ID2020 AT A GLANCE

The need for good digital identity is important and urgent.

Identity is vital for political, social and economic opportunity. But most systems used for identification are archaic, insecure, lack adequate privacy protection, and for one billion people, are inaccessible.

Two Converging Challenges:

Over one billion people, including millions of children, women and refugees, globally lack any form of recognized identification.

- Without an identity, individuals are often invisible - unable to vote, access healthcare, open a bank account, or recieve an education - and bear a higher risk of trafficking.
- Without accurate population data, public and private organizations struggle to broadly accurately deliver the most basic human services.

Universally, systems of digital identity frustrate users, businesses, civil society, and governments.

- For users, their data is fragmented across thousands of databases, entirely out of their control and hard to access.
- As cybersecurity risks increase, data is becoming a toxic asset for governments, companies and NGOs.
- GDPR mandates that the control of personal data rests with the individual and moves us towards a model where data is kept at source, rather than shared and aggregated.

The ID2020 Alliance is setting the future course of digital identity through a multi-stakeholder partnership, ensuring that digital identity is responsibly implemented and widely accessible. Alliance partners work together - through a transparent governance model - to:

- Fund and implement high-impact pilot pilot projects
- Shape the market by defining parameters for good digital identity and the development of technical requirements for interoperability
- Advocate for ethical approaches to digital ID that prioritize privacy and user-control.

We start with an ethical perspective and everything else follows.

Shared beliefs, outlined in the ID2020 Alliance Manifesto, underpin the commitment by our partners to "improving lives through digital identity." We are singularly focused on user-managed, privacy-protecting and portable digital identity.

- We believe that identity is a human right, and that individuals must be able to assert their identity without reliance on any single institution.
- We believe that for digital identity to improve lives it must be: privacy protecting; portable; recognized and trusted: and, owned and managed by the individual.
- We believe that, where data protection and privacy standards are met, a user-centric, portable digital identity can simultaneously improve service delivery and facilitate individual empowerment and protection.
- We believe that if designing for portability and user-centricity from the outset, implementation can be phased: meeting service delivery requirements presents an immediate opportunity for the implementing organization, while paving the way for broader use.
- We believe that a multi-stakeholder approach is essential to enable broad recognition, ensure diverse perspectives inform our approach, and ultimately reach scale.
- We believe that concurrent pilot projects with various partners will provide the strongest foundation for scaled-up implementation.
- We believe that technology offers opportunities, but is simply a piece of the puzzle.

We see ourselves as a coalition of the willing, with everything we do deriving from our ethical perspective. As that coalition grows, we believe are collective voice can shift the conversation beyond our partners.

ID2020

Why an Alliance?

- No government, company or agency can solve this challenge alone. As a collaborative effort of global partners, the Alliance is taking an approach that is holistic, market-based, and which is solving for scale at day one.
    - Partners pool capabilities, funding and innovation to crowd-source best practices.
    - As a collaborative effort of global partners -- our collective footprint numbers in the billions --, we can piggyback on the systems and networks that each of our partners already have in place. This minimizes the need to develop entirely new entry points for delivery and better positions our partner organizations to fulfill their individual mandates.
    - As the ID2020 Alliance build critical mass, our collective articulation of the parameters defining good digital ID can significantly shape the digital identity technology that is brought to market and adopted.

> Closing the identity gap is an enormous challenge. It will take the work of many committed people and organizations coming together across different geographies, sectors and technologies. But it's exciting to imagine a world where safe and secure digital identities are possible, providing everyone with an essential building block to every right and opportunity they deserve.
>
> Peggy Johnson, Executive Vice President Business Development, Microsoft

- An expansion of current initiatives ("business as usual") will be insufficient to bring about transformative impact. And ad hoc coordination also will not suffice –we need sustained and transparent collaboration.
    - Historically, investments in single use-case projects (i.e. for birth registration) have incentivized the development of siloed, non-interoperable systems. Changing the flow of funds is necessary to re-align incentives, with pooled funding serving as the catalyst for investments in holistic identity management systems that can provide benefit across use cases and throughout life.
- Strengthening national ID systems is an important and complementary thread of work, but full coverage of national ID systems does not afford critical individual protections
    - If reliant on state-issued credentials, individuals risk losing their identity and livelihoods due to misuse or regime change.
    - As individuals cross borders, either due to travel or displacement, they must be able to maintain and port their identity and an associated data.
- There is no other multi-stakeholder effort focused on portable, user-centric and privacy-protecting digital identity. ID2020 is unique in philosophy, transparent governance and market-driven approach

Our Partners:

Founding Partners

accenture Gavi The Vaccine Alliance Microsoft The Rockefeller Foundation IDEO.ORG

General Partners

kiva Mercy Corps HYPERLEDGER simprints fhi360 ICC iRespond

Who can participate in the ID2020 Alliance?

