Written evidence submitted by ID2020

Introduction

Since 2016, ID2020 has led the development of digital systems that provide individuals with trusted, verifiable, and portable ways to prove their identities. In the midst of the most devastating public health crisis of the last century, we are working to ensure that individual privacy and civil liberties are protected as technology solutions to support workplace and social re-entry are considered.

On March 23, Prime Minister Boris Johnson announced mandatory social distancing guidelines for residents of the United Kingdom, effectively putting the nation on lockdown. Similar orders around the world have proven an effective strategy for containing the spread of the SARS-CoV-2 virus.

Notwithstanding their effectiveness, there is broad recognition that the economic, social, and psychological costs have been enormous and cannot be maintained indefinitely. As governments around the world are facing growing pressure to resume public life and restore economic activity, the momentum behind “immunity passports” has accelerated.

On April 2, Secretary of State for Health and Social Services, Matt Hancock expressed support for a system of immunity passports, possibly in the form of a wristband. The health secretary has been cautious to predicate such plans on the availability of accurate serological testing and definitive evidence that the antibody confers a sufficient degree of immunity to those who possess it.

Most epidemiologists believe the antibody will offer some level of protection to those who have been exposed to the virus, but the presence and duration of immunity remains an open question. On April 24, the World Health Organization (WHO) issued a statement[1] noting that there is "currently no evidence that people who have recovered from COVID-19 and have antibodies are protected from a second infection." While the WHO is appropriately erring on the side of caution, a definitive answer to this question could be months or even years away.

We recognize that the deployment of some form of immunity passport or health credential is becoming increasingly likely. Therefore, ID2020 is proposing an alternate approach for “digital health credentials”, which might offer a path to safely mobilize a greater portion of the population while simultaneously addressing many of the criticisms and risks that have been raised to date.

Should the government elect to proceed, we advise caution accompanied by a full and transparent assessment of the risks and an open and inclusive public process.

---

[1] *World Health Organization Scientific Brief*, “Immunity Passports in the Context of COVID-19” (April 24, 2020) https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19

We must reject the temptation to treat technology as a panacea. Privacy and data security protections must be built into the technical architecture of any digital health certificate system. In order to safeguard personal rights and civil liberties, any technology solution must be accompanied by an appropriate, fit-for-purpose trust framework and legislative and regulatory actions to guide the implementation and ensure transparency.

Even with these safeguards in place, digital health certificates may still be insufficient to meet the current challenge. But absent such safeguards, we can be assured that they will do more harm than good.

To protect public health and restore economic activity, while simultaneously protecting civil liberties, governments, technologists, public health professionals, and privacy advocates must come together urgently to chart a path forward, together. The price of failure is simply too high.

Thinking Beyond "Immunity Certificates"

For the reasons outlined above and others, we do not believe that "immunity certificates", as currently conceived, offer a viable path forward.

We do, however, believe that there may be a workable alternative in the form of "digital health certificates" which, rather than providing proof of immunity, would serve as proof of a recent negative diagnostic test (which would need to be updated with some frequency) or of vaccination, when one becomes available.

Scientists are learning more about the SARS-CoV-2 virus every day, but are still in the early days of understanding how the virus functions. A definitive understanding of the immune response to this particular coronavirus could take months or even years to establish. To ensure that they achieve the desired objectives, digital health credentials should be premised on sound scientific evidence.

While the exact figure remains open to debate, the percentage of Britons who have been infected and, thus, possess the antibody represents a minute percentage of the population (the Office of National Statistics suggests approximately five percent nationally[2]). Thus, even if there was sufficient evidence to support immunity, the percentage of the population who would benefit from immunity certificates would be correspondingly modest. Conversely, predicating re-entry on a recent negative diagnostic test would be more resource intensive but would enable a far greater percentage of the population to return to public life.

The Department of Health and Social Care (in consultation with the WHO and other international bodies) would need to establish the duration of validity for a negative diagnostic test based on the best available scientific evidence. Risk profiles that take into account the prevalence of COVID-19 in a community (perhaps at the county level) and the degree of close-contact required in that area could be weighed to customize the

[2] Tala Khan Burki, *The Lancet Respiratory Medicine* (May 29, 2020) https://www.thelancet.com/journals/lanres/article/PIIS2213-2600(20)30247-2/fulltext

duration to fit the local context. Thus, individuals in a more rural county might require less frequent retesting than those residing in denser urban environments.

