Global Vaccine Passport System

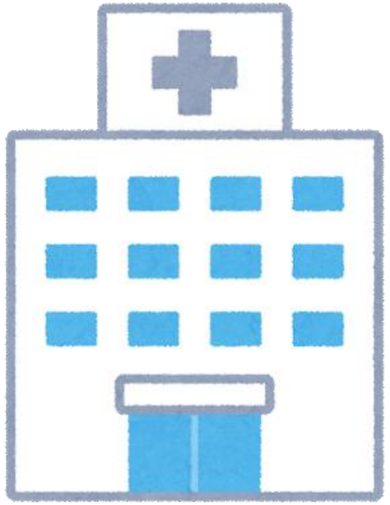
Compliant to International Standard ISO/IEC 24643 (Ecma-417) to protect privacy and prevent from counterfeit certificates

June 2021

What is Vaccine Passport System
How it can be used globally?

Domestic use, e.g,
at stadium entrance
to check if the holder's
vaccination is valid for the day

Vaccine Passport Server
To record vaccination record for all holders



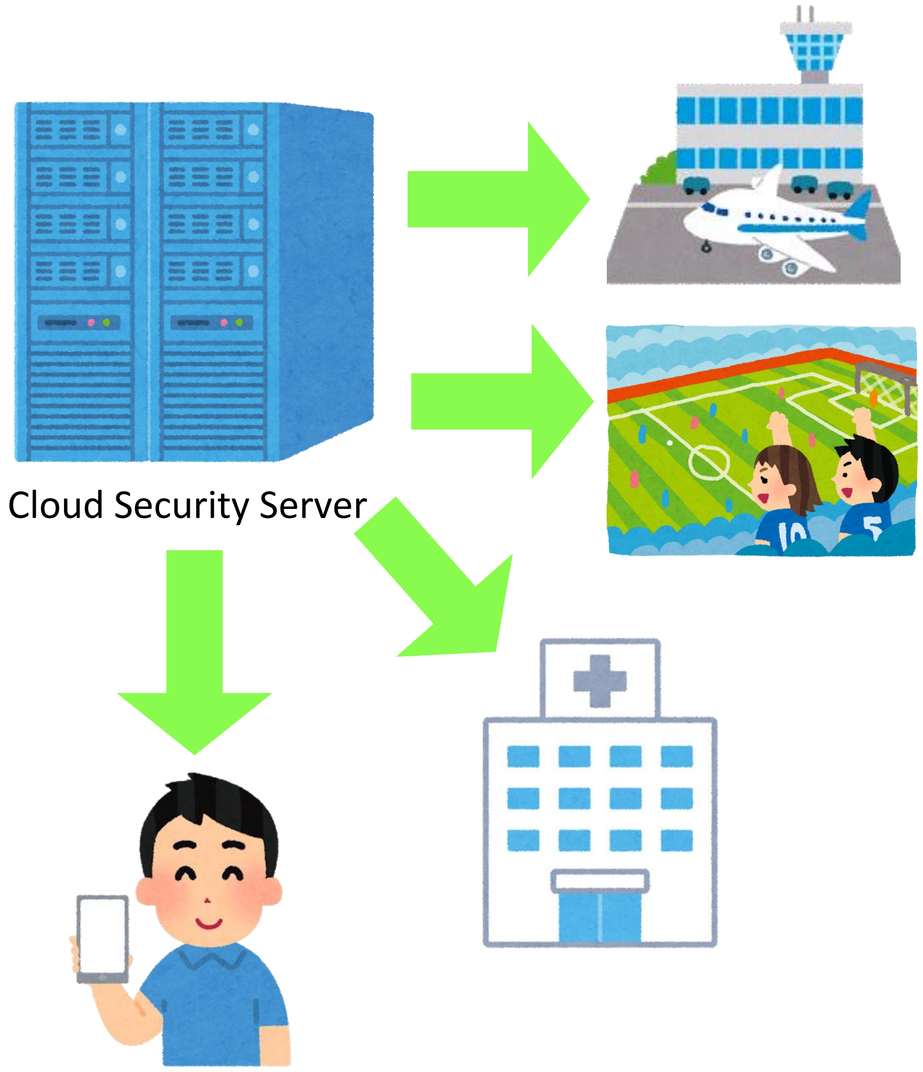
Original vaccination record
At the site where vaccinated,
Say a hospital

Cross-border use, e.g. at Passport Control

Vaccine Passport System enables an authorized people to check authenticated vaccination certificates, PCR negativity certificate of the holder via smartphone or tablet say by the immigration officer at the airport's passport control.