The ID2020 Alliance is differentiated by its inclusive, multi-stakeholder model and transparent governance

- The Alliance is open to all partners aligned with the beliefs outlined above and cleared through ID2020's due diligence processes.
- The governance model is designed to avoid dominance by any single institution or sector.
    - The two seats on the Board for representatives of private sector Founding Partners act as representatives of the pool of private sector Founding Partners. The same is true of the two seats for representatives of public sector Founding Partners.
    - We recognize that our collective impact will be maximized through collaboration across sectors, and even with direct competitors. To that end, Alliance partners are actively working to involve their own "rivals" in the Alliance's work.

The Alliance is committed to open standards, open source technology, and organizational transparency. While Alliance partners are able to help shape the Alliance's work, the Alliance is in no way is designed to create monopolies or vendor lock-in.

ID2020

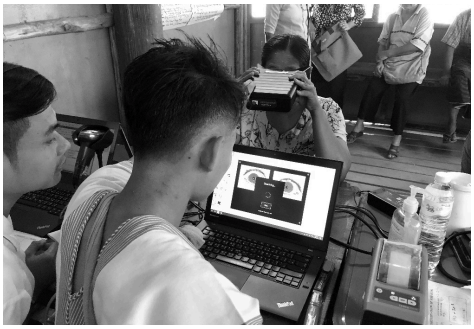
What projects does the ID2020 Alliance support?

The ID2020 Alliance supports - through funding and in-kind support - digital identity projects that simultaneously improve lives directly and generate evidence for how we maximize the potential of digital ID for everyone.

We believe that ad hoc pilots run by single institutions often have limited impact, are unsustainable, and do little to advance a larger learning agenda. Instead, we approach projects with a focus on pooled innovation and the generation of a robust evidence base, acting as a clearinghouse for "good" digital identity projects, including both including both those developed by ID2020 Alliance partners and those submitted via our online portal.

- Our projects are chosen based on whether -- in addition to their direct impact -- they will answer open and critical questions.
- We apply a common monitoring & evaluation framework across all ID2020-supported projects, facilitating comparison across projects and yielding important learnings for scalability and replicability.

We're committed to project sustainability and scale, and help our partners to build an ecosystem of long-term partners around each project.



Health and Livelihoods in Mae La Camp

Thailand

The project is providing digital ID to up to 35,000 inhabitants of the Mae La Camp on the Thai-Myanmar border, in order to facilitate better access to healthcare services and improved continuity of care. The execution and evaluation period is planned for 18 months.

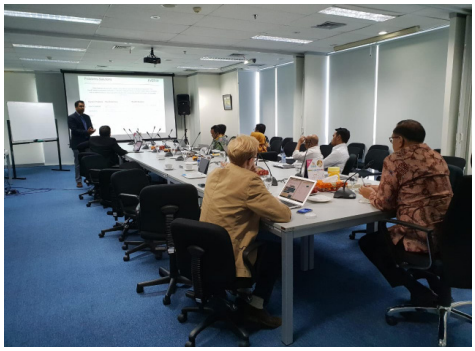
Objectives: Determine the extent to which issuing digital ID improves both access to and quality of healthcare in a highly challenging environment and assess the efficacy of the digital ID technologies, methods and procedures used in the project.

Energy Access for Low-Income Families

Indonesia

The project will provide digital ID to members of 6000 low-income families who receive government fuel subsidies, to streamline the disbursement process for the government and subsidy recipients, improve identification of qualified subsidy recipients, and reduce fraud. The project is planned for 6 months.

Objectives: Determine the extent to which issuing digital ID improves the overall fuel subsidy program from operational, financial, and beneficiary perception perspectives, and assess the efficacy of the digital ID technologies, methods and procedures used in the project.



How does ID2020 identify and select pilots?

There are two pathways by which ID2020 supported project come into being:

Online Submission: Proposals are accepted on a rolling basis. Any individual or organization meeting the required application and evaluation criteria is welcome to submit a proposal.

Partner-Led Development Alliance partners collaborate to develop a proposal, often testing the technology of one partner and its applicability in a use case proposed by another partner organization.

Evaluation: Proposals are evaluated by each of the four Advisory Committees to ensure fit with ID2020's technical, programmatic, advocacy and ethical goals

Decision taken by the ID2020 Board

ID2020

How is the ID2020 Alliance shaping the development of technology towards good digital identity?

