ID2020
ALLIANCE MANIFESTO

In September of 2018, ID2020 Alliance Partners, working in partnership with the United Nations High Commissioner for Refugees (UNHCR), drafted a formal articulation of our perspective on ethical approaches to digital identity. The landmark ID2020 Alliance Manifesto (www.id2020.org/manifesto) lays out these shared principles and forms a starting point to guide the future of digital identity globally.

1. The ability to prove one's identity is a fundamental and universal human right.

2. We live in a digital era. Individuals need a trusted, verifiable way to prove who they are, both in the physical world and online.

3. Over one billion people worldwide are unable to prove their identity through any recognized means. As such, they are without the protection of law, and are unable to access basic services, participate as a citizen or voter, or transact in the modern economy. Most of those affected are children and adolescents, and many are refugees, forcibly displaced, or stateless persons.

4. For some, including refugees, the stateless, and other marginalized groups, reliance on national identification systems isn't possible. This may be due to exclusion, inaccessibility, or risk, or because the credentials they do hold are not broadly recognized. While we support efforts to expand access to national identity programs, we believe it is imperative to complement such efforts by providing an alternative to individuals lacking safe and reliable access to state-based systems.

5. We believe that individuals must have control over their own digital identities, including how personal data is collected, used, and shared. Everyone should be able to assert their identity across institutional and national borders, and across time. Privacy, portability, and persistence are necessary for digital identity to meaningfully empower and protect individuals.

6. Digital identity carries significant risk if not thoughtfully designed and carefully implemented. We do not underestimate the risks of data misuse and abuse, particularly when digital identity systems are designed as large, centralized databases.

7. Technical design can mitigate some of the risks of digital identity. Emerging technology — for example, cryptographically secure, decentralized systems — could provide greater privacy protection for users, while also allowing for portability and verifiability. But widespread agreement on principles, technical design patterns, and interoperability standards is needed for decentralized digital identities to be trusted and recognized.

8. This "better" model of digital identity will not emerge spontaneously. In order for digital identities to be broadly trusted and recognized, we need sustained and transparent collaboration aligned around these shared principles, along with supporting regulatory and policy frameworks.

9. ID2020 Alliance partners jointly define functional requirements, influencing the course of technical innovation and providing a route to technical interoperability, and therefore trust and recognition.

10. The ID2020 Alliance recognizes that taking these ideas to scale requires a robust evidence base, which will inform advocacy and policy. As such, ID2020 Alliance-supported pilots are designed around a common monitoring and evaluation framework.

    We humbly recognize that this is no easy task, but we see urgency as a moral imperative. This is why we have set ambitious targets and why we hold ourselves to account.