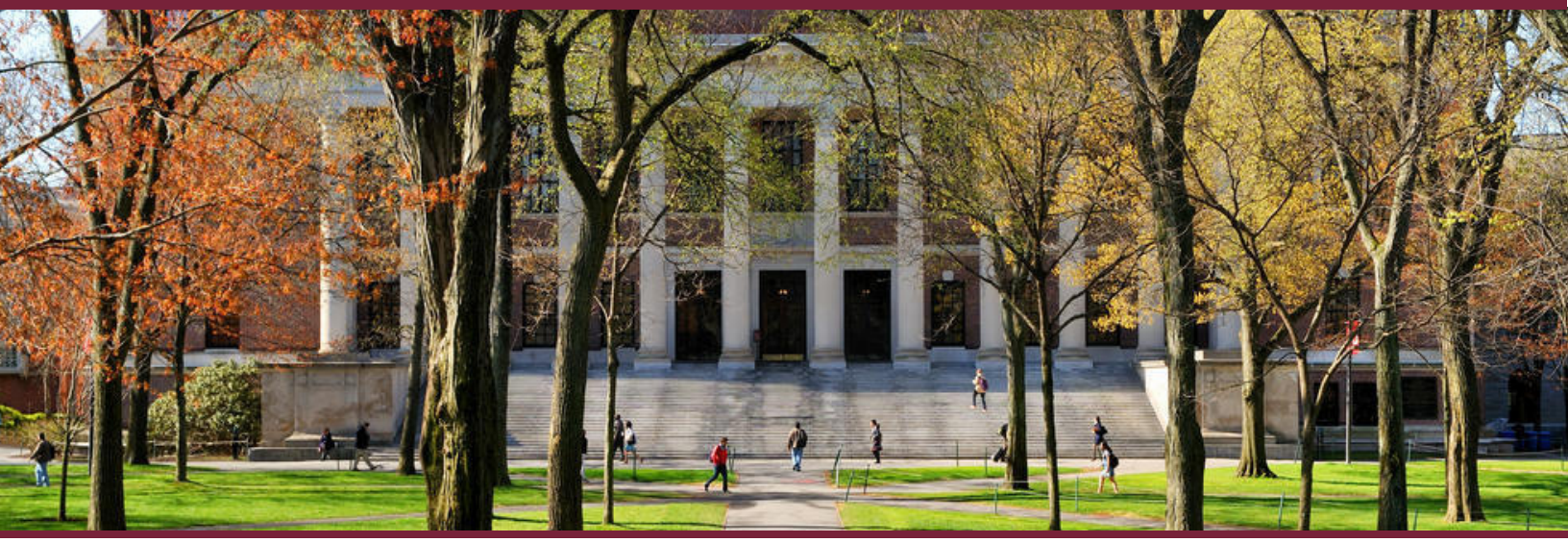
COVID-19 Rapid Response Impact Initiative | White Paper 8

Immunity Certificates:
If We Must Have Them, We Must Do It Right

April 20, 2020



Dakota Gruener[1]

EDMOND J. SAFRA Center for Ethics

Abstract

While widespread social distancing orders have proven effective at containing the spread of the COVID-19 virus (Harris 2020), the economic, social, and psychological consequences are enormous and cannot be maintained indefinitely (Sullivan and Chalkidoi 2020) .

As testing capacity ramps up, public health officials and policy makers are increasingly calling for the development of a verifiable credential or “immunity certificate"[4] that would allow individuals to prove their COVID-19 status. This is a complex proposal, one that raises concerns about privacy, exclusion, and inequality.

But preserving public health does not have to compromise personal rights. Identifying those who either have the antibodies to defeat the virus or have tested negative for the virus within a defined time period (and thus can safely return to work and school) can be done using identity technology that places control of private data in the hands of the individual.

[1] Executive Director, ID2020
[2] The Coronavirus Epidemic Curve is Already Flattening in New York City

The author would like to thank Kaliya Young (Merritt College) for her input to the paper, as well as Joshua Cohen (Apple) and Daniel Rosen (Centers for Disease Control and Prevention) for their review.

With additional gratitude to Danielle Allen, Pamela Dingle, Marielle Gross, Adrian Gropper, Vi Hart, Leah Houston, Lisa Maki, Josh Mandel, Joshua Simons, Amy Slater, Lucas Stanczyk, Lila Tretikov, Glen Weyl, and ID2020’s Board, Technical Advisory Committee and staff for their contributions and corrections. I called on the expertise of all of these people; I make no representation of where and how the report does or does not align with their views.