We believe that technology, while by no means a panacea, may help mitigate some of the risks of digital identity, offering greater privacy protection, while allowing for portability and verifiability.

In recent years, commercial interest in the digital identity space has grown enormously. This poses an opportunity to leverage private sector interests towards closing the identity gap, but the rapid evolution of the ecosystem also poses significant risks that a) technology with insufficient protections for privacy and user-centricity are widely adopted, b) that non-interoperable approaches limit the utility for individuals and simply replicate the status quo, or that c) critical intellectual property is patented by a particularly acquisitive actor and prevents wide accessibility.

ID2020's Technical Advisory Committee (TAC) is translating ID2020's principles into technical requirements -- detailing what "privacy-protecting, user-centric, and portable" digital identity looks like in practice -- and launching a certification mark to build demand for and recognition of ID2020-approved digital identity technology.

- It is our belief that these requirements will give direction to companies' product development roadmaps, steering the market towards technology that is responsible. Certification allows companies meeting our technical requirements to market themselves as-such and gives those implementing these technologies confidence in adopting certified solutions.
- Heavily weighted in these requirements is a focus on modularisation, open standards, open APIs, and the portability of data between component systems, each of which we believe are critical for interoperability, portability and avoidance of vendor lock-in.
- We don't see our role as writing technical standards -- there are plenty of organizations already doing so, with a diffusion of resulting standards. Instead, we want to focus on building critical mass around a set of standards so that interoperability is actually realized.

Alliance partners share a commitment to key principles for digital identity, but remain technology- and vendor-agnostic.

- We believe that technology will continue to advance, and that we cannot pin our approach on any single technology. Instead, our Technical Advisory Committee functions as a mechanism to continually evaluate emerging technologies as they surface,

How is the ID2020 Alliance governed?

- As an alliance, the success of this initiative depends on robust collaboration and a clearly defined means for stakeholder engagement.
- The model we've adopted is based on best-practices from comparable alliances and reflects the landscape of partners currently engaged, but we note, and even expect, that this model evolves as the alliance grows.
- The ID2020 Board acts as the governing body for the Alliance and comprises 11 members: five independent Directors, two Directors nominated as representatives of the public sector Founding Partners, two Directors nominated as representatives of the private sector Founding Partners, one Director nominated as a privacy expert, and one Director representing funding organizations.
- The Board is supported by four thematic Advisory Committees, which provide in-depth advice to the ID2020 Board. Membership in these committees is set by the Board, with Founding Partners eligible to nominate representatives to two Advisory Committees.
- Time-limited, deliverables-based working groups serve as a mechanism for partner action and collaboration on specific topics, with the output of working groups feeding into the agendas of the Advisory Committees. Any ID2020 Alliance body can initiate a working group, with membership in that group self-selected and self-managed.
- Identity2020 Systems Inc (dba ID2020), a US-registered 501(c)(3) based in New York, NY will act as the Secretariat for the Alliance. As such, ID2020 is responsible and accountable for day-to-day operations, including: raising money to fund digital identity projects, coordinating with implementing partners for project implementation, ensuring robust monitoring and evaluation, legal and financial management, and administration of the governance mechanism.

ID2020's Board and Leadership

Lionel Johnson (Chair) - President, Pacific Pension Institute

John Edge (Founder, Chair Emeritus) - Fintech Entrepreneur

Dakota Gruener (Executive Director) - Forbes 30 Under 30, Brown Biology and Political Science, Formerly with Gavi

Dr. Seth Berkley (Director, Gavi) - CEO, Gavi, the Vaccine Alliance

Elana Broitman (Director) - Senior Advisor, Office of Senator Kristin Gilibrand

Oliver Bussmann (Director) - Former UBS Global Chief Information Officer

Kim Cameron (Director, Microsoft) - Microsoft Chief Architect of Identity, originator of Seven Laws of Digital Identity

Ann Cavoukian (Director, Privacy) - Distinguished Professor at Ryerson University, originator of Privacy by Design

Chip Dempsey (Director) - Chief Commercial Officer, Options Clearing Corporation

Blythe Masters (Director) - CEO, Digital Asset

David Treat (Director, Accenture) - Global Blockchain Lead, Accenture

ID2020

Joining the Alliance

While joining the ID2020 Alliance is open to all, we recognize that the Alliance itself can only be successful if fully funded and if all partners contribute what they can to the effort. As such, we've designed a tiered model intended to ensure that partnering organizations contribute at a level appropriate for their skills and competencies, while recognizing the "bold bets" made by founding partners

