ID2020 Technical Requirements

V1.01

2019-04-28

Contributors:

Adam Cooper, ID2020
Brian Behlendorf, Linux Foundation
Daniel Bachenheimer, Accenture
Ankur Patel, Microsoft
Thomas Hardjono, MIT
Don Thibeau, Open Identity Foundation
Dakota Gruener, ID2020

Key Requirements

	Requirement	**Commentary**
1	APPLICABILITY	
1.1	Must be useful in both physical, offline and online scenarios.	Must take into account of, but not limited to the following: 1. Power may not be available to support identity transaction(s) 2. Wired or wireless data or cellular services may not be available to complete identity transaction(s) 3. Service requestor may not have a portable device 4. Service provider may have limited IT infrastructure
1.2	Must be resilient / usable in “rugged” environments.	Field equipment must be able to sustain long-term use in rugged environments for periods of time that exceed any pilot phase for example multiple years beyond implementation.
1.3	Must be cost effective across all aspects of the identity lifecycle.	Where the identity lifecycle is defined as: 1. Identity Proofing 2. Issuance

		3. Authentication 4. Authorization 5. ID management (including Recovery)
1.4	Must be easy for **end-users** to use throughout the identity lifecycle and require minimal user education	A human-centric design should be adopted.
1.5	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.	The Relying Party should be able to easily implement due to open standards, open APIs, and commonly available skills (for example OIDC and OAuth). The cost of implementation should be clearly defined for a Relying Party as well as the level of trust that can be placed in assertions of identity based on either legal or trust frameworks (for example).
1.6	Must be easy for **implementing agents** to use and to explain throughout the identity lifecycle	A human-centric design should be adopted.
2	IDENTIFICATION AND VERIFICATION	
2.1	Should be able to create a unique digital identity quickly and at low cost.	The identification process is inherently costly as it involves deduplication of the specified population in order to create a unique digital identity; in certain use cases uniqueness is not required.
2.2	Must support multiple forms of identification and proofing.	Biometrics can be used alone or, in conjunction with other forms of identity claims where the user will be bound to the claim once authenticated. Refugees often have no identity documents and a percentage of those that do may not be possess legitimate documents.
2.3	Must support manual override in case identity cannot be proven.	There should be a framework to support manual override but this should not be part of the foundational technical system. An audit trail should be maintained where manual override is applied.

2.4	Registration must be available offline as well as online.	Registration may be initiated offline by the user, but identity proofing will require connectivity for the registration or agent system. Similarly, credential issuance may be offline but reconciled when there is connectivity (e.g. may result in a credential revocation).
2.5	Should support the ability for the subject to create and use pseudonymous identity	Where possible, and permitted in the context of the of the identity system being implemented, the subject should have the ability to create and use pseudonymous identity.
2.6	A minimum client profile must be defined.	The client profile should observe the principle of data minimisation and ensure that a clear purpose is defined for each data item to be collected, processed and stored in order to identify the subject.
2.7	A failure mode should be included where the subject is not able to follow the normal procedure for identification.	For example, where identification would normally require fingerprints from both hands and the subject has previously suffered the loss of a hand. In this case failure mode procedures should be in place so that individuals are not excluded or disadvantaged unnecessarily.
2.8	Address Bias in Biometrics	Biometrics recognition systems trained using data collected from a specific demographic profile (age, gender, ethnicity, glasses wearers, etc.) have been shown to have a bias. The training set should be reflective of production demographics. Best practice should be observed. Poor data will affect accuracy e.g. the training data set should avoid bias. In production a performance analysis should be conducted to ensure that the system remains within specification.
2.9	Duplicate Prevention	Provision should be made in the system issuing claims (regardless of

