Identity Proofing & Management Service

Credential Policy

Doc ref: **ID.me.S.00.010**
Doc id: **ID.me CrP v5.0**

Notice

1) References to Kantara SAC are made within this document for the purposes of showing a conformity mapping. They are placed right-justified after any clauses (single or multiple) to which the conformity cross-reference applies, always at the lowest indexed level to which they apply, in the following fashion:

SACv4.0: «criterion reference»; «criterion reference»; etc.

2) References to IS27001 [10] are made within this document for the purposes of showing a conformity mapping. They are placed right-justified after any clauses (single or multiple) to which the conformity cross-reference applies, always at the lowest indexed level to which they apply, in the following fashion:

IS27001: «clause reference»; «clause reference»; etc.

CONTENTS

1 INTRODUCTION

1.1 Overview

This document sets forth the Credential Policy (CrP) for ID.me's Identity Proofing service. It follows the general structure of RFC 3647 [1].

The ID.me service provides our nation's veterans, first responders, and members of other designated groups (eligible parties) with a simple and secure way to verify their identities remotely, for online transactions, while minimizing the risk of identity theft. ID.me protects a user's identity while simultaneously providing assurance to businesses and government agencies that the user's identity and group status are reliably verified by an authoritative source. These assurances allow for participants to confidently complete electronic transactions in a secure environment. Use of the ID.me service provides eligible parties access to certain benefits, discounts, and information from various organizations who wish to limit access based on requirements related to the underlying value and eligibility associated with the benefit, discount, or information.

Assurance Levels (ALs) relate to the degree of confidence in a claimed identity and associated characteristic attributes (Charats, with a hard 'Ch') and the associated technology, and processes governing the operational environment. Assurance Levels are defined in a number of key documents, principally OMB M-04-04 [2], ISO 29115/ITU-T X.1254 [3], NIST SP 800-63-2 [4], FICAM TFS [5] and the Kantara Initiative's SAC [6]. Use of ALs is determined by the service's Relying Parties, according to the level of confidence or trust (i.e., assurance) they deem necessary to mitigate risk in their transactions.

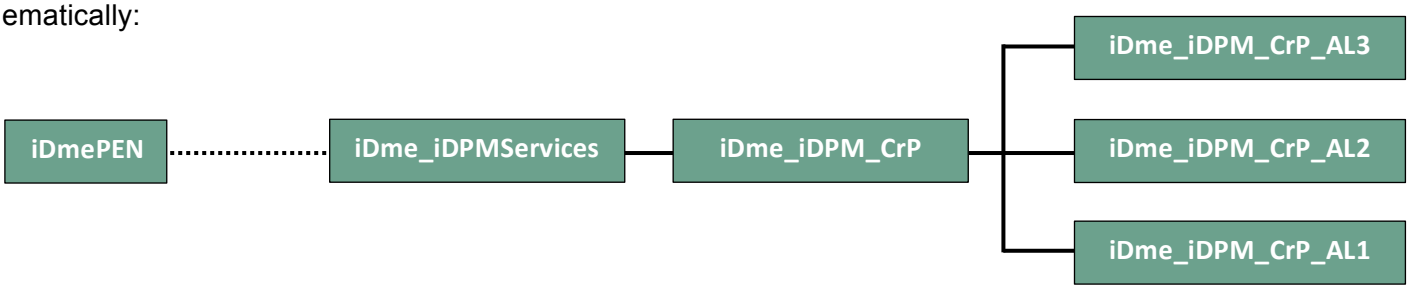
This service policy covers End User credentials issued at ALs 1, 2 and 3. It details how ID.me provides a remotely verified, online credential to eligible parties that can be trusted by relying parties consistent with the assurance level of the credential. How an enterprise becomes a Relying Party is not covered by this CrP.

