evernym

Responding to the COVID-19 Challenge

How **verifiable credential technology** can reboot public trust and support the fight against the COVID-19 pandemic.

BACKGROUND

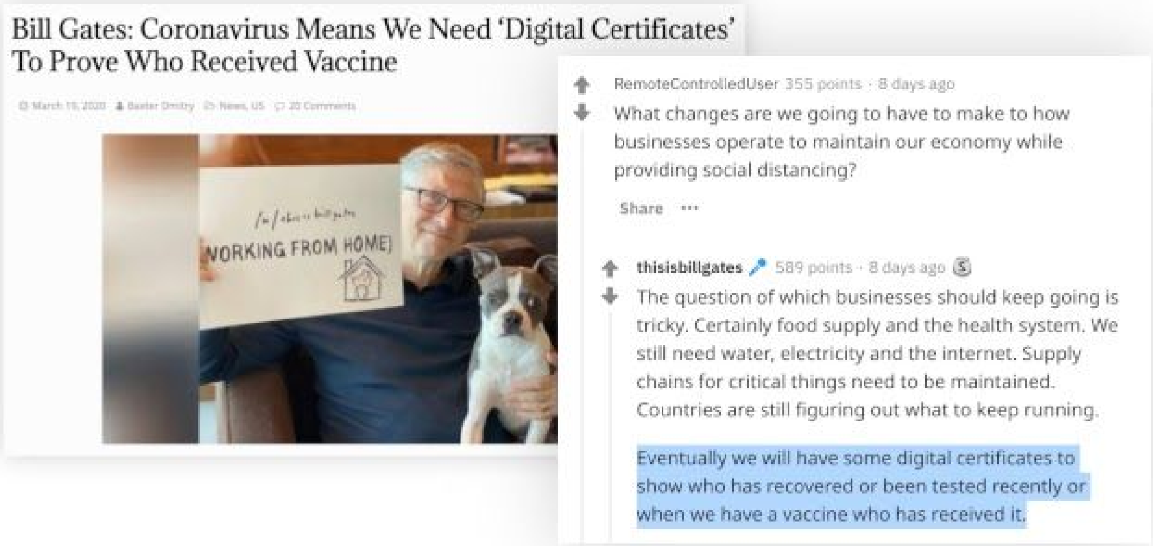
COVID-19 has changed the way we're currently living our lives and interacting with one another.

Today, each of us wrestles with life-or-death questions that we would not have dreamed of just a few short weeks ago:

- Am I a danger to my loved ones and friends—or vice versa?
- Is it safe to go to work in the local grocery store, or to deliver food and supplies?
- Can family members or staff enter a care facility for the elderly to help?

These same trust issues will become even more critical to containment as government lockdowns start to lift and life slowly starts to return to normal. The airline industry will need to know who has been cleared to travel, hospitals will need a way of knowing which visitors are safe to let in, and companies will need to prevent further spread once employees start returning to the office.

Informal trust is important, and as a society, we rely on conventions that build it. But it takes more than goodwill, common sense, and traditional manners when the backdrop is a life-threatening pandemic. **Formal, provable trust is required**, as both China and South Korea have demonstrated—and as Bill Gates astutely observed a few days ago: we will need “digital certificates to show who has recovered or been tested recently or when we have a vaccine who has received it.”



Bill Gates: Coronavirus Means We Need 'Digital Certificates' To Prove Who Received Vaccine

March 19, 2020 · Baxter Dmitry · News, US · 20 Comments

RemoteControlledUser 355 points · 8 days ago

What changes are we going to have to make to how businesses operate to maintain our economy while providing social distancing?

thisisbillgates 589 points · 8 days ago

The question of which businesses should keep going is tricky. Certainly food supply and the health system. We still need water, electricity and the internet. Supply chains for critical things need to be maintained. Countries are still figuring out what to keep running.

Eventually we will have some digital certificates to show who has recovered or been tested recently or when we have a vaccine who has received it.

Bill Gates on a March 18 Reddit AMA

Verifiable Credentials

There is very good news: the blueprint for the technology that Bill Gates imagines actually became a global standard last November. It's called **verifiable credentials**. As the digital equivalent of the credentials you carry in your wallet every day, verifiable credentials are already delivering value in pilots and early production deployments around the world.

This means that within a matter of weeks, healthcare facilities and COVID-19 testing services could start issuing digitally-signed credentials about a patient's COVID-19 status directly to their smartphones. With a quick touchless scan of a QR code, that individual can prove that he or she is currently virus-free, or has been vaccinated (once that is available). True to the spirit of verifiable credentials, this certificate could contain no personally identifiable information—meaning privacy and confidentiality can be preserved at all times—while still providing strong cryptographic proof that the credential belongs to that person.

Such a digital credential would be massively harder to fake or spoof than any paper or plastic credential. And it can be issued in seconds—and revoked in seconds if that individual's COVID-19 status changes.

But we must be careful: **the choices we make today about how these digital credentials are deployed will have implications for years to come**.