Conflict of Interest: The author is a shareholder in Nanomix, a privately-held point-of-care diagnostics company.

Abstract continued

Proactive adaptation of existing, purpose-built, privacy-preserving technology, grounded in respect for equity and human rights, offers a means to protect society from a resurgence of the disease, while safeguarding individual privacy and civil liberties. To protect individuals from surveillance, discrimination, fraud, or exclusion, we must ensure that systems developed to serve these purposes are private, secure, and accessible—and are developed using open-source technology and open standards for interoperability and universal access.

This paper outlines key technical and governance considerations necessary for a robust, privacy-protecting credentialing system, and discusses the risks of such programs. The paper also endeavors to sketch out the necessary rate of adoption and the likely ecosystem of partners required for successful implementation of immunity certificates. Finally, it offers a roadmap and call to action for policymakers (with a focus on North America and Europe) and to the technology community to align on standards to ensure we do not end up with fragmented implementations that fall short of meeting achievable, and essential, goals.

Table of Contents

01 Introduction

Countries around the world have resorted to an effective but blunt instrument—extreme social distancing—to stem the tide of the COVID-19 pandemic and prevent further strain on overburdened medical systems. While a necessary first step, such a strategy cannot persist indefinitely: we run the risk of deferring the spike to a later date and incurring virtually unfathomable economic, social, and psychological costs (Harris 2020). The world needs to reopen, but we must do so in a way that protects as many of us as possible and does not compromise our privacy.

There's a growing consensus that the best route forward is one in which the economy is selectively restarted in a manner that continues to protect the most vulnerable. Based on the premise—still to be scientifically proven—that people who have recovered from a COVID-19 infection acquire a level of immunity, these individuals could work and engage in some level of daily life without fear of reinfection or transmission to others. Similarly, those with a recent, negative PCR test (a genetic test to detect the presence of the virus) and no signs of infection or known exposure to the virus may also be able return to public activities.

In recent weeks, there has been growing interest in the concept of "immunity certificates," digital credentials that would allow individuals to share their COVID-19 status in a verifiable manner.

- The German government reportedly plans to issue "immunity certificates" to individuals who test positive for COVID antibodies by the end of April (Bienkov 2020a).
- The UK Health Secretary, Matt Hancock, has described an initiative pursuant to which, "People who have had the disease have got the antibodies and then have immunity can show that and therefore get back as much as possible to normal life" (Bienkov 2020b).
- The president of the Veneto region of Italy has proposed a "license" for citizens possessing antibodies. His call has been echoed by former Prime Minister Matteo Renzi who has raised the possibility of a "COVID pass" (Horowitz 2020).

Introduction

With the deployment of immunity certificates systems becoming increasingly likely, we believe there is significant value to proactively exploring the concept and ensuring that adequate safeguards, both technical and regulatory, are implemented should such programs move forward.

Ongoing work on decentralized digital identity provides the technical and ethical foundation for a secure, privacy-protecting model of immunity certificates. We believe it is possible to deploy systems that give individuals the ability to manage their own data, at a sufficient scale to assist people returning to the social sphere, while mitigating the ongoing risk of infection. Such technology exists today and can be quickly deployed.

But technology alone is not a panacea. While adequate privacy and data security protections can be built into the technical architecture of an immunity certificate system, full protection of personal rights and civil liberties depends on the development of an appropriate trust framework. Accompanying legislation and, in some cases, executive orders will be necessary to guide implementation.

With careful technical design and appropriate legislation, such an approach could be effective in the short term as nations struggle to control the pandemic and in the longer term for ongoing disease control as work sites, schools, and public places begin to reopen.

02 The Case for "Immunity Certificates"

In recent weeks, public health officials and policy makers have expressed a growing interest in the concept of "immunity certificates." Immunity certificates could provide a mechanism to enable those who present reasonable evidence that they pose a low risk of transmitting the COVID-19 virus to return to some public venues and activities. The certificates, carried on individual's smartphones, would indicate that they either had recovered from the infection and are, presumably, immune, or had a recent test indicating that they are not currently infected.

Such a system would make it feasible for 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. These individuals could share their results, time-stamped to show how recently the test was conducted, without being required to share their names or any other identifying information.