1.2 Policy Identification

a) This document and the derived policies shall be formally identified by their applicable full title and Policy OID. The OID path for this policy document is described in the following table and derives from assignments given in the 'ID.me.C.00.005 PEN Register'. Assertions relating to credentials issued according to practices described in this CrP shall be identified by at least one of the following Policy OIDs:

Element	Path / OID	Policy Title
iDme_iDPM_CrP	::= { iDme_IdPMServices.1 } (1.3.6.1.4.1.43927.10.1.1)	ID.me Identity Proofing & Management Credential Policy *(this document)*
iDme_iDPM_CrP_AL1	::= { iDme_iDPM_CrP.1 } (1.3.6.1.4.1. 43927.10.1.1.1)	ID.me Identity Proofing and Management Services Credential Policy – Assurance Level 1
iDme_iDPM_CrP_AL2	::= { iDme_iDPM_CrP.2 } (1.3.6.1.4.1. 43927.10.1.1.2)	ID.me Identity Proofing and Management Services Credential Policy – Assurance Level 2
iDme_iDPM_CrP_AL3	::= { iDme_iDPM_CrP.3 } (1.3.6.1.4.1. 43927.10.1.1.3)	ID.me Identity Proofing and Management Services Credential Policy – Assurance Level 3

Schematically:



SAC v4.0: ALn_ID_POL#010

1.3 IdP Roles

This section provides a brief description of each IdP role. The specific obligations of each role are more fully discussed later in this document.

1.3.1 End User

An individual person to whom a credential is issued (subject to successful identity proofing and verification).

1.3.2 Relying Party

A Partner enterprise which uses ID.me's authentication services to gain assurance as to an End User's identity and their eligibility for such services as the RP may offer. Generally abbreviated to 'RP'.

1.3.3 Authoritative Source

A repository which is recognized as being an accurate and up-to-date source of information. [ISO/IEC 29115:2011]

1.4 Credential Usage

An ID.me identity credential is issued to an End User in order for them to be authenticated by an eligible Relying Party with whom they wish to perform some transaction or exchange. Typically, Relying Parties will direct End Users to ID.me to perform their initial Sign-up and will specify the Assurance Level (AL) at which it requires credential issuance and authentication services for its specific website(s) or service(s).

Relying Parties only use authentication assertions only at the specified AL or lower and should not rely on an assertion for any service, exchange or transaction offered or transacted at a higher AL than that specified in the ID.me assertion, nor should they rely upon the assertion beyond its stated life-time.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This document shall be administered by ID.me Inc., whose offices are located at:

8281 Greenboro Drive,
Suite 600
Tyson's Corner, VA.22102, USA.
Tel: +1 866 775 4363
ISGF_Chair@ID.me.

1.5.2 CrP Approvals

ID.me's ISGF will review and approve changes to this document, final authority being the ISGF Chairperson.

SAC v4.0: ALn_CO_ISM#010, '#020; ALn_CM_CPP#030

1.5.3 CrP Revision

ID.me shall post notice of revision to this CrP(S) such that interested parties receive due notification of changes.

SAC v4.0: ALn_CO_NUI#010; ALn_CO_NUI#020

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

a) ID.me shall publish details of its credential policy and practices as well as other terms of service, pursuant to the policy statements herein and such additional material as may be required to fully advise all interested parties as to the services characteristics and the terms of its provision with regard to legislative, Terms of Service and policy obligations. These publications shall be maintained such that they always reflect the service as being operated at any given time;

SAC v4.0: ALn_CO_NUI#010; ALn_CO_NUI#020 a – e, j); ALn_ID_POL#030

b) ID.me shall maintain an internal repository of only that information relating to individual credentials, their statuses and the Subject's characteristic attributes and eligibilities which is necessary to deliver the service and comply with legislative, Terms of Service, contractual and policy obligations;

SAC v4.0: ALn_CM_CSM#010, '030, '#040; ALn_ID_VRC#025

c) ID.me shall require the End Users to acknowledge and authorize publication of their personal information to each RP with whom they interact.

SAC v4.0: ALn_CM_CRD#020

3 IDP CREDENTIAL ENROLMENT AND ISSUANCE

3.1 Subject Naming

a) ID.me shall support exclusively on-line (remote) Identity Proofing and Management services for individual persons;

b) At all ALs, End Users shall be bound to their credentials by means of an email address, possession and control of which they shall demonstrate before being granted full access to services;

c) At AL1 single factor authentication shall be provided. The email address provided need not bear any relation to the End User's actual identity and no real identity shall be required or be verified;

d) At ALs 2 & 3 it shall be ensured that End Users provide a real name that passes identity verification checks, such checks to be appropriate to the applicable AL. AL2 shall provide single-factor authentication: AL3 shall provide two-factor authentication;

e) All bound email addresses shall be unique within the service.

