or by telephone with the issuing authority, or
    ii. authenticate an electronic request as being from a recognized legal office, supported by a different credential at Assurance Level 4.

Re-key of a credential requires that the requestor be verified as the subject with as much rigor as was applied to the original identity proofing. The enterprise should not act on a request for re-key without first establishing that the requestor is identical to the subject.

In order to do so, the enterprise and its specified service must:

AL4_CM_RKY#010 Verify Requestor as Subscriber

Where the Subscriber seeks a re-key for the Subscriber's own credential:

a) if in-person, require presentation of a primary Government Picture ID document that shall be verified by a record check against the provided identity with the specified issuing authority's records, or

b) if remote:

   i. verify a signature against records (if available), confirmed with a call to a telephone number of record, or

   ii. authenticate an electronic request as being from the same Subscriber, supported by a different credential at Assurance Level 4.

***3.7.3.4.3** Re-key requests from any other parties must not be accepted.*

3.7.3.4.4 Secure Revocation/Re-key Request

This criterion requires that revocation requests between remote components of the service be made with secured communications.

The enterprise and its specified service must:

AL4_ID_SRR#010 Submit Request

Submit a request for the revocation to the Credential Issuer service (function), using a secured network communication if necessary.

3.7.4 PART D--CREDENTIAL STATUS MANAGEMENT

These criteria deal with credential status management, such as the receipt of requests for new status information arising from a new credential being issued or a revocation or other change to the credential that requires notification. They also deal with the provision of status information to requesting parties having the right to access such information.

3.7.4.1 Assurance Level 1 (Minimal)

3.7.4.1.1 Status Maintenance

An enterprise and its specified service must:

AL1_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL1_CM_CSM#040 Status Information Availability

Provide, with 95% availability, a secure automated mechanism to allow Relying Parties to determine credential status and authenticate the subject's identity.

3.7.4.2 Assurance Level 2 (Moderate)

An enterprise and its specified service must:

AL2_CM_CSM#010 Maintain Status Record

Maintain a record of the status of all credentials issued.

AL2_CM_CSM#020 Validation of Status Change Requests

Authenticate all requestors seeking to have a change of status recorded and published and validate the requested change before considering processing the request. Such validation should include:

a) the requesting source as one from which the Specified Service expects to receive such requests.

b) if the request is not for a new status, the credential or identity as being one for which a status is already held.

AL2_CM_CSM#030 Revision to Published Status

Process authenticated requests for revised status information and have the revised information available for access within a period of 72 hours.

AL2_CM_CSM#040 Status Information Availability

Provide, with 95% availability, a secure automated mechanism to allow Relying Parties to determine credential status and authenticate the subject’s identity.

AL2_CM_CSM#050 Inactive Credentials

Disable any credential that has not been successfully authenticated during a period of 12 [AL3: 9] [AL4: 3] months.

3.7.4.3 Assurance Level 3 (Substantial)

3.7.4.4 Assurance Level 4 (High)

3.7.5 PART E--CREDENTIAL VALIDATION/AUTHENTICATION

These criteria apply to credential validation and identity authentication.

3.7.5.1 Assurance Level 1 (Minimal)

3.7.5.1.1 Assertion Security

An enterprise and its specified service must:

AL1_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a relying party using a protocol that:

a) requires authentication of the Specified Service or of the validation source.

b) ensures the integrity of the authentication assertion.

AL1_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL1_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL1_CM_ASS#040 Assertion Lifetime

No stipulation.

3.7.5.2 Assurance Level 2 (Moderate)

3.7.5.2.1 Assertion Security

An enterprise and its specified service must:

AL2_CM_ASS#010 Validation and Assertion Security

Provide validation of credentials to a relying party using a protocol that:
a) requires authentication of the Specified Service itself or of the validation source.
b) ensures the integrity of the authentication assertion.

AL2_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL2_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL2_CM_ASS#040 Assertion Lifetime

Generate assertions so as to indicate and effect their expiration 12 hours after their creation.