Scientists are learning more about the COVID-19 virus every day. Some public health experts argue—and limited research appears to indicate—that possessing the antibodies could provide immunity over a certain duration of time (Radcliffe 2020). Widespread serological testing will help firm up our understanding of these issues and how they relate to an accompanying system for immunity certificates. At this point, however, the potential for reinfection and the duration of immunity remains an open question.

As the evidence becomes more conclusive, it will be up to the CDC, the WHO, and other public health organizations to define the threshold of protective immunity (measured by antibody concentration) that counts as "immune" and to establish the duration of immunity. Similarly, clear guidance is necessary on the duration of validity for a negative diagnostic test, particularly to define the degree to which an individual's risk profile (i.e., the prevalence of COVID-19 within their community or the degree of

The Case for "Immunity Certificates"

close-contact required at their worksite) should be weighed in assigning that duration. Such determinations must be made thoughtfully, with concern for equity and with appropriate consideration of the need to protect public health while remobilizing as much of the population as possible.

Ultimately, we expect there will be a vaccine for COVID-19. If it is modeled on the flu vaccine, we would expect that an individual would be considered immune for a single season or year following vaccination. The accompanying vaccination certificate would be valid for that duration. After this, individuals would either need to be revaccinated (particularly if the COVID vaccine, like the flu vaccine, is modified each year to match the circulating strain) and/or would need to be tested to measure present levels of immunity.

Furthermore, it will be up to governments, regulatory agencies, civil society groups, and other stakeholders to develop fit-for-purpose legislation and adequate regulation to ensure proper governance of immunity certificates systems.

Making access, especially to workplaces, contingent on possession of an immunity certificate, could be construed as making participation functionally mandatory. However, the ultimate decision of whether to participate or to share one's certificate must lie in the hands of the user. Furthermore, there must be a non-digital medium for immunity certificates for those who don't own a smartphone or are unwilling to opt into a digital system.

Conditioning access evokes civil liberties concerns. However, if those concerns are properly addressed, such a system would be less restrictive than the alternative of blanket lockdowns and could provide a feasible pathway to accelerate economic recovery.

The Case for "Immunity Certificates"

Immunity certificates are intended as a means for lifting blanket social distancing directives. They provide a pathway to accelerate economic recovery while avoiding a resurgence in the spread and impact of the virus. Given this, we believe there is significant value to proactively exploring the concept of immunity certificates and ensuring that, should such programs move forward, appropriate technical and regulatory safeguards are established from the outset.

03 Architecting for Privacy

In recent weeks, public health officials and policy makers have expressed a growing interest in the concept of "immunity certificates." Immunity certificates could provide a mechanism to enable those who present reasonable evidence that they pose a low risk of transmitting the COVID-19 virus to return to some public venues and activities. The certificates, carried on individual's smartphones, would indicate that they either had recovered from the infection and are, presumably, immune, or had a recent test indicating that they are not currently infected.

Such a system would make it feasible for 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. These individuals could share their results, time-stamped to show how recently the test was conducted, without being required to share their names or any other identifying information.

Scientists are learning more about the COVID-19 virus every day. Some public health experts argue—and limited research appears to indicate—that possessing the antibodies could provide immunity over a certain duration of time (Radcliffe 2020). Widespread serological testing will help firm up our understanding of these issues and how they relate to an accompanying system for immunity certificates. At this point, however, the potential for reinfection and the duration of immunity remains an open question.

As the evidence becomes more conclusive, it will be up to the CDC, the WHO, and other public health organizations to define the threshold of protective immunity (measured by antibody concentration) that counts as "immune" and to establish the duration of immunity. Similarly, clear guidance is necessary on the duration of validity for a negative diagnostic test, particularly to define the degree to which an individual's risk profile (i.e., the prevalence of COVID-19 within their community or the degree of

Architecting for Privacy

While immunity certificates could aid in the recovery effort, the architecture of credentialing solutions poses risks to privacy that must be mitigated.

A centralized credentialing program, in which a single entity (likely the government) collects a list of everyone who has been tested and their test results, would leave citizens exposed to privacy violations and abuse. We believe that efforts to create centralized credentialing programs should be actively opposed by civil society[3].

A carefully designed, decentralized approach to immunity certificates could meet the same objective—verifiable, portable credentials of one's testing status—while protecting privacy.