SAC v4.0: Aln_ID_POL#020; ALn_CM_CRN#020

3.2 Initial Registration

3.2.1 Account Sign-up

a) End Users shall be directed to ID.me's website by an eligible Relying Party. The RP shall, at the time, specify the required AL. This shall be the primary means by which an End User signs-up;

SAC v4.0: ALn_ID_IDV#000

b) At AL1 only, End Users shall also be permitted to sign-up for a credential directly at www.ID.me;

SAC v4.0: ALn_ID_IDV#000

c) In either of the above cases the applicable Terms of Service and Privacy Policy shall be made accessible before the End User is required to provide any sign-up information.

SAC v4.0: ALn_ID_IDV#000; ALn_CO_NUI#010

3.2.2 Account Creation

a) Account creation shall be initiated by having the End Users provide an email address, and select a password. The email address shall be unique within the service as a whole (i.e. may not be used multiple times for different ALs). Passwords shall exhibit at least 24 bits of entropy;

SAC v4.0: ALn_CM_CTR#020; ALn_ID_POL#020; ALn_CM_CRN#020

b) End Users shall be required to accept the applicable Terms of Service and Privacy Policy before the sign-up process is concluded. Record of the End User's acceptance shall be retained;

SAC v4.0: ALn_CO_NUI#040 a), 'NUI#050

c) A confirmatory email shall be sent to the End User requiring them to confirm their email address before any identity proofing is performed.

SAC v4.0: ALn_CO_NUI#040 a), 'NUI#050

3.2.3 Identity Proofing & Verification

a) At AL1, no identity proofing shall be performed;

b) At AL2 & 3, identity proofing shall require the End User's provision of the following information:

i) Given and family names;

ii) Full postal address (including street number, street name, city, state and postal zip code);

iii) Date (year, month and day) of Birth (DOB);

iv) Social Security Number (SSN);

v) Cell phone number.

c) At AL3, identity proofing shall be performed based upon the End User's provision of the above plus the following additional information:
i) Financial account number.

d) Identity proofing shall be performed by comparing the End User-provided information against an Authoritative Source. A notification of pass or fail shall be provided to the RP or End User, depending on how account creation was initiated;

e) On completion all information not required for ongoing management of the credential shall be securely purged.

SAC v4.0: ALn_ID_RPV#010

3.2.4 Credential Activation

a) At AL1 & 2, a credential shall become active when identity proofing and verification have been successfully completed;

SAC v4.0: ALn_ID_RPV#020

b) At AL2 & 3, in addition to successfully completing identity proofing and verification, a second-factor verification using the notified cell phone shall be required before activating the credential.

SAC v4.0: ALn_ID_RPV#020

3.2.5 Credential 'Step-up'

End Users shall be able to 'step-up' the AL of their credential at any time by successfully completing the necessary additional steps to achieve their desired AL.

SAC v4.0: ALn_ID_RPV#020

3.2.6 Credential Re-issuance and Renewal

End Users shall be able to reset their passwords online after being authenticated using their existing password. In the case of a forgotten password they shall be able to effect a reset by receiving a link to a reset page and responding to a security question which they established during their registration. In each case, if the credential was issued at AL3, the End User shall additionally be required to submit an OTP sent to their mobile device.

If the reset fails then Users shall be directed to Member Support for verbal authentication, before the reset is enabled.

SAC v4.0: ALn_CO_NUI#020

3.2.7 Registration Records

Irrespective of the outcome of the identity proofing, records of the identity proofing and verification process, of renewals and re-issuances, references of source documents, identity of Authoritative Sources, verification outcomes, and a time-stamp, shall be kept in accordance with §6.3.

SAC v4.0: ALn_CO_NUI#070, ALn_CO_SER#010, ALn_ID_VRC#010, ALn_ID_VRC#030, ALn_CM_RNR#050, ALn_CM_RVP#050

3.3 Authentication Protocols

3.3.1 End User Authentication

a) Only credentials which are active shall be authenticated;

SAC v4.0: ALn_CM_ASS#020

b) At AL1 & 2, each instance of an End User presenting their credential will require their authentication based upon the verification of their password;

SAC v4.0: ALn_CM_ASS#030

c) At AL3, each instance of an End User presenting their credential shall require their authentication based upon the verification of their password and their submission of an OTP sent to their mobile device;

SAC v4.0: ALn_CM_ASS#030

d) At all ALs a maximum of 100 failed authentication attempts shall be permitted within a 30-day period.