GVE maintains the vaccine passport server which enables hospital application, passport control/ immigration office application, passport holders' application to be connected without compromising privacy protection.

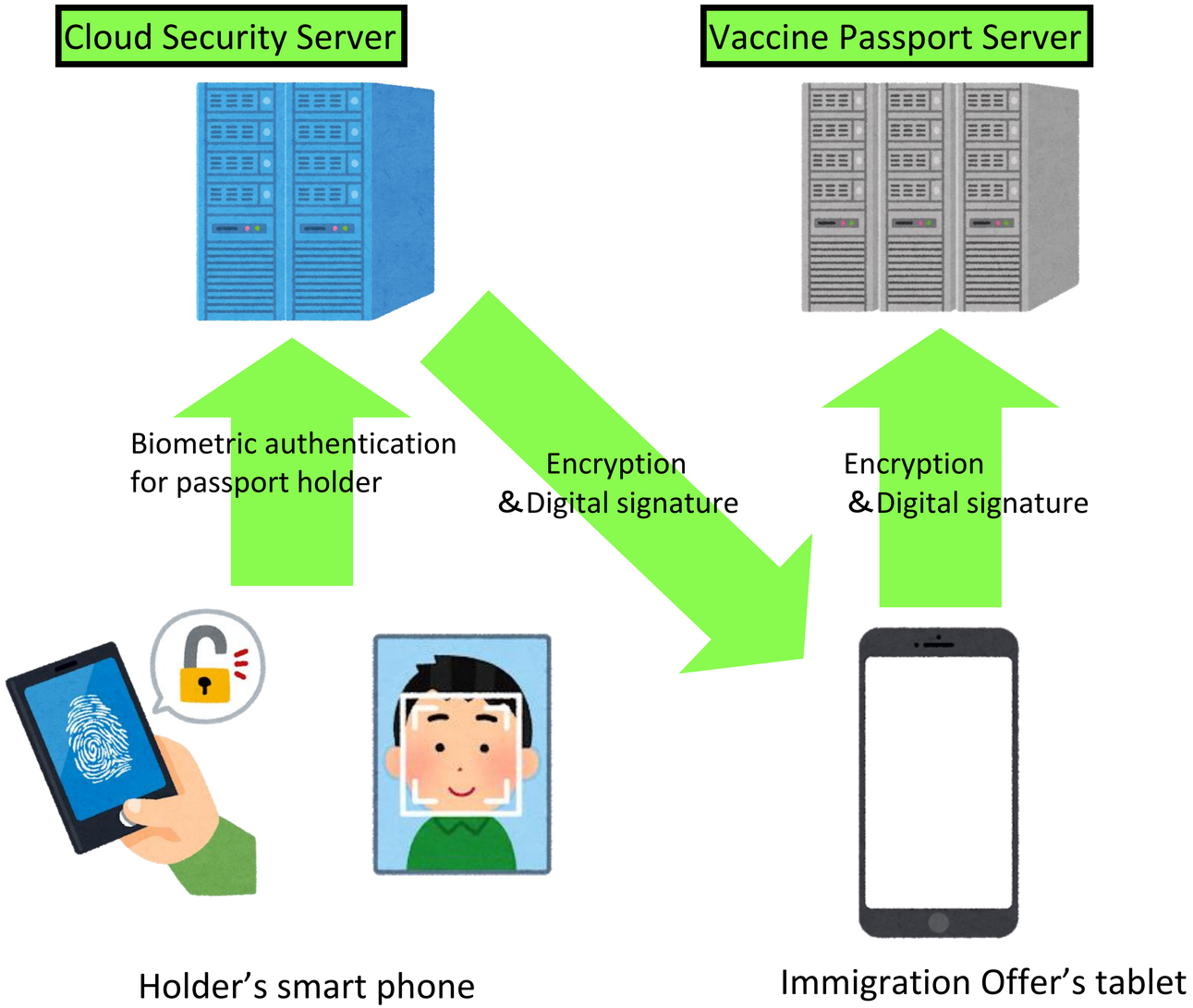
Security & Privacy Protection Enhanced System – Cloud Security Server



GVE's Cloud Security Server which contains GVE Hardware Security Module(GVE HSM) will ensure the security pathway between devices and the Vaccine Passport Server.
Each GVE HSM has the functions including (1) encryption, (2) storing digital keys for the holder, and (3) assigning digital signature for all communications.
Cloud Security Server consists of multiple GVE HSMs, enables 24/7/365 online system to access highly secured encrypted record in real-time.
This architecture is regarded as the most effective private data protection by design.