		pseudonymity or anonymity) to identify duplicates either at the time of registration, or by application of a batch processing process (as a consequence of offline or decentralisation solutions). The need for this feature is dependant on the requirements of the system. In the case of offline or batch processing there should be provision for mitigating processes where duplicate claims are detected in order to prevent identity fraud or the existence of duplicate identities based on biometric identification or due to a clash in the generation of identifiers (e.g. GUIDs).
3	AUTHENTICATION	
3.1	Must support multiple forms of pluggable authentication, including biometrics and cryptographic secrets	Authentication Assurance Level attributes should be available to the service provider (relying party).
3.2	Should support multiple “tokens” and smart phones / PCs	There should not be assumptions regarding the devices available to individuals with regards to authentication. Multiple methods of authentication should be available to ensure inclusivity.
3.3	Alternative methods of authentication in support of failure modes	Where the subject is unable to use the primary method of authentication (e.g. a biometric) an alternative authentication method should be provided of at least equivalent in strength to the primary method.
3.4	Authentication should be available offline.	Offline authentication should be possible but to check the validity of an identity may require an online validation check to an authoritative source. An identity token may require an online validation check or a check against a local copy of same.
4	PRIVACY AND CONTROL	
4.1	Must allow the user to have granular control over the sharing of personal data	Users should have the ability to allow or deny the sharing of personal data at the point of request, as a preference before

		request, or at a later point in time, by giving their informed consent.
4.2	Must allow users to have visibility and audit-ability of consent and accesses (i.e., sharing with 3rd parties), and revocation of consent	Users should have the ability to view audit data regarding the use of their identity, especially when consent is revoked. Consent, visibility of consent / use / withdrawal of identity information, ability to revoke consent. Systems should actively alert the user when something [data] they have consented to is used for a derivative use. Consent receipts must be recoverable.
4.3	Must allow custodianship / guardianship to be exercised for applicable persons.	Must allow parents / legal guardians / caregivers to be able to take appropriate action on behalf of a minor / person being cared for. All parties must have registered identities within the system. The rules for how the relationship is established between the parties is out of scope for these requirements but should be supported technically by metadata within the identity system. This metadata should describe the type of relationship (for example parent / child or caregiver / dependent) between the parties and any ancillary information that may assist a Relying Party with authorisation such as the method and verification of the representation being described.
4.4	Must have controls against the act by an adversary to access, delete, or modify the identity.	Security controls must ensure the confidentiality and integrity of identity data, at rest or in transit, and processes put in place to protect the underlying identity system from unauthorised access or abuse. Baseline standards for data security such as ISO/IEC 27001 and the implementation of an information security management system, or equivalent,

		should be considered where appropriate. Users should be provided with an easy-to-use response mechanism. In the case of a breach at the issuing authority (credential and/or claim) the user(s) and any relying parties must be alerted electronically by a method previously agreed with those parties.
4.5	Processing, retention, and sharing of identity data shall be transparent to the subject except where legal provisions prevents it.	Subjects should expect to be able to access information electronically when and how they want. This should include information regarding how, when and by who their identity data has been accessed. This should be inline with and respect the "transparency and access" principle."
4.6	Privacy of the Subject must be protected throughout the identity lifecycle.	The principles of Privacy by Design and Data Minimisation should be observed as should the spirit of GDPR even if that Regulation is not enforced by law for a particular implementation. There should be a clear explanation of how the identity system being implemented will support GDPR (as a baseline).
4.7	PII should not be immutable and the rights of the user observed.	The Right to be Forgotten should be used liberally. PII should not be immutable in the context of the identity system being implemented.
4.8	Data accuracy should be a priority and users should be able to view and amend errors or make required updates.	Subject should be able to update erroneous, out of date, or poor quality data to reduce identity errors.
4.9	The sharing of data should be avoided where aggregate computations are sufficient.	Approve only insights that are aggregate computations on personal data, yielding aggregate answers that reduce or eliminate the possibility of re-identification of an individual through correlation of data.
4.10	Change of identity	Subjects should be able to update their identity data (e.g. name, date of birth) and where necessary biometric data.