SAC v4.0: ALn_CM_ASS#035

3.3.2 Content

a) Assertions shall have default inclusions and shall be able to convey further data on request of the RP, subject to the End User's authorization and compliance with applicable legislation;
   e) Default inclusions at AL1 shall be:

      i) The unique identifier for the intended RP;
      ii) AL at which the credential was issued;
      iii) Unique user identity;
      iv) Lifetime.

SAC v4.0: ALn_CM_VAS#030

   f) Default inclusions at AL2 & 3 shall be:

      i) The unique identifier for the intended RP;
      ii) AL at which the credential was issued;
      iii) Unique user identity;
      iv) Verified End User names;
      v) Lifetime.

SAC v4.0: ALn_CM_VAS#030; AL3_CM_VAS#040

3.3.3 Protection

a) Cryptographic protections shall be employed to ensure that Assertions shall be strongly-bound to individual RPs, signed and encrypted, and transmitted through secured, mutually-authenticated communications. Additionally, RPs shall be associated with pre-defined end-points;

SAC v4.0: ALn_CM_VAS#010, '050, '060, '070, '100

b) Cryptographic techniques employed shall be selected from those listed as approved under the National Voluntary Laboratory Accreditation Program.

SAC v4.0: ALn_CM_VAS#010

3.3.4 Assertion Lifetime

SAML assertions shall have a lifetime of 5 minutes and be valid only for the Relying Party's domain.

SAC v4.0: ALn_CM_ASS#040

3.3.5 Single Use

Each assertion shall apply only to a specific transaction and shall only be re-sent in connection with that transaction.

SAC v4.0: AL3_CM_VAS#090

3.3.6 Reliability

Should there be any system failure during authentication, no assertion shall be generated.

SAC v4.0:

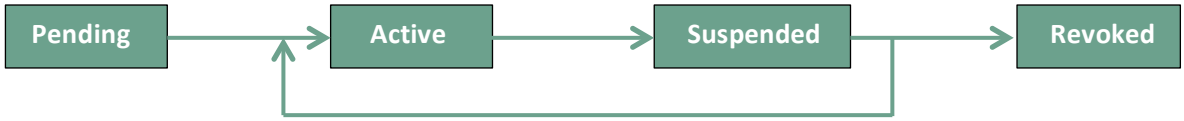
3.3.7 Re-Authentication

Re-authentication of a credential shall be permitted within 12 hours of an initial authentication so long as the session in which the original authentication took place remains active and the End User has been active within the last 30 minutes.

SAC v4.0: AL3_CM_VAS#110

4 CREDENTIAL LIFECYCLE

The status of a credential shall be maintained current in real-time, being recorded in one of the following states:



No publication of status shall be required since all credential management and authentication functions are handled by the ID.me service.

SAC v4.0:

4.1 Credential Validity Period

ID.me credentials shall have a validity period of 5 years, after which End Users must re-affirm their acceptance of the prevailing Terms of Service, Privacy Policies and any other required agreements. Credentials not re-affirmed within the 5 year period shall be suspended. Any re-affirmation of acceptance of terms and policies shall lead to the credential validity being re-set (and re-activated, if it has been suspended).

SAC v4.0: *AL2_CO_NUI#040, ALn_CM_RNR#050*

4.2 Authentication Process

a) End Users shall be authenticated on behalf of Relying Party websites/applications, either by signing-on at the ID.me website or through a Relying Party's site;

SAC v4.0:

b) At AL1 & 2, single-factor authentication shall be applied, requiring the End User to submit a username and a password which shall be against those associated with the account in the system database. On a successful match the authentication shall be complete;

SAC v4.0:

c) At AL3, two-factor authentication shall be applied, requiring the End User to first submit a username and a password which shall be against those associated with the account in the system database. On successful matching an SMS OTP message shall be sent to the registered mobile device associated with the account and the End User shall be given a url/page on which to enter the OTP. On a successful match with the transmitted OTP the authentication shall be complete.

SAC v4.0:

4.3 Credential Status Availability

A change in Credential status shall be available for immediate reference within the ID.me service.

SAC v4.0:

4.4 Lifecycle Events

The following subsections describe events that occur over the lifecycle of the Credential and the effect (if any) on the state/status of the Credential and if/how such status affects the operation of the Credential.

4.4.1 Credential Activation/Re-Activation

The IdP Credential shall be placed in an "*Activated*" state in accordance with section 3.2, initial registration. Activation is the process of binding the End User to the Account information (i.e., email address, postal address, cell phone #). Re-registration shall be required should the IdP Credential be placed in an inactive or revoked state over the course of its lifetime.