GVE HSM

End to end authentication System – Biometric authentication & Security Server



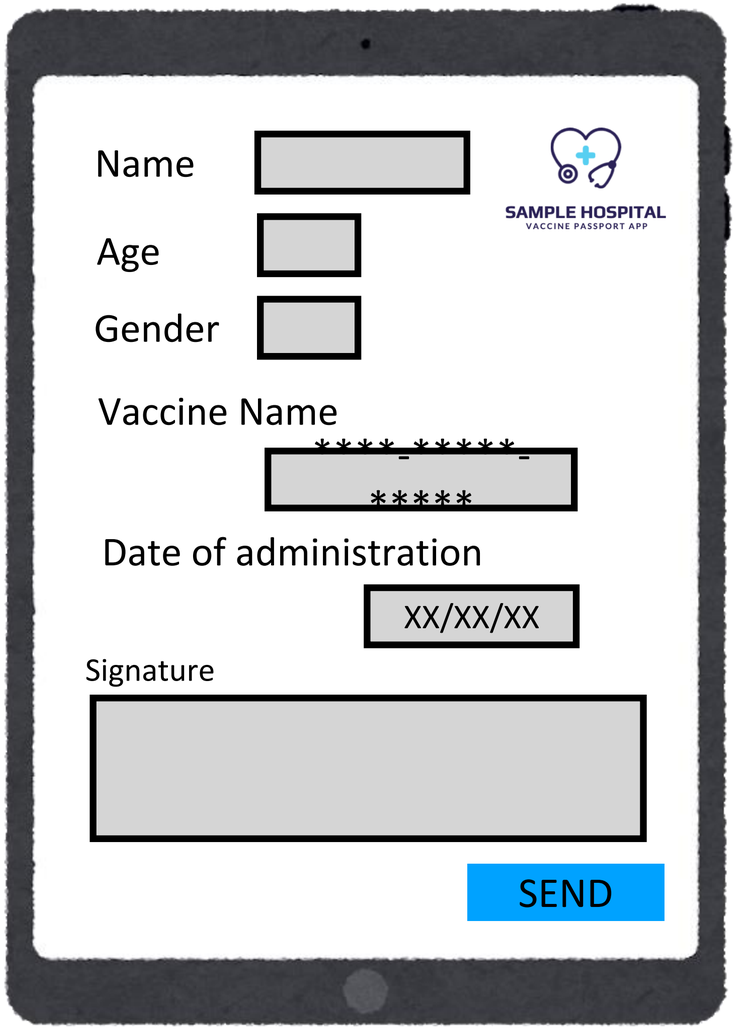
The device owned by the vaccine passport holder will access to the Cloud Security Server and obtain the digital signature while the data is being encrypted.

The combination of the digital signature and encryption enables the system to prevent unauthorized hacker from intercepting, changing the data or pretending the holder.

The data transmission among servers and devices are all done with digital signatures. By checking the authenticity of digital signature, counterfeit or intervention by an unauthorized party is prevented.

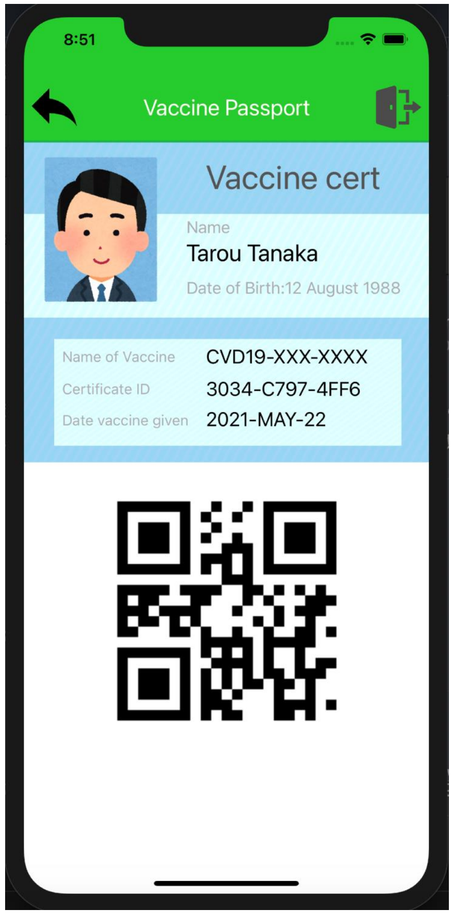
In order to check the access authority, the holder's device (e.g., smartphone, tablet) will check the person with biometric authentication. In this way, an unauthorized person cannot access to the application of the vaccine passport holder's device.

