Approval Profile

for

ID2020 Certification Mark

Version 1.0

Prepared by Adam Cooper

ID2020

28/04/2019

Table of Contents

Table of Contents ii
Revision History ii
1. Introduction 1
1.1 Purpose 1
1.2 Document Conventions 1
1.3 Intended Audience 1
1.4 References 1
2. Applicability 2
2.1 Overview 2
2.2 Achieving Compliance 2
3. Criteria 2
3.1 Responsible Organisation and Solution Description 2
3.2 Technical Requirements 3
3.3 Acceptable management and security policies and procedures 7
3.4 Assurance of the technical infrastructure 8
3.5 The suitability of personnel used (skills and competence) 9
4. Certification Mark 10
5. Publication of Evidence 10
6. Reassessment 10
7. Reassertion of Compliance 10
Appendix A: Glossary 11

Revision History

Name	Date	Reason For Changes	Version
Adam Cooper	05/03/19	Draft for review	0.1
Adam Cooper	28/04/19	Updated following peer review	0.2
Adam Cooper	28/04/19	Promoted to version 1.0 with clarifications for applicability assessment.	1.0

1. Introduction

1.1 Purpose

This Approval Profile defines the requirements for Providers of Digital Identity Solutions wishing to be awarded the ID2020 Certification Mark.

The ID2020 Certification Mark is an initiative by the ID2020 Alliance to create a Trustmark for solutions related to the processing of digital identities that meets the ID2020 Technical Advisory Committee technical requirements[1]. The Certification Mark draws upon the efforts of several organizations, including and most notably ThingsCon and their Trustable Technology Mark. We were tremendously inspired by their effort to develop a "badge of honour" for companies and organizations designing technology with user privacy and rights top-of-mind.

The development of the ID2020 Certification Mark was supported by the ID2020 Technical Advisory Committee, a group that comprises many of the world's foremost experts on digital identity and its underlying technologies.

The meaning of the ID2020 Certification Mark is as follows:

1. the Solution has been thoroughly evaluated against rigorous criteria by our experts;
2. the Solution Provider has agreed to keep to these criteria;
3. the Solution Provider subscribes to the ID2020 core principles of portability, persistence, privacy, and user control; and
4. the Solution Provider has agreed to act promptly and fairly to remedy faults.

1.2 Document Conventions

For ease of reference from other documents, each clause is given a tag and a title, adopting the general form of a Common Criteria Protection Profile, as follows:

GENERIC-1	Text describing the clause

1.3 Intended Audience

Any organisation providing or procuring identity services or identity solutions that align with the ID2020 principles and technical requirements.

1.4 References

[1] ID2020 Technical Requirements https://id2020.org/uploads/files/Technical-Requirements.pdf
[2] Certification Form https://id2020.org/technical-certification-mark

---

[1] ID2020 Technical Requirements - https://id2020.org/uploads/files/Technical-Requirements.pdf

2. Applicability

2.1 Overview

The applicability of this Approval Profile shall be described in evidence provided as a result of the Solution Provider completing an ID2020 Certification Mark Application Form and in any additional information requested by the ID2020 Secretariat or its Advisory Committees.

2.2 Achieving Compliance

Compliance with this Approval Profile will be achieved by satisfying the criteria identified in the following subsections.

Regardless of the Solution Type (see SOLUTION-1) the Provider should address all criteria described in the profile. Where criteria are not applicable the Provider should include a reason for non-compliance.

3. Criteria

3.1 Responsible Organisation and Solution Description

Information regarding the organisation responsible for the Solution being submitted for approval and basic information regarding the nature of the Solution.

ORGANISATION-1 Organisation name

Name of the company/organisation responsible for the digital identity Solution to be certified

ORGANISATION-2 Country of incorporation

An assertion of the country within which the organisation was incorporated or established.

ORGANISATION-3 Evidence of establishment

Evidence of the establishment of the organisation as a legal entity as required by law of the territory in which it was established. If there is a parent organisation evidence of the relationship between this organisation and the parent organisation should be provided.

ORGANISATION-4 Contact details

The applicant should provide postal address, email address, and website URL where available to ensure effective communication throughout the assessment for and term of certification.

ORGANISATION-5 Legal Authority

Evidence that the applicant is able to act on behalf of and represent the Solution Provider i.e. the organisation.