SAC v4.0:

4.4.2 Failed Authentication

Should authentication fail at AL1, 2 or 3, up to nine further attempts are be permitted before locking the credential. Unlocking the credential can happen either by a positive action by customer support personnel after a phone / email / multi-factor validation of the End User, unlocking the credential by proving ownership of the credential or expiry of a 72 hour time-out period, whichever the sooner.

SAC v4.0:

4.4.3 Suspension after inactivity

If a credential remains unused for a period of eighteen months or longer it shall be suspended and shall secondary validation before being re-activated.

SAC v4.0:

4.4.4 Modify Account Information

a) The End User shall be able to modify their Account information to reflect changes in their personal circumstances or to correct errors. Prior to being able to effect changes the End User shall be required to sign-in to their account, accounting for the applicable AL. Users shall only be able to change the following information, according to the applicable AL, and shall require new and full identity proofing for fields so-marked:

Field / value	At all ALs
Email address	Validate new email per §3.1 & §3.2.2
Password	Validate new password per §3.2.2
Mobile device number	Validate new mobile device per §3.2.2

SAC v4.0: ALn_CM_IDP #010; ALn_CO_CSM#020

b) Once used an email address shall not be accepted for any new sign-ups or account modification.

SAC v4.0:

4.4.5 Password Reset

In the event that their password is forgotten or compromised End Users shall be able to reset their password via a secure mechanism which shall employ a protocol of strength equivalent to that at which the credential was issued.

SAC v4.0:

4.4.6 Revocation

Revocation shall be supported at all ALs. Following an initial revocation request a credential may be suspended while the revocation request is authenticated, but once determined authentic the status shall become 'revoked' and thereafter the credential shall not be used. Should a revocation request not be authenticated or be withdrawn before being fully applied the credential shall be re-activated.

4.4.6.1 Circumstances for Revocation

Revocation shall be permitted only under the following circumstances.

4.4.6.1.1 Revocation Request from End Users

a) No End User revocation shall be provided at AL1;
At AL2 the End User may request a revocation, which shall be confirmed by sending an email requiring confirmation of the request to the email address of record;
At AL3 End User revocation shall follow the same process as for AL2 and in addition a second-factor confirmation shall be required.

SAC v4.0:

4.4.6.1.2 Revocation Request from Non-Users

At all ALs there shall be a means by which a recipient of a confirmatory message can respond by stating that they have not requested that the account be created, in which case the associated credential shall be revoked.

SAC v4.0:

4.4.6.1.3 Revocation Request from Authorized Bodies

At all ALs there shall be a means by which an authorized body, e.g. law enforcement, a RP (for cause) or other body having a recognized authority, can request revocation. Each such requestor shall be authenticated before any final action is taken. According to the authority and manner of request ID.me may suspend the credential pending further authentication and justification for the revocation, and shall either revoke or re-activate, according to its findings.

SAC v4.0:

4.4.6.1.4 Revocation by ID.me

ID.me shall revoke any credential, to accommodate instances of false representation, failure to comply with Terms of Service, or for any other reason, at its sole discretion and at any AL.

SAC v4.0:

4.4.6.2 Revocation Response Time

Once a request has been authenticated revocation shall be effected immediately, and that status used in any subsequent authentication requests.

SAC v4.0:

4.4.6.3 Revocation Notification

Once an End User's credential has been revoked all interested parties should be notified with 24 hours.

SAC v4.0:

5 FACILITY AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Physical Access Controls

a) Production facilities shall be housed in secure data centers which provide for geographical alternate sites and are protected by multi-layer physical security, minimizing the opportunities for unauthorized access, disclosure, loss or corruption of sensitive and system information, and of IT resources on which the service is dependent. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the service's equipment and records and protection from adverse environmental conditions;

SAC v4.0:

b) Where third-party hosting is used, the ability of the entity to provide facilities which meet the above policy requirements shall be determined either by physical inspection by responsible ID.me personnel and/or through review of independent analyses and audits of the facilities in question;

SAC v4.0:

c) Development facilities (which shall not hold real client data) shall also be protected by multi-layer physical security, minimizing the opportunities for unauthorized access, disclosure, loss or corruption of sensitive and system information, and of IT resources on which development is dependent. Back-up / disaster-recovery sites shall have the same level of protection. A reduced level of security shall be permissible to the extent that no real client data is stored but must still be sufficient to ensure that the sensitivity of proprietary information and the ability to support the production system is not compromised;

SAC v4.0:

d) Information and media transported between sites, and sensitive information and IT resources in the custody of staff, shall be protected from unauthorized access, disclosure, loss or corruption, having special regard for their use and potential storage in public areas (e.g. hotels, restaurants, car parks, ...);

SAC v4.0:

e) Back-up / disaster-recovery sites shall have the same level of protection.