Input vaccination record via Hospital Tablet Application



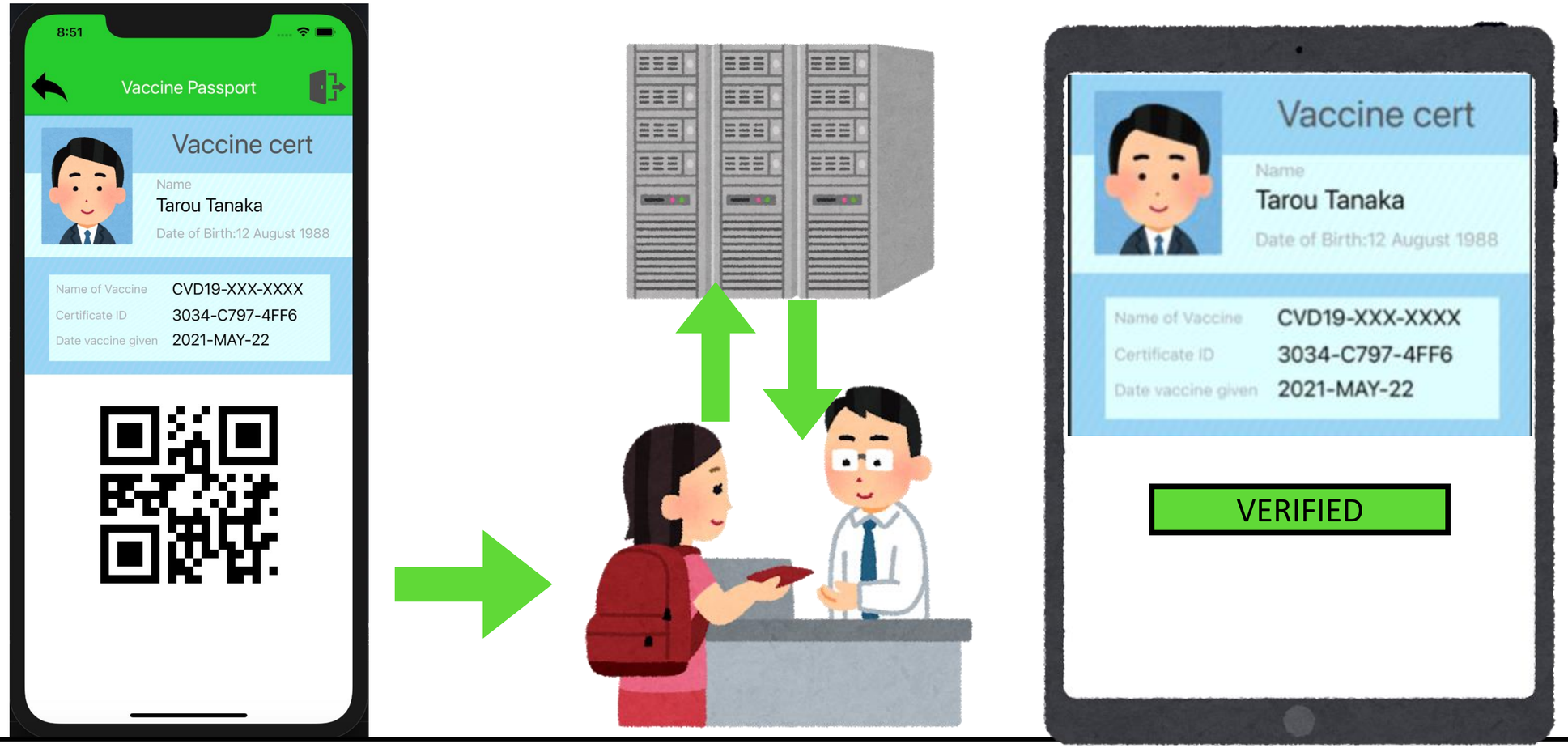
At hospital where vaccination takes place, vaccination details of each individual needs to be recorded.
The record will be sent to the vaccination server. The server will issue the access authority QR code which will be passed to the vaccinated person.
The vaccine passport holder will keep the QR code which enables to access to the server thus the passport holder can check his/her own record at the Vaccination Server at any time.