3.7.5.3 Assurance Level 3 (Substantial)

3.7.5.3.1 Assertion Security

An enterprise and its specified service must:

AL3_CM_ASS#010 Validation & Assertion Security

Provide validation of credentials to a relying party using a protocol that:
a) requires authentication of the Specified Service itself or of the validation source.
b) ensures the integrity of the authentication assertion.

AL3_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL3_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL3_CM_ASS#040 Assertion Lifetime

For non-cryptographic credentials**,** generate assertions that indicate and effect their expiration 12 hours after their creation; otherwise, notify the Relying Party of how often the revocation status sources are updated.

3.7.5.4 Assurance Level 4 (High)

3.7.5.4.1 Assertion Security

An enterprise and its specified service must:

AL4_CM_ASS#010 Validation & Assertion Security

Provide validation of credentials to a relying party using a protocol that:
a) requires authentication of the Specified Service itself or of the validation source.
b) ensures the integrity of the authentication assertion.

AL4_CM_ASS#020 No Post Authentication

Not authenticate credentials that have been revoked.

AL4_CM_ASS#030 Proof of Possession

Use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

AL4_CM_ASS#040 Assertion Lifetime

Notify the Relying Party of how often the revocation status sources are updated.

3.7.6 COMPLIANCE TABLES

Use the following tables to correlate criteria and evidence offered/compliance achieved. A table is provided for each assurance level. The tables are linked to their respective criteria and vice-versa, to aid referencing between them. Service providers preparing for an assessment can use the table appropriate to the level at which they are seeking approval to correlate evidence with criteria or to justify non-applicability of criteria (e.g., specific service types not offered): Assessors can use the tables to record the steps they take in their assessment and their determination of compliance or failure.

(THESE TABLES, AND OTHER BLANK TABLES IN PART 3, WILL BE COOMPLETED PRIOR TO PUBLIC EXPOSURE OF THE FRAMEWORK IN JANUARY 2005.)

Table 3-5 CM-SAC - AL1 Compliance

Clause	Description	Compliance

Table 3-6 CM-SAC - AL2 Compliance

Clause	Description	Compliance

Table 3-7 CM-SAC - AL3 Compliance

Clause	Description	Compliance

Table 3-8 CM-SAC - AL4 Compliance

Clause	Description	Compliance

4 ACCREDITATION AND CERTIFICATION RULES

4.1 **Assessor Accreditation** EAP certified services can be offered only by a CSP who is EAP-certified. EAP certification can only be granted by an EAP accredited assessor. Assessor accreditation requires the following steps:

1. An assessor submits an application for accreditation.
2. The EAP evaluates the application according to the criteria set for accreditation.
3. The applicant is notified of the EAP decision.
4. In the event of a negative decision, the applicant is offered an appeal.

4.1.1 CRITERIA FOR ASSESSOR ACCREDITATION

The Board of Directors or any committee or other entity the Board may empower by delegation (the Board) may choose to recognize the accreditation of another body in lieu of its own accreditation or as a supplement to its own accreditation. The Board shall apply the following criteria when determining whether to approve the application of an assessor for accreditation.

4.1.1.1 Expertise With Relevant Standards

Prior to accreditation, the assessor must demonstrate expertise in the application of at least one of the following evaluation standards. In addition, the assessor must demonstrate competence in the application of any supplemental evaluation criteria formally identified by the EAP and against which CSPs are to be assessed for certification by the EAP.

4.1.1.2 Business Expertise

The assessor must:

- Have been in existence for more than 1 month
- Be financially solvent and stable and reasonably certain to remain so for the foreseeable future
- Have sufficient financial resources, either through direct reserves, insurance or otherwise, to absorb the cost resulting from wrongful certification of a CSP upon its recommendation for the period of such certification and for 1 year thereafter
- Demonstrate excellence, breadth and depth in the relevant fields of endeavor, including electronic authentication, federated identity management, information security and the processes and methods of assessment of such fields
- Not have any key personnel or personnel directly involved in assessments or development and delivery of assessment reports and recommendations to the EAP who have been convicted of a crime

4.1.2 ASSESSMENT

Prior to accreditation, assessors may be subject to an on-site evaluation by the EAP or a designee. This assessment is to determine compliance with the current EAP criteria for accreditation and to evaluate expertise, processes and equipment necessary to conduct the certifications of CSPs according to EAP certification criteria and rules. Whether an on-site inspection is scheduled or not, the assessor shall provide information as provided for in Section 4.1.1.1 and Section 4.1.1.2.