		Where the user is unable to authenticate as part of the update process alternative modes of authentication should be provided. For example, where a biometric is used as the normal method of authentication a fall-back method such as a mobile OTP could be utilised. All changes should be auditable and verifiable by the user. Relying parties must be informed of the modality of authentication used in the context of change of identity, for example, biometric, or PIN. This will allow relying parties to manage risk when these changes are made by users.
5	ATTESTATIONS AND TRUST	
5.1	Must be able to store, and manage many attestations from governments and organizations	Privacy model must be easy to understand by the user, relying party and trust provider (including independent auditors). The issuance system must support issuance of claims by many parties such as governments and organisations. The system must support a subject being able to present claims issued to them without the risk of disintermediation. The system must support verification of claims by the issuer without the risk of disintermediation. The system should provide a claims receipt for issuance, presentation and verification.
5.2	Must be able to prove that attestations are genuine, untampered, pertains to the recipient and current status is active / not revoked	Identity related operations (of the system) must provide the ability to verify the issuance, presentation, and current state (e.g.validity) of any claim.

		Attestations should be “Provable": not just authenticity and veracity of the attestation, but the fact that it pertains to the recipient.
5.3	Must be able to attest how the identity proofing was performed.	Metadata should be provided to identify not only how the proofing was performed but also the Identity Assurance Level attained as a consequence of that proofing process and subsequent issuance of credentials.
5.4	Must not require point to point trust agreements across parties	Data sharing agreements must not be required where the subject is in control of the data.
5.5	Participation in Trust Frameworks	The system must be able to participate in a trust framework where a governance model is required to codify access rights, consensus, identity resolution, etc. The system must be able to support interoperability based on recognised standards to ensure addressability and verifiability of the presented claim. If such a framework is created, it must not impose mandatory participation for any of the basic functions of the system. Instead, it should be a set of standards/components parties can leverage to ascertain whether another entity or proof is valid within its context/rules.
6	INTEROPERABILITY	
6.1	Where possible / practical should be implemented using open source software.	Open source software and open standards for implementation should be adopted where appropriate although it is recognised that in some cases this is not possible (e.g. biometric devices). As a minimum open standards should be adopted at the edge of solution components to ensure interoperability and avoid vendor lock-in.
6.2	Must support open APIs for access to	Open APIs must be provided for all system

	data and integration with other identity system components / vendors.	components to ensure interoperability but also portability should components and/or vendors be replaced or Subjects require their data to be extracted and/or removed.
6.3	Each solution element used in implementing the Identity Lifecycle should be open standards based in order to minimize vendor lock-in	Barriers to vendor portability should be removed where possible as described in 6.1 and 6.2 above. “Can you fire your service provider”, is a good litmus test for true vendor portability.
6.4	Must be able to export the data in a machine-readable form.	Data when exported, as referred to in 6.2, should itself be provided in an open standard machine-readable format enabling ease of import into a new system/component.
7	RECOVERY AND REDRESS	
7.1	Must support secure recovery if one or more identity attributes is / are compromised / lost	Providers of identity attributes (data regarding the Subject including keys) should provide tools and/or support for secure recovery should compromise and/or loss of data be experienced.
7.2	Must support redress if identity is compromised or is inaccurate	Rules outlining mechanisms for redress should be included in either national law or as part of any agreement between the Subject and any identity proofing entity should that entity be the cause of any data error(s), breach or identity theft.
7.3	Must provide at least one key custodian in a recovery scheme	At least one custodian must exist for key recovery for the identity system being implemented and that this custodian is independent of Government where possible. In cases where Government is the only option available, assurances regarding privacy and consumer protection must be clearly made. A statement of intent regarding the future availability of non-government custodians should also be made regardless of whether the government is the initial custodian. Future solutions that support multiple

		custodians should be considered when proven in the field.

Recommendations

	Recommendation
R1	The system must observe the law as it applies to the deployment either by geography or as a consequence of the users affected by the system.
R2	Complex legal frameworks should be avoided particularly where the user is the nexus between two or more parties.