Such determinations must be made thoughtfully, with concern for equity and with appropriate consideration of the primary intent of protecting public health and secondary goal of re-mobilizing as much of the population as possible.

It is reasonable to expect that there will eventually be a vaccine. If modeled on the flu vaccine, we would expect that an individual might be considered immune for a single "season or perhaps a year, following vaccination. The accompanying vaccination certificate would remain valid for that duration. After this, individuals would either need to be re-vaccinated (particularly if the COVID vaccine, like the flu vaccine, is modified each year to match the circulating strain) or be re-tested.

Examining the Risks

Public health officials, privacy and social justice advocates, ethicists, and others have raised a variety of concerns about immunity certificates.

Broadly speaking, these criticisms fall into two categories; 1) technical concerns, relating to the privacy and security of sensitive health data and 2) equity and social justice concerns regarding the potential for health status to used as justification for discrimination or unintentionally exacerbate existing social inequities.

It is worth noting that the risks inherent to such a system are extremely context dependent. The implementation challenges in London are likely to be different than those in a town like Tunbridge Wells, for example.

Exclusion

Risk: Any digital health certificate program presents a risk of exclusion. Those able to prove their identity -- or, in this case, their health status -- are uniquely advantaged relative to those lacking verifiable proof. This is inescapable.

But equitable access is something that can be addressed. Some individuals will choose not to enroll because they mistrust either the government or the technology. Others will be unable to enroll because they do not have, or are unable to use, a smartphone. Vulnerable and marginalized communities are at particular risk of exclusion.

Mitigation: There must be an alternative means to prove one's testing status, such as a smart card, issued by the NHS. We recommend these approaches over the use of a wrist band as they can be easily concealed and thus cannot serve to stigmatize individuals on the basis of their health or socioeconomic status. To mitigate the risk further, any technology solution should allow more than one person to use a single mobile device to manage their credentials.

Ubiquitous, free, and convenient testing should be a necessary precondition for the implementation of any digital health certificate program. Because healthcare in the UK is delivered through the NHS, it is easier to ensure equitable access to testing, and

therefore to a digital health certificate. Other systemic barriers to care should be understood and addressed.

Privileged Immunity

Risk: Acquiring proof of one's testing status, especially if limited to proof of immunity, will be extraordinarily valuable. This creates potentially dangerous incentives for systemic abuse, fraud, and dangerous behaviors.

A poll published on May 8, 202 by the Daily Mail (and conducted by Redfield and Wilton Strategies)[3] reported that nearly one in five Britons (19 percent) would consider deliberately getting infected with the virus if the government introduces "immunity certificates". The dangers of such behavior are obvious, not just for the individuals but for public health.

Mitigation: ID2020's broader definition of digital health certificates helps address this by making more people eligible for reentry, thereby reducing the relative perceived value of immunity. Even with this, accompanying legislation can further reduce these incentives by ensuring that employment decisions, access to housing, and similar high-stakes determinations cannot take into account an individual's health status.

If the presence of immunity is ultimately established, a certificate carried by an uninfected individual who is able to show proof of a recent negative diagnostic test should afford the same access as one carried by someone with immunity incurred either as a result of having recovered from the illness or through vaccination.

Fraud

Risk: Because digital health certificates would be issued by the NHS, the risk of credential fraud is easier to mitigate than in a highly decentralized system like the United States.

Mitigation: Applying state of the art digital credential technologies can also mitigate the risks. It is worth noting that the potential for fraud is dramatically increased with the issuance of easily replicable media such as wristbands or paper-based cards.

Where possible, use of biometrics can provide a second layer of security, strongly binding the holder and the credential. We recommend the use of biometrics that are stored locally on the individual's device and which permit local authentication.

Careful verification processes should be followed to ensure that certificates are issued to the appropriate individuals and the standards and procedures for the verification of identity and the attribution of the data must be included as part of the accompanying Trust Framework.

---

[3] James Tapfield, *The Daily Mail*, "A FIFTH of Britons Would Consider Deliberately Getting Infected with Coronavirus If 'Immunity Certificates' are Introduced by the Government to Return to Normal Life" (May 8, 2020), https://www.dailymail.co.uk/news/article-8299905/A-FIFTH-Britons-consider-deliberately-getting-coronavirus-immunity-certificate.html

Scale

Risk: The public health benefits of a digital health certificate program can only be realized if the program reaches sufficient scale. Not only must we reach an appropriate level of adoption -- as established by epidemiologists – but we must also see high enough levels of adoption across the population. Because such a system would be implemented and managed by the NHS, this is easier to accomplish.