We believe that ongoing work on decentralized credentialing provides the foundation for a secure, privacy-protecting model of immunity certificates. These solutions can be leveraged to quickly deploy a system that is privacy-protecting and resistant to fraud, and which gives individuals exclusive control over their data.

We have endeavored to describe the architecture of a decentralized credentialing solution applied to "immunity certificates," as well as key considerations around the workflow, necessary partners, and governance. Additional considerations for policy-makers around the *use* of this technology are described in subsequent sections.

[3] Centralized contact tracing programs, throughout of the scope of this paper, carry many of the same risks of immunity certificate programs.

Digital Certificates

Digital certificates are the modern equivalents of paper certificates. In both forms, certificates constitute assertions issued by an authoritative source about an individual or organization. The yellow immunization card given to parents to track their child's vaccines is a common, globally recognized paper credential. The card lists an individual's immunizations and the dates they were administered, and are attested by a health professional.

Because paper credentials are subject to fraud and often require independent verification, such systems are unwieldy and impossible to scale to the challenge at hand. If an immunity certificate solution is pursued, it must have three important features:

- Privacy-protection:
    - Personal data should be stored on the device, and only maintained externally by systems that have regulatory obligations for recordkeeping 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 their age without sharing their full birthdate)

Architecting for Privacy

Digital Certificates

- Portability and wide recognition:
  - Based on open standards and protocols[4], 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

- Trustworthiness:
  - Integrity of the data needs to be secured (using cryptography) to prove that the issuer did issue the credential and when they did so

Over the past year, the World Wide Web Consortium (W3C) has completed the development of a Verifiable Credential standard (W3C 2019), which defines the following as components for verifiable claims.

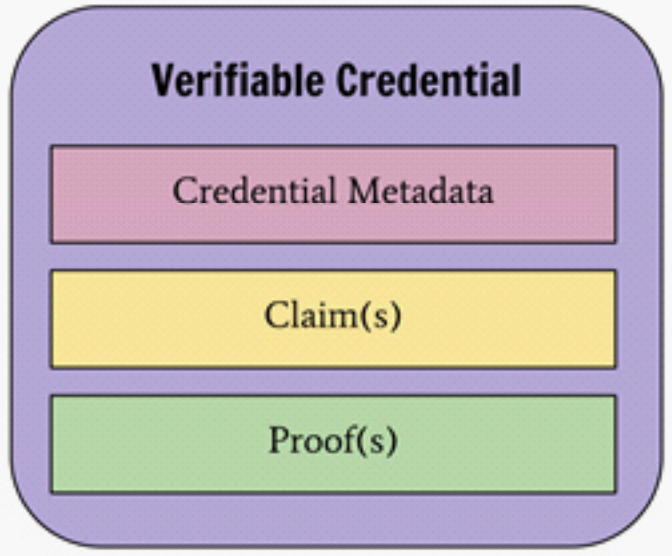


Figure 5: SOURCE: W3C 2019.

Credential metadata — This specifies the type of credential (in this case, an immunity certificate) and the type of information contained therein.

Claims — This is the data contained in the credential. For immunity certificates, the key data elements (i.e., name of the individual tested and test results) would need to be developed with input from medical professionals and public health experts, and formalized in a published schema.

[4] Without convergence on credential formats and communication protocols, the continued development of novel schemes puts at risk additional investment in new postures for hardening for security and privacy.

Architecting for Privacy

Digital Certificates

The HL7 Fast Healthcare Interoperability Resources (FHIR) specification provides a set of health care domain-specific models that could be used as the schema for claims within an immunity certificate. For example, the FHIR Diagnostic Report and Observation resources can be used to convey clinical laboratory findings and interpretations that can form the basis for downstream evaluation of the certificate.

Proofs — These are the digital signatures that "seal" the credential, proving that the credential was not altered in transit. All the information in the credential is bundled together and then digitally signed by the issuer with a private key.

When an individual presents a verifiable claim, this "seal" is checked by the organization or individual using the credential (known as the verifier). The verifier ensures that the proof signature matches the public key of the issuer, thus providing proof that the credential is real[5].

The Verifiable Credential standard is flexible, and can easily be applied to immunity certificates. Successful deployment of immunity certificates is dependent on answers to several questions:

1. **What data elements should the credential contain?** What are the essential elements of the credential (i.e., name of the person tested, test results, etc.). This must be developed by medical professionals and public health officials.
2. **Who is eligible to issue a credential?** Under what authority was it issued?