4.1.3 ACCREDITATION DECISION AND APPEAL

Within a reasonable time and at the discretion of the EAP, the EAP shall make a determination of accreditation and communicate that determination to the applicant.

In the event of a negative decision, the assessor may request an appeal of the accreditation decision by the EAP. Such request shall be considered by a three-member panel of the EAP Board of Directors or any committee or other entity the Board may empower by delegation, composed of people who have been uninvolved with the decision and are impartial.

4.1.4 MAINTAINING ACCREDITATION

After the initial year of accreditation, assessors may be subject to an on-site or remote surveillance evaluation. The surveillance assessment shall include review of at least the following:

- Internal audit reports
- Minutes of management review meetings
- Results of certification assessments, if any
- Any changes in key personnel, facilities and/or major test equipment
- Information on any other significant changes in the quality system of the assessor

The EAP, or a designee, may conduct an on-site reassessment or surveillance assessment of accredited assessors at a minimum of once every 2 years, for verification of continued compliance with EAP accreditation criteria and rules.

4.2 Certification of Credential Service Provider Offerings

Only a CSP whose product or line of business is currently certified by the EAP can issue or otherwise purvey certified credentials or validation of EAP certified credentials under an EAP brand or EAP business rules or for use within the EAP system.

4.2.1 PROCESS OF CERTIFICATION

The process of certification for each product or line of business for which certification is sought by a CSP includes the following steps:

1. A CSP seeking certification for a product or line of business begins the formal process by reviewing the list of EAP accredited and approved assessors. The CSP selects an assessor for commencing formal assessment, for which there shall be a separate contractual arrangement between the applicant and the chosen assessor.

2. The EAP accredited assessor selected by the applicant conducts an assessment of the CSP product or line of business. At the conclusion of the assessment process, the assessor and the CSP separately submit their respective materials to the EAP.
3. The assessor submits the assessment report and its recommendation regarding certification directly to the EAP.
4. The CSP submits an application for certification to the EAP, including agreement to the EAP business rules and other relevant EAP binding documents, as well as specification of each line of offerings for which certification is sought, and the assurance level (AL) at which each certification is sought.
5. After receiving the assessment and application materials from the assessor and CSP, respectively, the EAP evaluates the relevant information and makes a decision on certification.
6. The EAP communicates its decision on certification to the CSP and the assessor.
7. In the event of a negative decision, the CSP is afforded an appeal.
8. In the event of a positive decision, the CSP's certified product or line of business is added to the EAP Certified CSP offering list.

4.2.1.1 Application

The EAP shall provide an application form for certification as an EAP CSP both on the EAP web site and in paper form. The application shall include contact information; an agreement to abide by the EAP rules and any other applicable EAP requirements identified in the application, such as a license agreement or other terms and conditions; and an EAP appeal request form to request review of the final certification determination. In addition, the application shall require the applicant to specify the precise scope of each line of business for which certification is sought, the AL at which each certification is sought, and any existing applicable accreditation, certification or similar approvals granted to each specified line of business.

4.2.1.2 Initial Evaluation

Upon receipt of an application for certification, the EAP shall review the contents and audit report.

4.2.1.3 Assessment

Prior to certification, CSPs may be subject to an on-site assessment by the assessor. The assessment shall determine compliance with the current EAP Service Assessment Criteria.

An EAP accredited assessor will conduct an on-site reassessment or surveillance assessment of a CSP at least 1 year after certification and, at a minimum, once every 2 years thereafter, for verification of continued compliance with EAP certification requirements.