SAC v4.0:

5.1.2 Secure Disposal

When it no longer serves a purpose or should not remain on any storage mechanism being serviced or re-purposed, sensitive information shall be disposed-of using methods which meet or exceed the requirements of DOD 5220.22_M [7] or NIST SP 800_88 [8], ensuring that techniques applied match the storage media

technology in use. Where third-party services are used, those entities shall guarantee and take responsibility for observing or exceeding those same requirements.

SAC v4.0:

5.2 Procedural and Personnel Controls

5.2.1 Security Roles and Responsibilities

5.2.1.1 Trusted Roles Requirement

a) The roles and responsibilities for personnel for each service-related and security-relevant task shall be documented. Such roles define positions which underpin the assurances given through the secure development, operations and delivery of ID.me's service and shall include as a minimum:

i) Executive and management functions;
ii) Engineering and development functions;
iii) System information security functions;
iv) Service administrative functions;
v) Member Support functions;
vi) Audit (both internal and external) functions.

SAC v4.0: AL3_CO_OPN#020

g) Personnel fulfilling such roles, both employees and contractors, shall be subject to appropriate HR procedures to ensure their character, qualifications and experience meet the documented requirements, including any specific clearances required by the role. Assignment of personnel to trusted roles shall be authorized by the ISGF Chairperson or his/her delegate.

SAC v4.0: AL3_CO_OPN#030; AL3_CO_OPN#040

5.2.1.2 Personnel Resource Requirements

a) The number of personnel required to effectively operate the service across development, operations and support functions shall be determined and suitable resources recruited and applied;

SAC v4.0: AL3_CO_OPN#050

h) For highly-sensitive roles dual-personnel assignments and segregation of duties shall be designed and applied. No single person shall have more than one means of identifying themselves to the system.

SAC v4.0: AL3_CO_OPN#050

5.2.2 Personnel Qualifications

a) HR policies shall provide for and apply adequate checking of personnel, concerning backgrounds, criminal records, qualifications and experience. Adequate training shall be provided to ensure that staff are competent to apply the tools used to develop, operate and support the service, including progressive training to ensure that state-of-the-art technologies and best practices are adopted and applied at all times;
i) Such requirements shall apply to third-party personnel as well as ID.me's direct employees.

SAC v4.0: AL3_CO_OPN#030

5.3 Event Logging

a) A log of all relevant security events shall be maintained, employing both automated and manual logging;

SAC v4.0:

j) Event logs shall be retained and protected against unauthorized access, loss or corruption and be available to support audit functions and any investigative processes, both internal and those conducted under lawful oversight. Event logs shall be retained for a minimum of five years, and otherwise as required by applicable legislation, contract or policy.

SAC v4.0:

5.3.1 Types of Events Recorded

Logs shall capture at least the following events and associated information:

a) any applicable event serial / sequence number (intended to provide a unique reference for the event, either as an instance, or to track an asset, e.g.);
b) the date and time of the event;
c) the nature of the event;
d) the device, application, network or operating system, or person, identifying the event; and
e) other pertinent information as further set out below.

5.3.1.1 End User Sign-up

The following information about End User sign-up shall be recorded, both at initial sign-up and for any subsequent changes, whether initiated by the service or the End User:

a) the unique user id;
b) references of any specific identifying information sources submitted, according to AL;
c) references to how the identity information was verified;
d) responses received to identity verification;
e) associated device(s) (at AL3);
f) acceptance of applicable terms and policies.

SAC v4.0:

5.3.1.2 Credential Revocation

The following revocation information shall be recorded, whether fully prosecuted or not:

a) the identity of the requesting source;
b) the authority of the requesting source and measures taken to authenticate the source;
c) the End User unique identity associated with the credential for which revocation is sought;
d) the reason for revocation;
e) the revocation decision (i.e. upheld – credential revoked; denied – credential reactivated).

SAC v4.0:

5.3.1.3 Credential Status Changes

Any credential status changes between Sign-up and Revocation shall be recorded.