[5] This process is a use of public-key cryptography for so-called digital signatures, in which a message is signed with the sender's private key and can be verified by anyone who has access to the sender's public key. This verification proves that the sender had access to the private key, and therefore is likely to be the person associated with the public key. This also ensures that the message has not been tampered with, as a signature is mathematically bound to the message it originally was made with, and verification will fail for practically any other message, no matter how similar to the original message. See https://en.wikipedia.org/wiki/Public-key_cryptography.

The answers to such questions must be addressed at both the technology and governance levels.

It is important to acknowledge that no technical solution is without risk. While we believe that the architecture outlined above minimizes privacy risks, the technology is new and has not been deployed at a scale proposed for an immunity certificate program. Nonetheless, we believe the risks of this newer, decentralized approach are dwarfed by the known risks of alternate approaches that require a greater level of centralization.

Certificate Issuance and Use

Successful deployment and use of immunity certificates would require processes for credential issuance and use that are simple and introduce minimal friction.

In order to gain an immunity certificate, an individual will need either a test indicating the presence of COVID-19 antibodies or a negative test for the virus within a defined time period and verified by a licensed issuer, and a phone app enabling the results of that test to be shared in a confidential way. It is worth noting that in the case of a negative diagnostic test, the certificate would remain valid only for a limited time before it expires. At all times, the app would only display the results from the most recent test.

While there may be a variety of technical approaches to implement immunity certificates, the following one would adhere to ID2020's technical and ethical principles.

Architecting for Privacy

Certificate Issuance and Use

Credential Issuance

1. An individual downloads a digital wallet app on their phone.
2. The app generates and encrypts a unique identifier that cannot be traced back to the individual or device.
3. The individual undergoes testing by an ecosystem practitioner.
4. The practitioner takes a photo of the individual to accompany the test results in order to associate the results to the individual being tested.
5. When this individual's test results are received, an issuer (health care provider or testing lab) issues a verifiable credential of the individual's test status with a digital signature of authenticity. Public keys, which are associated with the private keys used to create the signatures, are published to a distributed database.
6. The issuer sends the credential directly to the app on the individual's phone.

Credential Use

1. When the individual attempts to gain access to, for instance, a place of work, the business will verify the validity of the credential, then make a determination to grant or deny access. This verification does not require contacting the issuer of the credential.
2. As part of the process of determining whether to grant or deny access, the verifier can compare the cryptographically verified photo against the individual through manual means or through automated facial recognition.

Eligible Issuers

How and where tests are run will have significant implications for who is able to issue a verifiable credential and presents an important governance consideration.

Architecting for Privacy

Certificate Issuance and Use

Currently most COVID tests (both PCR and serological) are run in central labs. Health care providers take patient samples and send them to a lab for analysis. Once a health care provider receives a patient's results from the lab, the provider shares the results with the patient.

If credential issuance is limited to health care providers, public health testing laboratories, and FDA-certified commercial laboratories, existing regimes (board licenses and lab certifications) can be leveraged to constrain eligible issuers to a known set. These individuals and organizations would be responsible for issuing credentials and would therefore be legally responsible for the accuracy of the information therein. We suggest the creation of a trust framework that publishes clear rules for being an eligible issuer. Such rules must take into account existing regulatory boundaries.

Approximately 81% of Americans and 45% of the global population have smartphones that would enable them to access the proposed digital credential (Pew 2019 and Silver 2019). As smartphone penetration is significant but not universal, alternate forms of credentials (including, but not limited to physical credentials) may be required for individuals without a device and for those in low-connectivity settings. Defining these physical credentials is beyond the scope of this paper. However, we note that the same issues of credential fraud and misuse are at least equally relevant.

We anticipate that testing will increasingly move in the coming months to point-of-care (Modern Healthcare 2020), which greatly expands the number of individuals/entities able to issue an immunity certificate. Some of the devices used for point-of-care testing are "smart devices" that are equipped with Bluetooth or Wi-Fi connectivity (Abbott 2020) and could hypothetically issue verifiable claims directly.