4.2.2 CRITERIA FOR CERTIFICATION OF CSP LINE OF BUSINESS

4.2.2.1 Standard Evaluation Criteria Used by Assessor

For each line of business for which certification is sought, the practices, operations, organization, personnel and other relevant aspects of a CSP must be assessed against one of the following evaluation standards:

Table 4-1. Evaluation Standards for Different Assurance Levels

Assurance Level	Evaluation Standard
1	tbd
2	tbd
3	tbd
4	tbd

When multiple offerings share one or more assessment criteria, the criteria need only be considered once per assessment Such criteria may include management organization, physical security or personnel who are common to each line of business for which certification is sought. In addition, criteria that have been previously assessed positively by an adequate assessor and assessment process and that are equivalent to EAP criteria may be relied upon for purposes of an EAP assessment. Whether such criteria are deemed adequate and equivalent must be decided by the EAP Board. Such determination by the Board may be triggered by a request by a previously-assessed applicant CSP, an accredited assessor or on the initiative of the Board itself. Such determinations may be published from time to time as assessment guidance by the EAP.

4.2.2.2 Supplemental Criteria Used by Assessor

The criteria applied by assessors are identified in the EAP Service Assessment Criteria (Section 3).

4.2.3 CERTIFICATION DECISION

4.2.3.1 Assessor Delivers Report and Recommendation

Upon conclusion of the assessment, for each line of business for which certification has been sought, the assessor shall deliver to the EAP a final assessment report, including a recommendation on whether to certify the assessed CSP.

4.2.3.2 EAP Makes Certification Decision

Upon receipt of each assessment report and recommendation on certification from the assessor, the EAP shall determine, within a reasonable time to be set by the EAP Board, whether to deny certification to the CSP, certify the CSP, or take such other action as may be appropriate, including requesting further information, contractual agreements or provable action from the CSP by a certain date.

The decision of the EAP shall be communicated to both the CSP and the assessor within a reasonable time, to be set by the EAP Board.

4.2.4 APPEALS PROCESS

Upon receipt of the EAP decision on certification, a CSP may request an appeal of that decision. Upon receiving the Appeal Request from a CSP and within a reasonable period of time, to be set by the EAP Board, the EAP shall appoint a three-member review panel from among EAP Board of Directors or any committee or other entity the Board may empower by delegation, comprised of people who have been uninvolved with the decision at issue and are impartial. Said panel shall consider the request and make a final determination. The panel may make its determination based solely upon the information presented in the appeal request, including any attachments, or it may request additional information from one or more parties or schedule a hearing to permit the affected parties to further clarify and present their positions.

4.2.5 MAINTAINING CERTIFICATION

The CSP must notify the assessor and the EAP of any material change that may lower the assurance level of the certified product or line of business 60 days before the change is performed or immediately upon the incidence of any unplanned change. The EAP, in consultation with the assessor, will determine whether the changes are sufficient to require re-assessment. The re-assessment, if required, need only cover those elements that have changed.

Annual renewal agreements are required for a certification to remain in effect. The CSP warrants continued compliance with the criteria of the assessment in this agreement and provides annual audit results. An independent third party must audit any certified product or line of business assessed at AL2 or higher every 2 years. Other audits may be internal. The EAP, in consultation with the assessor, may require a partial reassessment if the scope of the audits does not include all applicable criteria. Additional maintenance activities may be stipulated in the participation agreement between the EAP and the CSP.

4.3 Process for Handing Non-Compliance

The following process for handling non-compliance applies both to accredited assessors and to certified CSPs, unless otherwise noted.

4.3.1 COMPLIANCE DETERMINATION

Upon receipt by the EAP of credible information that an assessor or CSP is not in compliance with the requirements for accreditation or certification, the EAP Board or staff or a committee at Board discretion shall determine whether the assessor or CSP is in fact in material non-compliance with EAP requirements and shall communicate the determination to the affected parties. The Board of Directors shall establish further criteria, as needed, detailing conduct or circumstances constituting material non-compliance with EAP rules or standards.

4.3.2 PERIOD TO CURE

An assessor or CSP found to be in material non-compliance shall be afforded an opportunity and period of time to remedy the non-compliance, provided such period does not unduly jeopardize the integrity of the EAP System or the rights or property of another party.

4.3.3 ADMINISTRATIVE RECOURSE

Based on review of all available data and in light of all the relevant circumstances, the EAP Board of Directors may take administrative recourse against any signatory determined to be in material non-compliance with these business rules, to include, as needed, any of the following remedies.