SAC v4.0:

5.3.2 Security Incidents

a) Controls shall be applied to provide prevention and detection of security incidents which could imperil the secure operation of the service, and alerts shall be provided based on defined thresholds of activity being exceeded, according to the nature of the event[1]. Any significant events shall be logged and reviewed for signs of suspicious or unusual activity. Automated logs shall be continuously monitored to provide real time alerts;

SAC v4.0:

b) Records shall be kept of reviews of event logs and shall ensure that the integrity of logs remains preserved;

SAC v4.0:

c) Actions taken based on alerts and audit log reviews, and their outcomes, shall be documented and reviewed for completeness and effectiveness.

SAC v4.0:

1 Detection of an attempt by a human intruder to break in would probably have a 'frequency threshold' of zero, i.e.it would be worthy of immediate attention, whereas that for system penetration attempts from the same IP address (given their constancy) may have a threshold of hundreds or thousands.

5.4 Risk Assessments

Risk Assessments shall be conducted at least every six months to ensure that any new threats are identified and that existing controls are providing a level of risk mitigation which is accepted by management, in accordance with the ISM Policy. Such risk assessments shall include a review of actual controls against those found in IS27001 Annex A and shall be based on the service being classified as 'High Assurance' at AL3, in accordance with NIST FIPS 199 [9].

SAC v4.0:

5.5 Records Protection and Retention

5.5.1 Record Protection

a) Logical and physical access controls as required elsewhere in this CrP shall protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any credential data repositories or credential management processes, whether records are stored on-site or by third parties;

SAC v4.0: ALn_CO_ESM#050

k) Where necessary, measures shall be taken to ensure the long-term accessibility of storage media over the required period.

SAC v4.0: ALn_CO_ESM#050

5.5.2 Record Retention Period

Unless otherwise specified in this CrP, the default retention period for records shall be five years from their creation or last use, whichever the later, or a longer period if so dictated by other (over-riding) policy, contract or legislation.

SAC v4.0: AL3_ID_VRC#030

5.6 Business Continuity

a) The service shall be included within ID.me's overall Business Continuity Planning such that in the event of a significant disruption to operations, critical business activities can be resumed (if necessary) and continued;

l) The production system shall plan for and be deployed such that there is an alternate site capable of picking-up the operational load until the disrupting event can be resolved. This shall include redundant capacities and mirrored or backed-up copies of critical information, such as End User and RP account data, logs, test data and procedures, system build and configuration records, ...

SAC v4.0:

5.7 Availability of Services

The service shall employ redundancies and back-up measures which ensure its 99.9% availability, excluding scheduled maintenance time and events totally outside of ID.me's control.

SAC v4.0:

5.8 Termination of Services

If it becomes necessary to terminate the service ID.me shall take reasonable measures to give notice to End Users, RPs, out-sourced providers and other interested parties. It shall then, after expiration of the notice period, effect the revocation of all End User credentials, any PKI certificates which it uses to secure its operations and services, and to ensure the long-term preservation of all records, for their required retention period. This plan shall be outlined in the Terms of Service.

SAC v4.0: AL3_CO_ESM#055

6 TECHNICAL SECURITY CONTROLS

6.1 Network Security

a) Communications between all service components outside of a common DMZ shall be encrypted and mutually-authenticated using protocols which meet or exceed recognized best practices for the threat scenario used by the risk assessment process;

SAC v4.0:

b) End User Sign-up shall be protected by end-end encryption such that all data transfers are secured;

SAC v4.0:

c) 24/7 automated monitoring and test script execution shall be maintained with automated notification to operational personnel. In addition, daily system management reports shall be produced, reviewed and protectively stored. These reports shall, as a minimum, address security events, transactions processed, system usage/capacity, availability.

SAC v4.0:

6.2 Key Management

a) Knowledge of private key activation codes shall be limited to a minimum group of personnel, on a need-to-know basis. There shall be provision for non-availability of code-holders so as to ensure that critical functions can be actioned when required without imperiling the service;

SAC v4.0:

b) On re-assignment or termination of any of those trusted roles there shall be a procedure to effect a code- or key-change;

SAC v4.0:

c) In the event that a key is compromised in any way it shall be replaced and the compromised key revoked.

SAC v4.0:

6.3 Information Security Management and Lifecycle Controls

This CrP is governed by the ID.me ISM Policy and as such shall fall within its provisions for information security management practices. The principles of that policy and of IS27001 shall apply to all requirements of and practices derived from this CrP.