Vaccine passport holder application



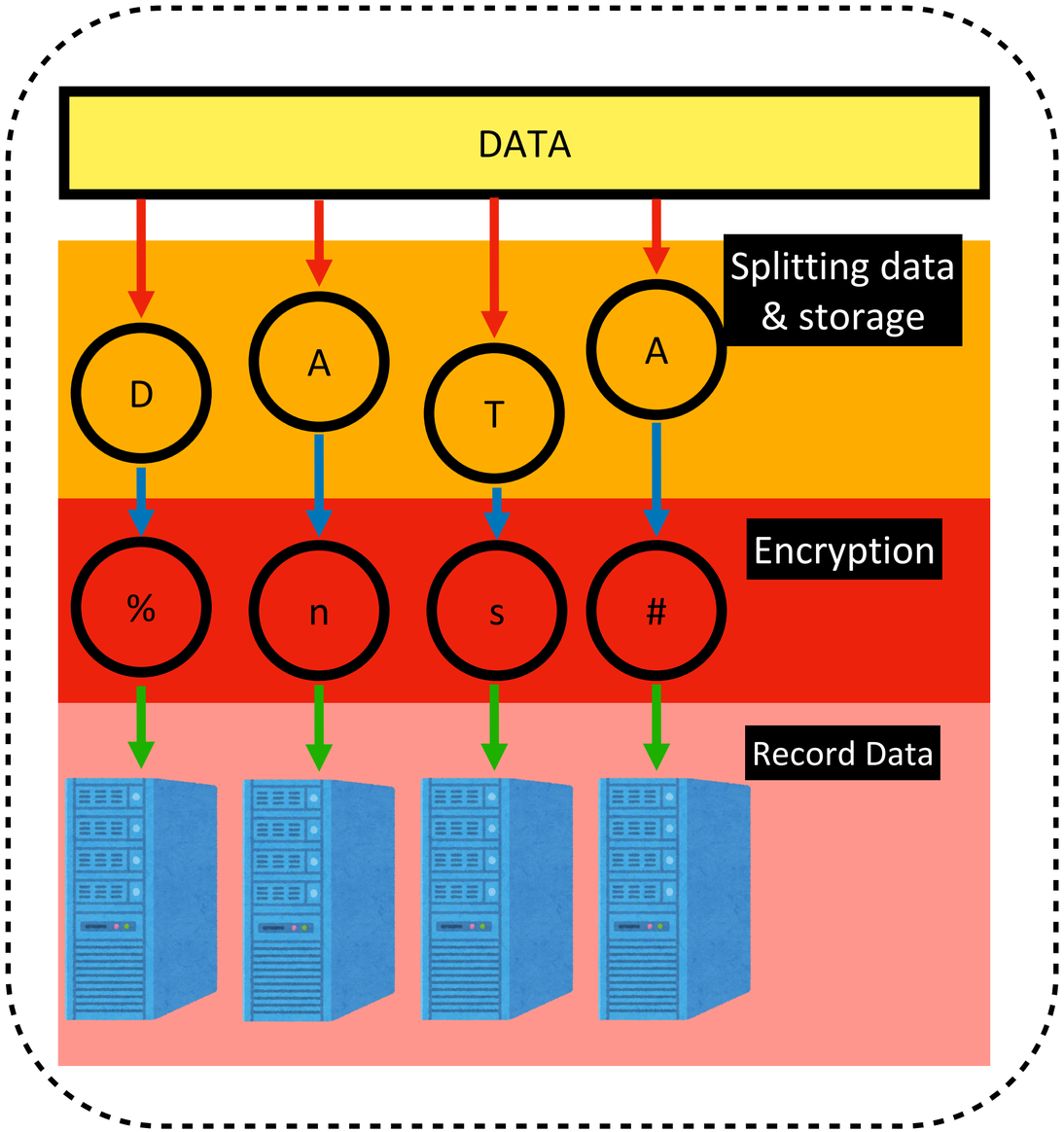
The holder is able to access her own vaccination record by her mobile device via vaccine passport application.
The default is to show QR code which is the Identification number for the access to the relevant vaccination record, the immigration Officer is ablet to access to the right record in the vaccine passport server.

Immigration Officer Tablet Application as an example



An authorised officer at the passport control area, say at the airport or at border, is able to access in real-time the vaccination record of the vaccine passport holder by reading the QR code from the device (e.g., smartphone) or paper of the holder.
QR code is the unique identification reference number (ID) for the holder.
Using the unique ID created by the Vaccine Passport Server enables the authorized person to check if the record is authenticated original data. This will prevent counterfeit or forgery attempts.
In order to prevent the forgery attempt, each of the vaccination record has a unique reference number which will not overlap for 8 billion people around the world for more than 100 years.

Additional Private Data Protection
Multiple-layer Protection Architecture for Confidential Data



In order to achieve the maximum protection for private data, GVE's Vaccine Passport Server will (1) split data in pieces and (2) encrypt each split data by different encryption method.

The data is recorded and stored in a number of physically separated servers.

Under GVE's maximum security regime, even the unauthorized access is made to one of several servers and stolen, it would be impossible for the unauthorised party to reconstruct the original data.