4.3.3.1 Warning

The non-complying party may be given a warning. The warning may be confidential or may be publicized within the EAP or publicized more broadly, at the discretion of the EAP Board of Directors.

4.3.3.2 Credential Revocation

The non-complying party may be required to revoke one or more EAP-branded credentials or to remove the EAP brand from such credentials.

4.3.3.3 Non-compliance Fees

The non-complying party may be subject to a schedule of fees, to be specified by the EAP Board of Directors. The fees may increase according to the length of time before the party comes back into compliance.

4.3.3.4 Suspension

The non-complying party may have its participation in the EAP System suspended, including the suspension of accreditation or certification, pending coming back into compliance.

4.3.3.5 Termination

The non-complying party may have its participation in the EAP System terminated, including the termination of accreditation or certification.

4.4 Acceptable Public Statements Regarding EAP Accreditation and Certification

It is acceptable for a party to indicate that it is an "EAP Accredited Assessor" or an "EAP Certified Credential Service Provider" for any period during which such statement is true. However, no party may make any public claim, whether to media outlets, in bids and other proposals, in marketing materials or otherwise, regarding its status as an applicant for accreditation or certification, nor can it claim that it is in the process of achieving such status.

5 EAP GLOSSARY

Accreditation. The process used to achieve formal recognition that an organization has agreed to the EAP operating rules and is competent to perform assessments using the Service Assessment Criteria.

AL. See *assurance level*

Applicant. An individual or person acting as a proxy for a machine or corporate entity who is the subject of an identity proofing process.

Approval. The process by which the EAP Board accepts the compliance of a certified service and the ETSP responsible for that service commits to upholding the EAP Rules.

Approved encryption. Any cryptographic algorithm or method specified in a FIPS or a NIST recommendation. Refer to http://csrc.nist.gov/cryptval/

Approved service. A certified service which has been granted an approval by the EAP Board.

Assertion. A statement from a verifier to a relying party that contains identity or other information about a subscriber.

Assessment. A process used to evaluate an electronic trust service and the service provider using the requirements specified by one or more Service Assessment Criteria for compliance with all applicable requirements.

Assessor. A person or corporate entity who performs an assessment.

Assurance level (AL) . A degree of certainty that a claimant has presented a credential that refers to the claimant's identity. Each assurance level expresses a degree of confidence in the process used to establish the identity of the individual to whom the credential was issued and a degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four assurance levels are:

Level 1 (Minimal): Little or no confidence in the asserted identity's validity
Level 2 (Moderate): Some confidence in the asserted identity's validity
Level 3 (Substantial): High confidence in the asserted identity's validity
Level 4 (High): Very high confidence in the asserted identity's validity

Attack. An attempt to obtain a subscriber's token or to fool a verifier into believing that an unauthorized individual possesses a claimant's token.

Attribute. A property associated with an individual.

Authentication. Authentication simply establishes identity, not what that identity is authorized to do or what access privileges he or she has.

Authentication protocol. A well-specified message exchange process that verifies possession of a token to remotely authenticate a claimant. Some authentication protocols also generate cryptographic keys that are used to protect an entire session, so that the data transferred in the session is cryptographically protected.

Authorization. Process of deciding what an individual ought to be allowed to do.

Bit. A binary digit: 0 or 1

Brand. See EAP Branded Credential.

Certification. The EAP's affirmation that a particular credential service provider can provide a particular credential service at a particular assurance level.

Claimant. A party whose identity is to be verified.

Certification Body. An organization which has been deemed competent to perform assessments of a particular type. Such assessments may be formal evaluations or testing and be based upon some defined set of standards or other criteria.

Certified service. An electronic trust service which has been assessed by an EAP-recognized certification body and found to be compliant with the applicable SACs.

Credential. An object to be verified when presented in an authentication transaction. A credential can be bound in some way to the individual to whom it was issued, or it can be a bearer credential. Electronic credentials are digital documents that bind an identity or an attribute to a subscriber's token.