SOLUTION-1 Solution Type

The Solution may be a Relying Party, Identity Provider, Attribute Provider, Intermediary, Credential Service Provider, or part thereof. This should be clearly articulated by the applicant.

SOLUTION-2 Solution Core Operations

An indication of the usual operational use of the Solution should be provided i.e. Registration, Credentialing, Authentication, Authorisation or Transaction Intermediation.

SOLUTION-3 Solution Description

A description of the solution being assessed as part of the application. This should include a clear definition of scope, capability, and intended use of the Solution. A description of any expected relying party or end user (person) community.

3.2 Technical Requirements

Solutions will be assessed against the ID2020 Technical Advisory Committee Technical Requirements. The latest version of these requirements can be obtained from the ID2020 website.

Evidence must be provided in support of each technical requirement to ensure that the assessor is able to understand how the Solution meets criteria.

3.2.1 Applicability

With reference to the ID2020 Technical Requirements (see 1.4 above) and the ID2020 Alliance Manifesto[2], the Solution Provider must provide a detailed account of how applicability requirements will be met for assessment by the ID2020 secretariat.

Many of the criteria for Applicability are difficult to measure and not entirely technical in nature therefore the Solution Provider must provide detailed evidence to support their submission. Responses to these criteria will be considered by the secretariat as a prerequisite to further assessment under this profile.

APPLICABILITY-1 Offline and offline capability

Must be useful in both physical, offline and online scenarios.

APPLICABILITY-2 Resilient and suitable for long term use

Must be resilient / usable in “rugged” environments.

APPLICABILITY-3 Cost effective

Must be cost effective across all aspects of the identity lifecycle.

APPLICABILITY-4 Ease of use

Must be easy for end-users to use throughout the identity lifecycle and require minimal user education. A human centric approach should be demonstrated.

[2] ID2020 Manifesto - https://id2020.org/uploads/files/Alliance-Manifesto.pdf

APPLICABILITY-5 Ease of implementation for relying party

Must be easy to implement by the Relying Party and have a clear explanation of cost as well as implications for the use of digital identity.

APPLICABILITY-6 Ease of use for implementing agents

Must be easy for implementing agents to use and to explain throughout the identity lifecycle.

3.2.2 Identification and Verification

IDV-1 Prompt, cost effective delivery of digital identity

Should be able to create a unique digital identity quickly and at low cost.

IDV-2 Multiple forms of identification and proofing

Must support multiple forms of identification and proofing.

IDV-3 Manual override

Must support manual override in case identity cannot be proven.

IDV-4 Offline registration

Registration must be available offline as well as online.

IDV-5 Pseudonymous identity

Should support the ability for the subject to create and use pseudonymous identity

IDV-6 Minimum client profile

A minimum client profile must be defined.

IDV-7 Failure mode

A failure mode should be included where the subject is not able to follow the normal procedure for identification.

IDV-8 Bias in Biometrics

The solution must Address Bias in Biometrics.

IDV-9 Duplicate Prevention

The solution must support the prevention of duplicate identities.

3.2.3 Authentication

AUTHENTICATION-1 Multiple forms of pluggable identity

The solution must support multiple forms of pluggable authentication, including biometrics and cryptographic secrets

AUTHENTICATION-2 Support for multiple tokens

The solution should support multiple “tokens” and smart phones / PCs

AUTHENTICATION-3 Alternative methods of authentication

The solution must support alternative methods of authentication in support of failure modes

AUTHENTICATION-4 Offline authentication

The solution should support offline authentication.

3.2.4 Privacy and Control

PRIVACY-1 Granular control

The solution must allow the user to have granular control over the sharing of personal data

PRIVACY-2 Visibility and audit-ability

The solution must allow users to have visibility and audit-ability of consent and accesses (i.e., sharing with 3rd parties), and revocation of consent

PRIVACY-3 Custodianship / guardianship

The solution must allow custodianship / guardianship to be exercised for applicable persons.

PRIVACY-4 Controls against adversary

The solution must have controls against the act by an adversary to access, delete, or modify the identity.

PRIVACY-5 Transparency

Processing, retention, and sharing of identity data must be transparent to the subject except where legal provisions prevents it.

PRIVACY-6 Protection throughout the identity lifecycle

Privacy of the Subject must be protected throughout the identity lifecycle.

PRIVACY-7 Avoid immutable PII and observe rights

PII should not be immutable and the rights of the user observed.