Even with 100 percent coverage in one area, if other communities are mistrustful of the program, are unable to access testing, or lack the technical infrastructure required, we risk a situation where communities are variably eligible to return to work. This could exacerbate existing disparities and undermine the program's overall success.

Even if every measure is taken to embed privacy into the design of the system, we must recognize that distrust may still limit adoption. Widespread concerns around data collection may make individuals wary of participating in such a program and skeptical that they will have the sole right to access and manage their personal data.

Mitigation: Extensive stakeholder outreach and collaboration with civil society organizations to develop the program, participate in monitoring, and jointly produce and disseminate consistent and accessible messaging can help build public trust and promote participation.

The Technology

As an organization deeply committed to human rights and civil liberties, ID2020 discourages the use of publicly visible identifiers, such as wristbands, in the strongest possible terms. At a minimum, they increase the potential for health status to be used in a discriminatory manner. At worst, it is easy to imagine scenarios in which they could result in violence.

We suggest a more privacy-protecting approach, such as a digital "certificate", carried on an individual's smartphone, supplemented by a smart card for those who do not have or are unwilling to use a smartphone. Digital certificates are the modern equivalents of paper certificates. In both forms, they constitute assertions, issued by an authoritative source about an individual or organization.

Such a system would enable workplaces, medical facilities, airlines, and food preparation businesses (to name just a few examples) to require individuals to disclose their COVID-19 status as a condition of access. If designed with privacy in mind from the outset, such a system would allow individuals to share their health status without providing their names, address, or any other personal identifying information.

If a digital health certificate solution is pursued, it must be:

- **Privacy-protecting**:

    - Personal data should be stored on the device, and only maintained externally by systems that have regulatory obligations for record keeping or explicit end-user consent.
    - Encrypted in-transit and at-rest
    - Cryptographically signed as authentic and verifiable
    - Secured, preferably through biometrics
    - Adhere to industry best practices for data minimization and privacy by design
    - Support selective disclosure of information and obfuscation of attributes (i.e. allowing an individual to share her age without sharing her full birthdate)

- **Portable and widely recognized**:
    - Based on open standards and protocols, to ensure robustness and ready availability of vendors
    - Interoperable across digital devices and systems, and device agnostic as much as possible
    - Adopted widely enough that users find real utility and public health objectives are met

- **Trusted**:

    - The integrity of the data needs to be secured (using cryptography) to prove that the issuer did issue the credential and when it did so.

Aside from wristbands, some have suggested other low-tech approaches, such as an equivalent to the internationally recognized yellow immunization card (Carte Jaune). However, because paper credentials often require independent verification, such systems are unwieldy and will be difficult to scale to the challenge at hand. Given the perceived value of a certificate that would allow an individual to return to work and other public activities, paper certificates or even wristbands inevitably invite fraud and counterfeiting. A smart card would be more difficult to counterfeit and would integrate more easily with the smartphone-based system.

Ongoing work on decentralized digital credentials provides the technical and ethical foundation for a secure, privacy-protecting model of digital health certificates. We believe it is possible to rapidly repurpose and deploy systems that give individuals the ability to manage their own data, at a sufficient scale to support a return to public life, while mitigating the ongoing risk of infection.

Certified Solutions: Getting the Technology Right

In 2019, ID2020 launched the first and, to date, only, certification mark for digital identity at the World Economic Forum in Davos, Switzerland. The ID2020 Certification Mark recognizes digital identity solutions that adhere to the highest standards for user-management, privacy-protection, portability, and interoperability.

The Certification offers technology companies a roadmap for the development of ethical, inclusive digital identity solutions. To be eligible for certification, solutions must adhere to the functional, outcomes-based Technical Requirements.

In addition to helping developers create better products, certification also provides a "third-party seal of approval" so that implementers, including governments — and ultimately, end-users — can trust that the technology was developed in accordance with the highest ethical and technical standards to mitigate the inherent risks. This market-based approach is already shifting the technical landscape and we have seen major multinational technology companies amend their technical approaches to comply with ID2020's requirements.

Over the past year, 29 applicants from Norway to Kenya to the United States have submitted thoughtful, detailed applications, and worked with our staff and advisory committees to complete the application process.