Credential management. DEFINITION REQUIRED

Credential service. A type of electronic trust service that supports the verification of identities (identity proofing), the issuance of identity-related assertions/credentials/tokens, and the subsequent management of those credentials (for example, renewal, revocation and the provision of related status and authentication services).

Credential service provider (CSP) . An electronic trust service provider that operates one or more credential services. A CSP can include a Registration Authority.

Credential service. A reliable, efficient means of disseminating credential information.

CSP. See *credential service provider*.

Cryptographic token. A token for which the secret is a cryptographic key.

EAP. See *Electronic Authentication Partnership*

EAP assessor. An organization that has agreed to the EAP Rules and that has been accredited to conduct assessments of credential service providers.

EAP-branded credential. Information indicating the individual identity of a natural person, according to a CSP certified by the EAP to issue, process, validate or otherwise purvey such credential.

EAP credential service provider. Organization that has agreed to the EAP Operating Rules and other applicable Rules, and that has been Certified to issue, process, validate, etc., an EAP Branded Credential.

EAP credential service provider. Organization that has agreed to the EAP Rules and other applicable rules, and that has been certified to issue, process, and validate, an EAP-branded credential

EAP-recognized assessor. A body that has been granted an accreditation to perform assessments against Service Assessment Criteria, at the specified assurance level(s).

EAP-recognized certification body. A certification body which has been accredited by, or whose qualifications have been otherwise established by, a scheme which the EAP Board has deemed to be appropriate for the purposes of determining an ETSP's competence to perform assessments against EAP's criteria.

Electronic Authentication Partnership (EAP). The multi-industry partnership working on enabling interoperability among public and private electronic authentication (e-authentication) systems.

Electronic credentials. Digital documents used in authentication that bind an identity or an attribute to a subscriber's token.

Electronic trust service (ETS). A service that enhances trust and confidence in electronic transactions, typically but not necessarily using cryptographic techniques or involving confidential material such as PINs and passwords

Electronic trust service provider (ETSP). An entity that provides one or more electronic trust services.

ETS. See *electronic trust service*

ETSP. See e*lectronic trust service provider*

Federated identity management. A system that allows individuals to use the same user name, password, or other personal identification to sign on to the networks of more than one enterprise in order to conduct transactions.

Federal Information Processing Standards (FIPS) . Standards and guidelines issued by the National Institute of Standards and Technology (NIST) for use government-wide. NIST develops FIPS when the Federal government has compelling requirements, such as for security and interoperability, for which no industry standards or solutions are acceptable.

FIPS. See *Federal Information Processing Standards*

Identification. Process of using claimed or observed attributes of an individual to infer who the individual is.

Identifier. Something that points to an individual, such as a name, a serial number or some other pointer to the party being identified.

Identity authentication. Process of establishing an understood level of confidence that an identifier refers to an identity. It may or may not be possible to link the authenticated identity to an individual.

Identity. A unique name for single person. Because a person's legal name is not necessarily unique, identity must include enough additional information (for example, an address or some unique identifier such as an employee or account number) to make a unique name.

Identity binding. The extent to which an electronic credential can be trusted to be a proxy for the entity named in it.

Identity proofing. The process by which identity-related information is validated so as to identify a person with a degree of uniqueness and certitude sufficient for the purposes for which that identity is to be used.

Identity proofing policy. A set of rules that defines identity-proofing requirements (required evidence, format, manner of presentation, validation), records actions required of the registrar, and describes any other salient aspects of the identity-proofing function that are applicable to a particular community or class of applications with common security requirements. An identity proofing policy is designed to accomplish a stated assurance level.

Identity proofing service provider. An electronic trust service provider which offers, as a standalone service, the specific electronic trust service of identity proofing. This service provider is sometimes referred to as a Registration Agent/Authority (RA).

Identity proofing practice statement. A statement of the practices that an identity proofing service provider employs in providing its services in accordance with the applicable identity proofing policy.

Issuer. Somebody or something that supplies or distributes something officially.

Level of assurance. See *assurance level*

Network. An open communications medium, typically, the Internet, that is used to transport messages between the claimant and other parties.

Password. A shared secret character string used in authentication protocols. In many cases the claimant is expected to memorize the password.