PRIVACY-8 Data accuracy

Data accuracy should be a priority and users should be able to view and amend errors or make required updates.

PRIVACY-9 Computations rather than data sharing

The sharing of data should be avoided where aggregate computations are sufficient.

PRIVACY-10 Change of identity

The solution must allow an authorized user to update identity information

3.2.5 Attestations and Trust

TRUST-1 Attestation management

Must be able to store, and manage many attestations from governments and organizations

TRUST-2 Attestation proof

Must be able to prove that attestations are genuine, untampered, pertains to the recipient and current status is active / not revoked

TRUST-3 Identity proofing

Must be able to attest how the identity proofing was performed.

TRUST-4 Trust agreements

Must not require point to point trust agreements across parties

TRUST-5 Trust frameworks

Participation in Trust Frameworks must be possible.

3.2.6 Interoperability

INTEROP-1 Open source

Where possible / practical should be implemented using open source software.

INTEROP-2 Open APIs

Must support open APIs for access to data and integration with other identity system components / vendors.

INTEROP-3 Standards

Each solution element used in implementing the Identity Lifecycle should be standards-based in order to maximize interoperability.

INTEROP-4 Data export

Must be able to export the data in a machine-readable form.

3.2.7 Recovery and Redress

RECOVERY-1 Secure recovery

Must support secure recovery if one or more identity attributes is / are compromised / lost

RECOVERY-2 Redress

Must support redress if identity is compromised or is inaccurate

RECOVERY-3 Key custodians

Must provide at least one key custodian in a recovery scheme

3.3 Acceptable management and security policies and procedures

Applicants should demonstrate acceptable policies and procedures for the management of solution development and security throughout the organisation.

Examples of evidence that could be produced by the applicant are as follows:

1. A documented statement of applicability describing the control measures to be implemented and reasons for their selection to meet the base criteria and any additional specific criteria;
2. Presentation of a documented ISMS and any supporting opinion of a qualified external assessor;
3. Evidence may be offered against widely recognised standards such as ISO/IEC 27001 and ISO/IEC 27002.

MANAGE-AND-SECURE-1 Risk assessment

The Solution Provider must carry out a risk assessment to evaluate risks and determine the security requirements and operational controls necessary to manage and reduce risk to a level commensurate with the Solution being assessed. The risks identified and the countermeasures implemented to mitigate and manage those risks shall be documented.

MANAGE-AND-SECURE-2 Adequacy of administrative and management procedures

The Solution Provider shall ensure that administrative and management procedures (e.g. an Information Security Management System or ISMS) are applied, are adequate, and are based upon recognised standards.

INFOSEC-1 Defined information security policy

the Solution Provider management shall provide direction on information security by defining an information security policy and ensuring publication and communication of the policy to all employees.

INFOSEC-2 Maintenance of infrastructure

Any information security infrastructure necessary to manage the risks identified by the Provider shall be maintained at all times. Any changes that will affect the level of security provided shall be approved by the Provider management.

INFOSEC-3 Security controls and operating procedures

The security controls and operating procedures for operational facilities, systems and information assets comprising the Solution shall be adequately documented, implemented and maintained. Documentation shall identify all relevant targets and potential threats related to the Solution and the safeguards required to avoid or mitigate those threats.

MANAGE-AND-SECURE-3 Information Security best practice

The process of risk assessment of the Solution and the development of the ISMS shall be fit for purpose. It is therefore recommended that the process used aligns with current best practice as accepted by the information security industry.

INFOSEC-4 Management of cryptographic hardware

Where cryptographic hardware is utilised as part of the Solution clear procedures for its management and deployment (including any delivery to users or administrators of the Solution), should be in place. The use of non-trusted channels for the exchange of information with users and/or agents should be avoided (e.g. post, telephone).

INFOSEC-5 Contingency plans

Contingency plans shall be developed that describe how, in the event of an incident or disaster (e.g. loss of confidential data), operations may be restored and users alerted accordingly.

INFOSEC-6 Confidentiality and integrity of records

The Solution must ensure the confidentiality and integrity of current and archived records concerning Service provision and/or user data.

INFOSEC-7 Event logging

Solution shall be logged and these logs retained securely in line with regulatory requirements and in respect of user privacy. These logs must be timestamped and detailed enough to facilitate investigation should an incident occur.