Lateral flow point-of-care tests, including the Cellex test approved by the FDA on April 1st (FDA 2020), promise fast testing in a format akin to a home pregnancy test. At the moment, use of these tests is

restricted only to laboratories certified under the Clinical Laboratory Improvement Amendments of 1988 (CLIA), but we can envision a scenario, months from now, when millions of tests are distributed for use in homes and field settings. Should this occur, we believe it is critical that individuals continue to rely on a trusted third party—in effect, a biomedical notary—who can attest "I saw the test be administered, and can vouch for the date and results."

Finally, once a vaccine is developed and brought to market, we will need to expand the ecosystem of entities eligible to issue credentials to include health care professionals who are administering vaccines.

Interoperability

Our world is built on common standards. Standardized measures for weight and length allow us to easily compare prices between gallons of milk, or distances between locations. The internet, similarly, is built upon thousands of standards, including the SMTP protocol for email that ensures that any email client that can "speak" SMTP can send an email to any other client using the same protocol. HTML acts as a common language such that any browser, built by any company, will display the same content on a website.

Open standards provide interoperability across a wide array of systems and applications. Open standards are created by internationally recognized standards bodies with the input and agreement of diverse companies and are free and open to anyone to implement.

There are two relatively mature open standards that have been developed for decentralized identity:

Verifiable Credentials: This standard, which has been approved by the W3C, defines a data format

for verifiable credentials. It allows any individual or organization to package a credential with claims about any other organization or individual. This can be used to create a common credential for COVID-19 status that is widely recognized and accepted.

Decentralized Identifier: This standard, which is in the process of being standardized at the W3C, provides the means to share and look up cryptographic key material necessary to create proofs.

A third protocol for authentication and communication of such credentials and identifiers is necessary to achieve meaningful interoperability. Such a protocol would enable issuers to issue credentials to individuals using different digital wallets, and would enable individuals to present their credentials to any verifier. Convergence within the technical community around an authentication and communication standard is of immediate and critical importance.

04 Implementing for Equity and the Protection of Civil Liberties

The immunity certificate model poses risks for individuals and public health alike. The primary risk stemming from the design of these technologies is the risk to privacy. Solutions must be designed to protect the privacy of individuals, whether immune or infected, while facilitating the sharing of data necessary to control the pandemic and return individuals to their work and day-to-day routines.

However, the most important risk associated with the widespread use of this technology is the risk that such individual liberties as freedom of movement, freedom of association, and free choice of occupation will be arbitrarily or discriminatorily restricted. Mitigating these known risks is a matter of public policy; as such, it is essential that policymakers considering an immunity certificate program openly discuss known risks, as described below, and enact enabling legislation that mitigates risks to the extent possible.

Risks of Exclusion

Any digital ID program presents a risk of exclusion: those able to prove their identity, or in this case their testing status, are uniquely advantaged relative to those lacking verifiable proof. In many countries around the world, national digital ID programs have become requisite to claim pensions, food rations, and other vital social services. But any individuals who didn't enroll or couldn't enroll, either due to marginalization, inaccessibility, or mistrust of the government, have found themselves increasingly locked out of these services and without redress. Electronic systems often produce binary answers—an individual is eligible or ineligible—and have inflexible rules around them.

Vulnerable and marginalized communities are at particular risk of exclusion. A system that relies on ownership of a smartphone means that some people, often the elderly, the homeless, and those in

low-income areas, will not be able to access the technology. Given this, an alternative means to prove one's testing status, such as paper-based printouts from a doctor's visit, must be considered acceptable proof by employers, venues, and individuals. To mitigate the risk further, solutions should allow more than one person to use a single device to manage their immunity certificates.

A further risk, particularly in the current phase of the pandemic when testing capacity is limited, is the risk of discrimination in terms of who has access to testing, and therefore to an immunity certificate. Systemic barriers to accessing the medical system may disproportionately hinder low-income and minority communities from being tested (Perrin and Turner 2019). And undocumented individuals and those lacking state-issued forms of identification may be unable or unwilling to access testing sites or to confirm their identities to a doctor for the purpose of credential issuance. Ubiquitous, free, and convenient testing will help to mitigate such concerns, but will not address them entirely.

For any reentry program to be successful, all persons must be able to interact with the system and receive immunity attestation without fear or risk. Only truly comprehensive programs will minimize the risk of additional peaks of the pandemic and avoid the most underserved disproportionately bearing the social, economic, and health-related harms of the pandemic.

Risks Posed by Privileging Immunity

Two scenarios have been proposed under which individuals will be able to return to work, school, and some social activities. In the first scenario, people who have had COVID-19 and have recovered with presumed immunity will, by identifying themselves as belonging in this group, be eligible to return to many normal activities.