Practice statement. A formal statement of the practices followed by an authentication entity (e.g., RA, CSP or verifier) that typically defines the specific steps taken to register and verify identities, issue credentials and authenticate claimants.

Public key. The public part of the asymmetric key pair that is typically used to verify signatures or encrypt data.

Public key infrastructure (PKI) . A set of technical and procedural measures used to manage public keys embedded in digital certificates. The keys in such certificates can be used to safeguard communication and data exchange over potentially unsecure networks.

Registration. An entry in a register, or somebody or something whose name or designation is entered in a register.

Relying party. An entity that relies upon a subscriber's credentials, typically to process a transaction or grant access to information or a system.

Role. The usual or expected function of somebody or something, or the part somebody or something plays in a particular action or event.

SAC. See *Service Assessment Criteria*

Security. A collection of safeguards that ensures the confidentiality of information, protects the integrity of information, ensures the availability of information, accounts for use of the system, and protects the system(s) and/or network(s) used to process the information.

Service Assessment Criteria (SAC) . A set of requirements levied upon specific organizational and other functions performed by electronic trust services and service providers. Services and service providers must comply with all applicable criteria to qualify for EAP approval.

Signatory. A party that opts into and agrees to be bound by the EAP Rules according to the specified procedures.

Specified service. The electronic trust service which for the purposes of an EAP assessment is the subject of criteria set out in a particular SAC, or in an application for assessment, in a grant of an approval or other similar usage as may be found in various EAP documentation.

Subject. An entity that is able to use an electronic trust service subject to agreement with an associated subscriber. A subject and a subscriber can be the same entity.

Subscriber. A party that has entered into an agreement to use an electronic trust service. A subscriber and a subject can be the same entity.

Threat. An adversary that is motivated and capable to violate the security of a target and has the capability to mount attacks that will exploit the target's vulnerabilities.

Token. Something that a claimant possesses and controls (typically a key or password) that is used to authenticate the claimant's identity.

Trust framework. The body of work that collectively defines the industry-led self-regulatory framework for electronic trust services in the United States, as operated by the EAP. The trust framework includes descriptions of criteria, rules, procedures, processes, and other documents.

Verification. Establishment of the truth or correctness of something by investigation of evidence.

6 PUBLICATION ACKNOWLEDGEMENTS

The EAP would like to thank the following working group chairs and vice chairs for their commitment and dedication to the Trust Framework.

Interim Chair: James Lewis, The Center for Strategic and International Studies
Interim Vice Chair: David Temoshok, U.S. General Services Administration

Business Requirements & Processes Work Group
Chair: Linda G. Elliot, PingID Network
Vice Chair: Thomas Greco, beTRUSTed

Credential Services Assessment Criteria & Levels of Assurance Work Group
Chair: Robert J. Schlecht, Mortgage Bankers Association of America
Vice Chair: Von Harrison, U.S. General Services Administration

Credential Services Assessment Criteria Sub Work
Chair: Nancy Black, HollenGroup
Vice Chair: Richard Wilsher, The Zygma Partnership

Levels of Assurance Sub Work Group
Chair: Peter Alterman, National Institutes of Health
Vice Chair: Noel Nazario, KPMG LLP

Interoperability Sub Work Group
Chair: William E. Burr, National Institute of Standards and Technology
Vice Chair: Kurt Van Etten, eBay, Inc.

Evaluation, Accreditation & Compliance Work Group
Chair: Gary Glickman, Giesecke & Devrient Cardtech, Inc.
Vice Chair: Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers

EAP Governance Work Group
Chair: Paula Arcioni, State of New Jersey, Office of Information Technology
Vice Chair: Roger J. Cochetti, CompTIA

Consultants
Yuriy Dzambasow, A&N Associates, Inc.
Dan Greenwood, Commonwealth of Massachusetts
Richard Wilsher, The Zygma Partnership

Members of the various work groups include:

Khaja Ahmed, Microsoft Corporation
Michael A. Aisenberg, VeriSign, Inc.
Peter Alterman, National Institutes of Health
Paula Arcioni, State of New Jersey, Office of Information Technology
Jonathan Askins, ACXIOM Corporation
Asaf Awan, Parkweb Associates
Stefano Baroni, SETECS