We are encouraging governments and other implementing entities considering digital health credentials to adopt the ID2020 Certification Technical Requirements or even require certification of all technology solutions as a condition for consideration.

ID2020 Certification Technical 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	Where possible, and permitted in the context of the of the identity system being implemented, the

	pseudonymous identity	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.
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	Users should have the ability to view audit data regarding the use of their identity, especially when

	accesses (i.e., sharing with 3rd parties), and revocation of consent	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 would be supported technically by metadata within the identity system.
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 unauthorized 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.
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 Minimization 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 Right to be Forgotten should be used liberally.

	the rights of the user observed.	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.
5	**ATTESTATIONS AND TRUST**	
5.1	Must be able to store, and manage many attestations from governments and organizations	Certificates kept local to subject Privacy model must be easy to understand by the user, relying party and trust provider (including independent auditors). Claims issuers and claims recipients can always keep a copy of the claims they issue
5.2	Must be able to prove that attestations are genuine, untampered, pertains to the recipient and current status is active / not revoked	System becomes a key distribution network to check attestations “Provable": not just verify of 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	Complex legal frameworks should be avoided particularly where the user is the nexus between two or more parties. Equally data sharing agreements should not be required where the subject is in control of the data.
5.5	Participation in Trust Frameworks	There should be an overall trust framework to participate in the system and a governance model is required to codify access rights, consensus, identity resolution, etc. 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 recognized 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 data and integration with other identity system components / vendors.	Open APIs must be provided for all system 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 breach or identity theft.
7.3	Must provide at least one key custodian in a recovery scheme	Subjects should be able to rely on a trusted custodian to perform key recovery in the case of loss or compromise. It is recommended that at least one custodian exists for the identity system being implemented although at scale we would expect multiple custodians to exist.

Conclusion

This is a moment for caution and deliberate progress.

We recognize that governments around the world are under incredible social, political, and economic pressures to expedite the return to public life and restart their economies and that these objectives must be managed concurrently with efforts to protect public health and safeguard the capacity of healthcare systems.

Given what little we know about the human body's immune response to the SARS-CoV-2 virus, we do not believe that "immunity passports", strictly defined, offer a viable path forward at this time. We also recognize that the digital health certificates we have suggested as a possible alternative may likewise be insufficient to meet the current challenge.

No solution is perfect, but with technology solutions that adhere to ID2020's stringent Certification Technical Requirements; a comprehensive trust framework; and accompanying legislative and regulatory actions, developed through extensive and open stakeholder engagement, digital health credentials may be worth considering.

Recommendations

- Proceed with caution and transparency.
- Neither wristbands nor any other kind of visible marker or insignia should be used to certify, assert, or classify individuals on the basis of health status.
- At this time, digital health certificates should only be considered as proof of a recent negative diagnostic test.
- When a vaccination becomes available, and if the presence of durable immunity is established, then the application may be expanded.
- If expanded, a digital health certificate should afford the same access or privileges whether it asserts a recent negative diagnostic test, immunization, or immunity.
- Access to testing must be ubiquitous and equitable. This means there must be adequate capacity for retesting (the frequency of which should be established by public health authorities).
- Establish clear principles to guide the development of any system for digital health credentials.
- Considering adopting the ID2020 Certification Technical Requirements or even require certification of all proposed technology solutions as a condition for consideration.
- Develop a comprehensive trust framework and legislative agenda to guide the implementation, mitigate risks, and ensure transparency.

- Careful verification processes should be followed to ensure that certificates are issued to the appropriate individuals and the standards and procedures for the verification of identity and the attribution of the data must be included as part of the accompanying Trust Framework.
- There must be an alternative (such as a smart card) to prove one's testing status for those unable or unwilling to use a smartphone. The medium should be difficult to counterfeit.
- The technology solution should also allow multiple people to use a single mobile device to manage their credentials.
- Secure the system using biometrics that bind the holder and the credential, optimally stored locally on the individual's device and which permit local authentication.
- The public engagement process should be extensive, open, and transparent. It should include (at a minimum) public health experts, frontline health providers, technologists, economists, employers, privacy and social justice advocates, and a medical ethicist.
- Establish a technical advisory committee with a mandate to develop the trust framework and an oversight committee to monitor implementation, ensure transparency, and build public trust.

June 5, 2020