Implementing for Equity and the Protection of Civil Liberties

Risks Posed by Privileging Immunity

In the second scenario, individuals who haven't had COVID-19 (as demonstrated by a lack of antibodies in their blood test) and who show no indication of being infected may also be able to resume their daily activities if they undergo frequent testing to confirm their uninfected status.

Each of these scenarios carries the potential for abuse. Acquiring proof of one's testing status will be extraordinarily valuable, creating potentially dangerous incentives for systemic abuse. This is a concern as testing capacity ramps up—until testing is truly ubiquitous, inequities in access to testing will have profound implications for who can return to work and to day-to-day life.

And although the certificate carried by an uninfected individual should afford the same access as one carried by someone with presumptive immunity, the requirement for regular testing for uninfected individuals, particularly when testing capacity is constrained, will likely privilege those with immunity. Clear guidance from the CDC or WHO is necessary to ensure that the duration of validity for a negative test is established based on the best scientific evidence, with concern for equity and with appropriate consideration of the need to protect public health while mobilizing as much of the population as possible.

Even with careful legislation and convenient testing, some uninfected individuals, desperate to return to their daily lives, may deliberately risk infection, betting that they'll recover and be eligible for the "golden ticket" certifying their immunity. The dangers in such behavior are obvious, not just for the individual, but for the public's health. These risks should be addressed in accompanying legislation to ensure that employment decisions, such as hiring and firing, cannot be made on the basis of health status. Wage protections for those who contract the virus, or who test positive and therefore must be quarantined, would further reduce these incentives.

A second risk relates to credential fraud. An unscrupulous health care provider or testing facility may

find the economic gain from the production of falsified testing data to be irresistible. Rapid, convenient, and free testing should reduce the temptation of credential fraud. Available technologies can also mitigate the risks. Careful verification processes should be followed to ensure certificates are issued to the right individuals, and the standards and procedures for the verification of identity and attribution of the data must be included as part of the trust framework developed. Where possible, use of biometrics may provide a second layer of security, strongly binding the holder and the credential; we recommend the use of biometrics that are stored locally on an individual's device and that permit local authentication.

Liability

The issue of legal liability for testers and for the developers and deployers of the proposed digital certificate system can be addressed through legislation that indemnifies these parties from liability Such legislation could be modeled on the National Childhood Vaccine Injury Act of 1986 (42 U.S.C. §§ 300aa-1 to 300aa-34), which established a federal "no fault" compensation scheme for individuals who may have been injured by specific covered vaccines.

Necessary Scale

Public health benefits promised by an immunity 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. Even with 100% coverage in one area, if other communities are mistrustful of the program, lack access to testing, or lack the technical infrastructure required, we risk a situation where communities are variably eligible to return to work, which could exacerbate existing disparities and undermine the program's overall success.

Implementing for Equity and the Protection of Civil Liberties

Necessary Scale

Even if every measure is taken to embed privacy into the design of the system, we must recognize that distrust may limit adoption. Widespread concerns around data collection may make some individuals wary of participating in such a program and skeptical that they will have the sole right to access and manage their personal data. Trustworthy, consistent, and accessible messaging will help mitigate these risks. Additionally, significant effort should be directed at mobilizing civic leaders and other influencers to lend their support to the initiative.

05 Looking Ahead

While many are eager to deploy such a system, an effective immunity certificate program rests on widespread testing and fit-for-purpose governance structures, neither of which is yet available. As such, we believe that the next six weeks, as testing capacity continues to ramp up, provide a window to develop the necessary governance structures (legislation, regulation, and trust frameworks) in order to mitigate the risks of immunity certificates systems.

Existing work on verifiable credentials could provide a strong foundation for decentralized, privacy-protecting immunity certificates, and a number of companies are rapidly developing the platforms needed to issue them. We know of at least three efforts which should be ready for deployment in May, and expect that many more will emerge in the coming weeks. But these systems can only be effective once testing and governance are implemented.