Paul Barrett, Real User Corporation
Nancy Black, Hollen Group
Debb Blanchard, Enspier Technologies/GDT
Warren Blosjo, 3Factor
Daniel Blum, Burton Group
Iana Bohmer, Northrop Grumman Information Technology
Christine Borucke, Electronic Data Systems
Kirk Brafford, SSP-Litronic, Inc.
Mayi Canales, M Squared Strategies, Inc.
Richard Carter, American Association of Motor Vehicles Administration
Kim Cartwright, Experian
James A. Casey, NeuStar, Inc.
Ray Cavanaugh. Entegrity Solutions
Chuck Chamberlain, U.S. Postal Service
Cornelia Chebinou, National Association of State Auditors, Comptrollers and Treasurers
Rebecca Chisolm, Sun Microsystems Federal
Roger J. Cochetti, CompTIA
Dan Combs, Global Identity Solutions
John Cornell, U.S. General Services Administration
Sarah Currier, CheckFree Corporation
Chris Daly, IBM Corporation
Kathy DiMaggio, Sigaba Corporation
Yuriy Dzambasow, A&N Associates, Inc.
Josh Elliott, American Management Systems
Clay Epstein, Indentrus LLC
Irving R. Gilson, Department of Defense
Gary Glickman, Giesecke & Devrient Cardtech, Inc.
James A. Gross, Wells Fargo
Kirk R. Hall, GeoTrust
Von Harrison, U.S. General Services Administration
Christopher Hankin, Sun Microsystems, Inc.
Michael Horkey, Global Identity Solutions
Katherine M. Hollis, Electronic Data Systems
Robert Housel, National City Corporation
Burt Kaliski, RSA Security, Inc.
Shannon Kellog, RSA Security, Inc.
James Kobielus, Burton Group
Patrick Lally, SSP-Litronic, Inc.
Steve Lazerowich, Enspier Technologies/GDT
Phillip S. Lee, SC Solutions, Inc.
Peter Lieberwirth, Authentidate
Chris Louden, Enspier Technologies/GDT
J. Scott Lowry, Enspier Technologies/GDT
Adele Marsh, PA Higher Education Assistance Agency
Patty McCarty, Private ID Systems
Doug McCoy, SAFLINK Corporation
Ben Miller, InsideID
Larry Miller, Identrus LLC
Sead Muftic, SETECS
Noel Nazario, KPMG LLP
Michael R. Nelson, IBM Corporation
Simon Nicholson, Sun Microsystems, Inc.

Pete Palmer, HIMSS NHII Task Force Advisor, Guidant Corporation
Stephen Permison, Standards Based Programs
Bob Pinheiro, Independent Security Researcher
Stephen L. Ranzini, University Bank
Christiane Reinhold, BearingPoint
Donald E. Rhodes, American Banker Association
Randy V. Sabett, Cooley Goodward, LLP
Ravi Sandhu, NSD Security
Dean Sarff, Minerals Management Service
Donald Saxinger, FDIC
Robert J. Schlecht, Mortgage Bankers Association of America
Howard Scmidt, eBay, Inc.
Ari Schwartz, Center for Democracy and Technology
John Shipley, The Shipley Group
Stephen P. Sill, U.S. General Services Administration
Helena G. Sims, NACHA – The Electronic Payments Association
Bill Smith, Sun Microsystems, Inc.
Tadgh Smith, IBM
Judith Spencer, U.S. General Services Administration
William Still, ChoicePoint Public Sector
Michael M. Talley, University Bancorp
David Temoshok, U.S. General Services Administration
Richard Thayer, ComTech, Inc.
John Ticer, NeuStar, Inc.
Kevin Trilli, VeriSign, Inc.
Matthew Tuttle, beTRUSTed
A. Jerald Varner, U.S. General Services Administration
Martin Wargon, Wave Systems Corporation
Richard Wilsher, The Zygma Partnership
David Weitzel, Mitretek Systems, Inc.
Michael Wolf, Authentidate
Gordon R. Woodrow, ClearTran, Inc.
Steve Worona, EDUCAUSE