SAC v4.0: Aln_CO_ISM#020, Aln_CO_ISM#120

7 PROFILES

7.1 SAML

At AL2 & 3, authentication assertions shall comply with the requirements of the FICAM TFS profile published at http://www.idmanagement.gov/documents/SAML20_Web_SSO_Profile.pdf.

8 COMPLIANCE AUDIT

8.1 Internal Service Audit

In view of the company's size, ID.me shall apply rigorous Quality Assurance measures to the development and improvement of its services, through all stages of the life-cycle, in lieu of formal internal audits.

8.2 Independent Audit

a) In accordance with ISM Policy §25.1, ID.me shall undergo an initial and subsequent renewal assessments to attain and maintain Kantara Approval, which shall be performed by a Kantara-Accredited assessor, in accordance with the prevailing Kantara requirements for Approval renewal at the applicable ALs;

SACv4.0: AL3_CO_ISM#080

b) Records of audits and supporting evidence shall be archived for a minimum of four years from the date of audit (Kantara Approval period plus 12 months). Such records shall be protected against unauthorized access, loss, alteration, public disclosure, or unapproved destruction in accordance with section 6.4.

9 LEGAL

Stipulations relating to fees, insurances, warranties, disclaimers, limitations of liability, indemnities, terms of supply, termination, confidentiality, privacy, notices, amendments, dispute resolution, governing law and other representation and legal matters shall be presented in the service's Terms of Service, Privacy Policy and other documents, all of which shall be brought explicitly to the End User's attention (see also §3.2.2).

SAC v4.0:

10 REFERENCES

Ref.#	Document / Source
[1]	Request for Comments (RFC) 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", © The Internet Society (2003). http://www.ietf.org/rfc/rfc3647.txt
[2]	OMB M_04_04, "E_Authentication Guidance for Federal Agencies", Office of Management and Budget, 2003_12_16. http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04_04.pdf
[3]	ISO/IEC 29115:2013 // ITU_T Rec. X.1254 (12/2011) "Information technology __ Security techniques __ Entity authentication assurance framework", joint ISO / ITU_T publication2. https://www.itu.int/rec/T_REC_X.1254_201209_I/en
[4]	Special Publication 800_63_2, "Electronic Authentication Guideline", National Institute of Standards and Technology, 2013_08. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800_63_2.pdf
[5]	"Authority To Offer Services (ATOS) For FICAM TFS_Approved Identity Services", FICAM TFS Program, Version 1.0.1, 2014_02_17.
[6]	Kantara IAF_1400 v4.0, "Service Assessment Criteria", © 2014 Kantara Initiative. http://kantarainitiative.org/confluence/display/certification/Apply+_+CSP+Approval
[7]	DOD 5220.22_M, "Operating Manual", National Industrial Security Program, 2006_02 modified 2013_03_18. (Chapter 5, Section 7 applies, as referenced). http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf
[8]	Special Publication 800_88, "Guidelines for Media Sanitization", National Institute of Standards and Technology, 2006_09. http://csrc.nist.gov/publications/nistpubs/800_88/NISTSP800_88_with_errata.pdf
[9]	Federal Information Processing Standard 199, "Standards for Security Categorization of Federal Information and Information Systems", National Institute of Standards and Technology, 2004_02. http://csrc.nist.gov/publications/fips/fips199/FIPS_PUB_199_final.pdf
[10]	ANSI/ISO/IEC 27001:2013, "Information technology -- Security techniques -- Information security management systems – Requirements", American National Standards Institute, 2013-10. http://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fIEC+27001%3a2013

2 Note that the foreword of the ITU-T version explains that that version has four differences from the ISO version.

11 REVISION HISTORY

Version	Date	Description	Comments
1.0	2014-07-24	Formally released (stand-alone – see CrPS as separate document)	Released under DoA
2.0	2014-08-11	Document reference added	Released under DoA
3.0	2014-11-05	Approved release	RGF
4.0	2015-02-11	Adoption of revisions resolved through PoT preparation	Approved by RGW with delegated authority of MST.
5.0	2015-09-02	Correction to proofing policy, to state practice already correctly applied (§3.2.3 b) v), §3.2.4 b)).	Approved by COO, on ISGF's recommendation.

12 APPROVAL

COO, ID.me
James Pottenger COO / ISGF Chairman 2015-09-02

SACv4.0: ALn_CO_ISM#020
IS27001: A.5.1.1