Over the next month, as testing and credentialing systems come online, the immediate priorities for collaboration are:

1. The development of a standardized schema for describing the state of immunity, without reference to any specific serological method and history of symptoms and testing. This should be developed, ideally, at the international level.
2. Development of fit-for-purpose legislation and regulation, and agreement on a trust framework that clearly defines, within a given jurisdiction, who is eligible to issue a certificate.
3. Agreement within the technical community on an authentication and communication protocol appropriate for this use case. ID2020 will support this through the ID2020 Certification Initiative, certifying only those solutions that are truly interoperable.
4. The establishment of government-led national- and state-level working groups of policymakers, health care providers, laboratories, businesses, and civil society to serve as fora for the consideration of needed measures to ensure the establishment, integrity, utility, and adoption of an effective and civil liberties-protecting certification system.

06 Conclusion

Immunity certificates may be an essential next step to reversing the economic and social consequences of COVID-19. Proactive use of intentionally designed technology—decentralized, privacy-protecting, and built on open standards—provides a route to the creation of such certificates without surrendering privacy. But these systems can only be effective once testing is ubiquitous, convenient, and free.

The use of such systems poses significant concerns about equity and civil liberties that must be addressed through careful enabling legislation. Therefore, stakeholders from the public and private sectors need to work together in order to develop the capacities and protections necessary to ensure that the benefits of these systems are realized, and their risks are mitigated.

07 References

Abbott. 2020. i-STAT 1 Wireless. Product Information. https://www.pointofcare.abbott/us/en/offerings/istat/istat-wireless

Bienkov, Adam. 2020a. "Germany Could Issue Thousands of People Coronavirus 'Immunity Certificates' So They Can Leave the Lockdown Early." *Business Insider*, March 30, 2020. https://www.businessinsider.com/coronavirus-germany-covid-19-immunity-certificates-testing-social-distancing-lockdown-2020-3.

Bienkov, Adam. 2020b. "The UK Plans to Issue Coronavirus 'Immunity Passports' so People Can Leave the Lockdown Early." *Business Insider*, April 3, 2020. https://www.businessinsider.com/uk-plans-coronavirus-immunity-passports-so-brits-can-leave-lockdown-2020-4.

FDA. 2020. Cellex: Fact Sheet for Healthcare Providers. EUA Letter April 1, 2020. https://www.fda.gov/media/136625/download

Harris, Jeffrey E. 2020. "The Coronavirus Epidemic Curve is Already Flattening in New York City." National Bureau of Economic Research. NBER Working Paper No. 29617. Issued April 2020. https://www.nber.org/papers/w26917.

Horowitz, Jason. 2020. "In Italy, Going Back to Work May Depend on Having the Right Antibodies." *New York Times*, April 4, 2020. https://www.nytimes.com/2020/04/04/world/europe/italy-coronavirus-antibodies.html

Modern Healthcare. 2020. "FDA Approves the First COVID-19 Point-of-Care Diagnostic Test. Posted March 23, 2020. https://www.modernhealthcare.com/technology/fda-approves-first-covid-19-point-care-diagnostic-test

Perrin, Andrew, and Erica Turner. 2019. "Smartphones Help Blacks, Hispanics Bridge Some—But Not All—Digital Gaps with Whites." Pew Research Center, posted August 19, 2019. https://www.pewresearch.org/fact-tank/2019/08/20/smartphones-help-blacks-hispanics-bridge-some-but-not-all-digital-gaps-with-whites/

Pew Research Center. 2019. "Mobile Fact Sheet." Posted June 12, 2019. https://www.pewresearch.org/internet/fact-sheet/mobile/

Radcliffe, Shawn. 2020. "How Antibody Testing Can Help Us Fight COVID-19." *Healthline*, posted April 4, 2020. https://www.healthline.com/health-news/how-antibody-testing-can-help-us-fight-covid-19-#When-will-testing-be-widely-available?

References

Silver, Laura. 2019. “Smartphone Ownership Is growing Rapidly Around the World, but Not Always Equally.” Pew Research Center: Global Attitudes & Trends, posted February 5, 2019. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/

Sullivan, Richard, and Kalipso Chalkidoi. 2020. “Urgent Call for an Exit Plan: The Economic and Social Consequences of Responses to COVID-19 Pandemic.” Center for Global Development, posted March 31, 2020. https://www.cgdev.org/blog/urgent-call-exit-plan-economic-and-social-consequences-responses-covid-19-pandemic.

W3C. 2019. Verifiable Credentials Data Model 1.0: Expressing Verifiable Information on the Web. W3C Recommendation, November 19, 2019. https://www.w3.org/TR/vc-data-model