Disposable ID - a new trust- and privacy-based-approach for Health Certificates on SARS-CoV-2

The world has globally locked down due to SARS-CoV-2 (commonly referred to as COVID-19). A worldwide run has begun on building digital solutions to support the rebooting of civil life, travel and economic activities. To date, most focus was laid on so-called 'contract tracing'. Another important lever could be the credible exchange of health certificates. But exchanging and tracking individuals health status potentially even by apps can lead to massive invasion of individuals privacy and data autonomy. A citizen-network of almost 150 international researchers, privacy advocates and civil activists have created a joint proposal on building technology layers for self sovereign identities to manage SARS-CoV-2 health certificates and data on a user centric and user controlled environment.

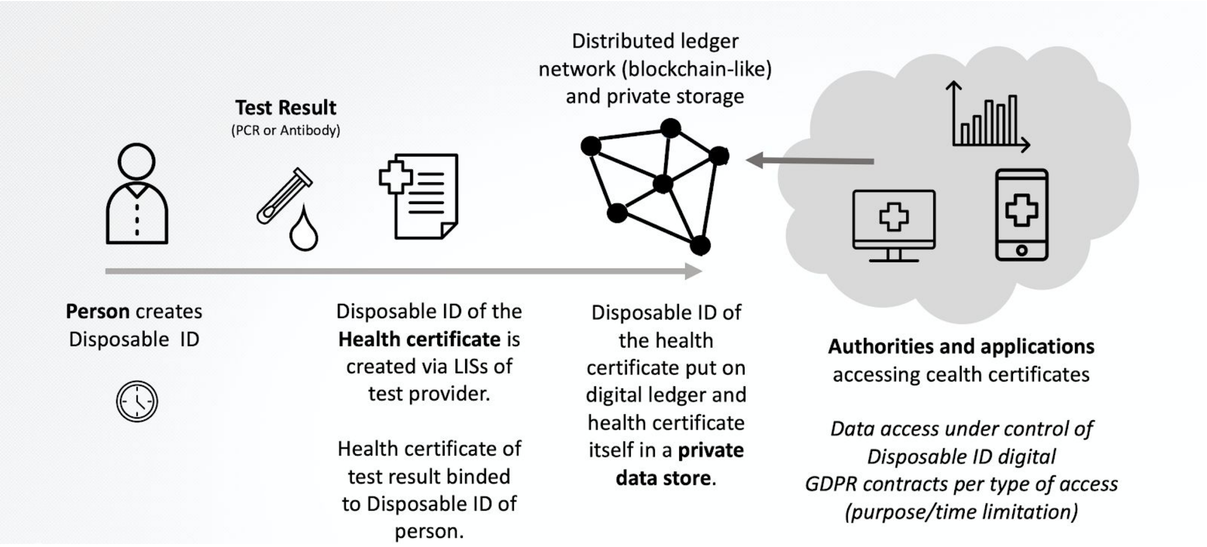
They advocate a technical concept called **"Disposable IDs"**, enabling storage and exchange of SARS-CoV-2 health data in line with the strong European data protection policies of GDPR and SSI (Self Sovereign Identities). The Disposable ID is a decentralized and cryptographic security-based scheme to link digital data with an individual's information. The unique approach: individuals can create multiple "IDs" and connect selected data to it that they wish to share for a specific usage or event. They can subsequently limit the lifetime and distribution of such an ID+Data to a specific person or authority, for a specific time, purpose and even location. All data linked to such a Disposable ID is therefore closely controlled by the user defined conditions, which the user can also revoke at any time. In this way, individuals get a self sovereign, complete control on all data connected to their respective Disposable IDs.

How Disposable IDs will enable SARS-CoV-2 health certificates

A system based on Disposable IDs will enable the creation (and sharing) of an official health status, via a digital certificate , to remain entirely under the individuals control, without losing control of their privacy, fundamental citizen rights or data sovereignty[1]. Owners of multiple

[1] Data sovereignty is a country-specific requirement that data is subject to the laws of the country in which it is collected or processed and must remain within its borders.

Disposable IDs can choose to limit the lifetime of it's linked data by revoking a Disposable ID, for example once the data is no longer relevant or required. Individuals will also be able to control the personal identifying data to be connected to their health certificate, for example a validated photograph, or fingerprint, no name, address or other information that is not required in the event of being required to demonstrate health status. There is no possibility for 3rd parties to recover a disposed ID or to recover the data and events tied to such IDs. Furthermore it may be possible for an individual to keep a detailed overview of who has connected with or accessed each Disposable ID + Data. As Disposable IDs are made for distributed ledger systems (for example DP-T3) the system provides an important building block for app based sharing of individuals health certificates and status on SARS-CoV-2.



Distributed ledger network (blockchain-like) and private storage
Test Result
(PCR or Antibody)
Person creates Disposable ID
Disposable ID of the Health certificate is created via LISs of test provider.
Health certificate of test result binded to Disposable ID of person.
Disposable ID of the health certificate put on digital ledger and health certificate itself in a private data store.
Authorities and applications accessing cealth certificates
Data access under control of Disposable ID digital GDPR contracts per type of access (purpose/time limitation)

Fig.1: Automatic transfer of health certificates binded to Disposable ID from lab tests to digital wallets (schematic illustration)

Automated health certificates from lab testing to a personal digital wallet is only one use case the Disposable ID community is working on. It is hoped that this development will provide invaluable support and even speed up rebooting of society and the economy after a period of pandemic isolation or lock-down. Including for example the controlled opening of workplaces, large events and even global travel but in a way that supports rather than compromises current data sovereignty, in a safe, secure and privacy respecting way. A smartphone enabled digital certificate allows individuals to securely store their SARS-CoV-2 testing results in a private data store while keeping full control of this sensitive data, for as long as it remains relevant. Such a certificate can be shared for various events, for example to proceed boarding a plane or accessing public events. To ensure a stable architecture and adequate testing and peer evaluation before putting it to use, the current DIHD technology under development is focused primarily on the the widely predicted second wave at the end of the year as well as supporting a safer   post-corona lockdown ‘new’ normal.

A NGO for Disposable IDs for high level transparency and independency

While reliable technology is crucial, the DHID group believes in the principles of privacy, transparency and openness to build to earn public trust and gain high adoption and acceptance rate by users , authorities and other organisations. To provide a high level of transparency and independence of the technology stack, Disposable IDs will be maintained by a Foundation in Belgium. This NGO is settled in the European Union to comply with the strong European standards on privacy and data protection.

Get more information on Disposable IDs on GitHub:
https://github.com/disposableidentities/healthcrisis

Join the Telegram Channel to contribute the community:
https://t.me/joinchat/PVV8JxfWegIq3SIFMuS1Gg