	PRIVATE SECTOR		PUBLIC SECTOR		INDIVIDUALS
Commitment	**Founding Partners**	**General Partners**	**Founding Partners**	**General Partners**	
Initial Commitment*	Based on # of employees: **$1M** (5,000+) **$500K** (500 - 4,999) **$200K** (50 - 499) **$50K** (<50)	n/a	No financial contribution is required for participation of public sector organizations; however, all partners will be expected and required to participate in applicable ways through the contribution of human capital, intellectual property and/or goodwill. Public sector Alliance partners are also encouraged to help finance the work of the ID2020 Alliance to the extent that grants and donations are a core operational function of the partnering organization.		
Annual Commitment*	Based on # of employees: **$250K** (5,000+) **$125K**(500 - 4,999) **$50K** (50 - 499) **$12.5K** (<50)	Based on # of employees: **$100K** (5,000+) **$50K**(500 - 4,999) **$20K** (50 - 499) **$5K** (<50)			
Benefits					
Logo on ID2020 Website	yes (featured)	yes	yes (featured)	yes	
Right to use ID2020 logo on partner website	yes	yes	yes	yes	
Participation in ID2020 events	yes (preference for speaking slots)	yes	yes (preference for speaking slots)	yes	
Organizational representative eligible for one of four (4) partner seats on the Executive Board	yes		yes		
Eligibilty to directly nominate representatives to two (2) Advisory Committees	yes		yes		
Eligibility for Advisory Committee participation through the General Partner nomination process		yes		yes	yes
Eligibility for Working Group involvement	yes	yes	yes	yes	yes

* Participation as a Founding Partner requires an up-front commitment as outlined above. The upfront commitment includes the first two (2) years of membership at the Founding Partner level. At the third anniversary of membership, Founding Partners are asked to contribute on an annual basis at the rate outlined above.

Technical Requirements v0.9

(short-form, we're happy to share the full version anytime)

ACCESSIBILITY

- Must be useful in physical, offline and online scenarios
- Must be usable in rugged environments
- Must be cost-effective across all aspects of the identity lifecycle
- Must be easy for end-users to use throughout the identity lifecycle and require minimal user education
- Must be easy to implement by the relying party and have a clear explanation of cost as well as the implications for the use digital identity
- Must be easy for implementing agents to use and explain throughout the identity lifecycle

IDENTIFICATION AND VERIFICATION

- Should be able to create a unique digital identtiy quickly and at low cost
- Must support multiple forms of identification and proofing.
- Must support manual override in case identity cannot be proven
- Registration must be available offline as well as online
- Should support the ability for the subject to create and use pseudonymous identity
- A minimum client profle must be defined
- A failure mode should be included where the subject is not about to follow the normal procedure for identification.

AUTHENTICATION

- Must support multiple forms of pluggable authentication, including biometrics and cryptographic secrets
- Should support multiple "tokens" and smart phones / PCs
- Alternative methods of authentication in support of failure modes
- Authentication should be available offline.
-

PRIVACY AND CONTROL

- Must allow the user to have granular control over the sharing of identity data
- Must allow users to have visibility and audit-ability of consent and accesses (i.e., sharing with 3rd parties), and revocation of consent
- Must allow custodianship / guardianship to be exercised for applicable persons.
- Must have controls against the act by an adversary to access, delete, or modify the identity.
- Processing, retention, and sharing of identity data shall be transparent to the subject except where legal provisions prevents it.
- Privacy of the Subject must be protected throughout the identity lifecycle.
- PII should not be immutable and the rights of the user observed.
- Data accuracy should be a priority and users should be able to view and amend errors or make required updates.

ATTESTATIONS AND TRUST

- Must be able to store, and manage many attestations from governments and organizations
- Must be able to prove that attestations are genuine, untampered, pertains to the recipient and current status is active / not revoked
- Must be able to attest how the identity proofing was performed.
- Must not require point to point trust agreements across parties
- Participation in Trust Frameworks

INTEROPERABILITY

- Where possible / practical should be implemented using open source software.
- Must support open APIs for access to data and integration with other identity system components / vendors.
- Each solution element used in implementing the Identity Lifecycle should be open standards based in order to minimize vendor lock-in
- Must be able to export the data in a machine-readable form.

RECOVERY AND REDRESS

- Must support secure recovery if one or more identity attributes is / are compromised / lost
- Must support redress if identity is compromised or is inaccurate
- Must provide at least one key custodian in a recovery scheme