3.4 Assurance of the technical infrastructure

INFRASTRUCTURE-1 Security controls

The Solution Provider shall ensure that security controls are built into any technical infrastructure of the Solution. These controls, and any physical or administrative security measures, should ensure any level(s) of assurance described in an accompanying ISMS.

In addition, the following should be considered:

- Security policy;
- Security organisation;

- Asset classification and control;
- Personnel security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Systems development and maintenance;
- Business continuity management;
- Compliance with legal and security policy requirements.

3.5 The suitability of personnel used (skills and competence)

Applicants must provide evidence of the definition, modification and application of the required personnel procedures and processes, particularly for those staff in sensitive roles (with regard to the provision of the solution).

PERSONNEL-1 Risk assessment includes personnel trustworthiness

The security requirements and operational controls associated with the trustworthiness of personnel shall be addressed within the risk assessment.

The Solution Provider must ensure that personnel and hiring practices enhance and support the trustworthiness of service operations. In particular:

PERSONNEL-2 Appropriate skills

The Solution Provider must employ personnel who possess the expert knowledge, experience and qualifications necessary to develop, support and maintain the Solution.

PERSONNEL-3 Defined security personnel roles

The job descriptions of security personnel should reflect the roles and responsibilities required by the security policy. Roles upon which the ongoing secure operation of a service depends must be clearly defined.

PERSONNEL-4 Separation of duties and privileges

The Provider must ensure that job descriptions for all personnel (including temporary staff) maintain a separation of duties and least privilege. Duties and access levels should be dependent on background screening, employee training, skills, experience and awareness.

PERSONNEL-5 Practice in-line with ISMS

Personnel must exercise administrative and management procedures and processes that are in line with the Provider's information security management procedures.

PERSONNEL-6 Conflict of interest

Personnel in trusted roles must be free from conflicting interests that might prejudice the impartiality of any service operations.

4. Certification Mark

The certification mark, once awarded, will be accompanied by a URL pointing to the Solution's certification listing on the ID2020 website. This will help to ensure that the public record of certification is easily available to individuals accessing Solution Provider resources.

Certification will be awarded for no longer than 3 years from the date of issue. Solution Providers may resubmit their Solution(s) for re-certification at the 3-year anniversary should they so wish.

Rules for the use of the certification mark by the successful Solution Provider will defined in a separate licence document available publicly on the ID2020 website.

ID2020 reserves the right to revoke certification for any Solution and/or Solution Provider that deviates from these rules.

5. Publication of Evidence

The list of Solutions that have achieved certification against this profile will be published in a trusted list hosted as part of the ID2020 website. Alongside each notice of certification will be a record of the evidence provided during assessment and the result of the approval process.

All certification notices will be dated for issue and renewal purposes.

A revocation list will also be published for Solutions that have lapsed certification or have broken the terms of certification as outlined in this profile or in regards to the Certification Mark Licence.

A facility will be provided for the reporting of a suspected or actual breach of the terms of certification as part of the ID2020 website.

6. Reassessment

A Reassessment is an Assessment performed for any of the following reasons:

- The previously assessed Solution has materially changed;
- There has been a change in the volume of business to the extent that the Solution Provider Service capacity or its financial guarantees could be affected;
- The organisation offering the Solution has materially changed, or its outsourcing arrangements have changed
- An Approval Profile under which the Solution was previously assessed has been updated, and the existing approval has come up for renewal, or the Solution Provider wishes independently to obtain approval under the new Profile.

7. Reassertion of Compliance

The Provider must provide a formal reassertion of compliance to this profile and the standards it cites on an annual basis starting on the first anniversary of a certification mark being awarded.

Reassertions of compliance should be received within 1 of the certification anniversary date.

Provider's not providing an annual reassertion of compliance will result in revocation of the certification mark and a notice to that effect being published on the trusted list.

Appendix A: Glossary

The following common terms are used in this approval profile.

Solution	The technical component, application or service being submitted for approval against the profile.
Solution Provider	The organisation responsible for creating or providing the Solution being assessed.
Provider	See Solution Developer.
Relying Party	An entity reliant on assertions of identity from a 3rd party.
Identity Provider	An entity able to provide proof of identity for an individual or other entity.
Attribute Provider	An entity able to provide trusted data related to an identity / entity.
ISMS	Information Security Management System as described in ISO/IEC 27001.