The extraordinary efforts of China's central government have saved many locally, and by extension, throughout the world. However, they depend upon a strong central government that's willing to abridge personal autonomy in troubling ways. Citizens are scanned as they board busses, approach crosswalks, and cross barricades. A complete record of movements and body temperatures, hour-by-hour and interaction-by-interaction, is compiled and tracked for many citizens.

This perhaps unavoidable in the heat of the early stages of an emergency. However, we need to think about the long-term consequences of building such digital infrastructure across society. Is it appropriate when a lockdown is lifted? Do we want a world where our data can be demanded or shared without our consent? There is a real danger of these emergency solutions becoming the new normal, and we cannot accept a loss of privacy or a surveillance economy as the defaults once this crisis is over. The privacy rules around the usage of these credentials will shape civil society for years to come.

Solutions put forward are not just about our global health. They become central to helping our global economy recover from this pandemic.

While work will be required for additional implementations, the technology, and the standards are here. Verifiable credential technology is already powering several key projects, spanning government (verifiable public directories), financial services (banks, credit unions, FinTechs), healthcare (doctor onboarding), humanitarian services (portable identity for refugees, privacy-preserving HIV testing), and many other sectors.

Beyond digital test certificates

Of course, digital credentials can be used for a lot more than just identifying whether or not someone has been tested or vaccinated.

The global response to COVID-19 has simply accelerated an existing trend towards an increasingly digital society. Millions around the globe are now working from home for the first time, and many more are taking their first online classes. Almost overnight, organizations have been forced to redesign their information architecture in a way to authenticate and onboard users remotely.

For some, this is a temporary measure. For others who have enjoyed the opportunity to work and study remotely, this will be a lasting trend.

In healthcare, where resources are re-allocated across hospitals with the most demand, we're seeing our front-line healthcare professionals (and even students and retired doctors) mobilized to meet demand. Hospital IT staff must now find a way to onboard physicians to new hospital systems, track capacity and movement across hospitals, and prove that temporary staff are qualified to treat patients. And all of this has to be done as quickly and seamlessly as possible.

We're also seeing a surge of non-critical visits conducted through video chat in an effort to "flatten the curve," and we must also support telehealth use cases in which healthcare professionals can prove their qualifications remotely, and patients can prove their coverage, all in a way that protects patient privacy.

All of these use cases–and likely, many more that will surface in the coming weeks–can benefit from the same verifiable credential technology, and we're working with partners to design the optimal architecture for each.

Transparent collaboration is key

In order to design and deploy this solution at the speed and scale necessary, we're calling on the world's governments, healthcare organizations, tech companies, and innovators to collaborate on COVID-19 credentials, with a focus on **three areas**:

1. Credentials: Define a set of immediately useful verifiable credentials and the technical requirements for issuing and verifying them. Focus on very specific trust problems unique to the COVID-19 pandemic. Investigate and understand the unintended consequences of their use.

2. Rules: Design and publish a **governance framework** that defines what policies must be followed by issuers of these credentials, what levels of assurance they will provide about the security and privacy of the data. Further, define what happens if something goes wrong, and set out the safeguards required to prevent abuse by governments, hackers, and others with power.

3. Technology: Cooperate on advancing existing verifiable credential-focused open source technology such that a greater number of organizations can more easily make use of it.

Special consideration and provision must be made towards **inclusion**—many populations do not have smartphones, Internet access, or even traditional forms of physical identity credential.

Alignment on the aforementioned points will help to facilitate an environment in which technology companies can focus on deploying solutions that can be widely adopted. Further, solutions adhering to these guidelines will benefit from being globally interoperable; a credential issued by any organization, anywhere, can be verified by any other.

When people and organizations can start making better-informed decisions based on verifiable COVID-19 credentials, uncertainty will be reduced, which will help kickstart the economy. We will start to develop clear rules and customs about what other kinds of credentials are needed when. With this technology, we can create a common tool that could help each of us know what it takes to stay safe.

Ready to support this initiative?

Evernym is already working with others to put this plan into action. We're collaborating with our community, as well as with some of the smartest people on the front line of the COVID-19 response to help design industry-standard COVID-19 credentials and a globally-interoperable governance framework. We're talking to other global leaders within the verifiable credentials ecosystem, and we're engaged with global brands, many of whom have already offered their support. But this endeavor will take many hands and your help might be critical.

We're now issuing a call to action for any organization with specific verifiable credential expertise, as well as those looking to help sponsor or deploy the technology. If you'd like to join us in this initiative, please contact us at covid19@evernym.com or visit www.evernym.com/covid19 for more information.

Further reading

- A Gentle Introduction to Verifiable Credentials (Evernym, Oct 2019)
- Yuval Noah Harari: The World After Coronavirus (Financial Times, Mar 2020)
- Privacy Could Be the Next Victim of the Coronavirus (Fortune, Mar 2020)
- Coronavirus and Privacy: Finding the Middle Ground (Computer Weekly, Mar 2020)
- We're Not Going Back to Normal (MIT Technology Review, Mar 2020)
- What Can Go Wrong: Credential Fraud Threat Modeling (Hyperledger Aries, May 2019)