guardtime

guardtime.com

Guardtime

VaccineGuard

by Guardtime Health
Ain Aaviksoo (Chief Medical Officer)
Garrett Day (Lead Product Engineer)

Whitepaper
January 2021

Solution overview and technical characteristics | January 2021

(Accompanying “VaccineGuard User Guide”)

Contents

BACKGROUND 3

WHY VACCINEGUARD? 4

HOW DOES VACCINEGUARD HELP? 5

WHAT IS VACCINEGUARD? 7

- Globally verifiable Certificate with reliable data 7
- Privacy-preserving Certificate verification 9
- End-to-end visibility of authentic vaccines supply chain 10
- Real-time insights for vaccination program steering 11
- Pharmacovigilance and other post-vaccination monitoring 13

KEY TECHNICAL ASPECTS 14

- General service design and architectural criteria 14
- Privacy management 15
  - Where is data stored and processed? 15
  - How is the verification facilitated? 17

GETTING STARTED WITH VACCINEGUARD 17

- What do I Need? 17
  - 1. No-Premise Deployment 18
  - 2. On-Premise Deployment 18
  - 3. Subscription 18
- Pilot Engagement 19

Background

The Covid-19 pandemic has revealed an urgent need for a global and cross-sector response to mitigate the spread of communicable diseases which are capable of severe global impact. Vaccination against the virus is expected to be one of the core strategic approaches to this end, as it reduces both the individual risk of carrying and spreading the infection as well as protecting public health by reducing the probability of disease spread.

Implementing an effective global vaccination program against SARS-CoV-2 for 7.7 billion people in every corner of the world within 2 years is perhaps one of the most complex endeavors ever undertaken. It may be the largest product launch in human history and poses huge risks for public officials as well as for the companies involved in this undertaking.

Roll-out must balance equitable access in the initial shortage phase and overcome skepticism expressed by large part of the population later on. A robust public health monitoring system is required to steer this effectively. It is important to keep track of vaccinations at the individual level (e.g. multiple doses, side-effects etc.) as well as at the population level (priority management, uptake and allocation fairness etc.). Quality monitoring (pharmacovigilance) is more important than ever due to record speed of development, the number of totally new technologies used for Covid19 vaccines, and the sheer number of competing vaccines that are being deployed simultaneously.

On the other hand, manufacturing and distributing the vaccines on this scale around the world requires logistical planning and cooperation of multiple organizations within and across countries with clockwork precision. Government authorities and private companies need to work closely together while maintaining integrity of their respective roles. Good and reliable information becomes vital for maintaining public trust under such circumstances.

Equally important is the need to establish a system that will allow reliable verification of being immunized. As the need to go back to normal activities and travel is overwhelming there will be a huge incentive for bad actors in public and private organizations, as well across the medical supply chain, to produce fraudulent attestations and incorrect procedures to counterfeit and divert vaccines.

Reopening the economy locally as well as globally requires any vaccination certificate solution to provide assurance that the individual has been truly and effectively vaccinated. This requires a reliable link between the individual, the specific (functional) vaccine and a trustworthy healthcare institution where the vaccination was given.

Guardtime has developed and is globally implementing VaccineGuard – the solution to monitor vaccination campaigns and supply-chain in real time connected by globally verifiable vaccination certificates.

VaccineGuard can be applied worldwide with uniform security, both on paper and with modern digital platforms, regardless of the country's level of digital development. The proposed solution can be integrated with existing, proprietary IT systems to ensure fast implementation of the solution. The solution is being piloted as part of a collaboration on digital health between the World Health Organization and the Government of Estonia.

Why VaccineGuard?

VaccineGuard is built to make Covid19 vaccination campaigns a success instead of a mess. For this, we link multiple systems that are all integral to vaccination delivery into common reliable information and communication space - locally and worldwide.

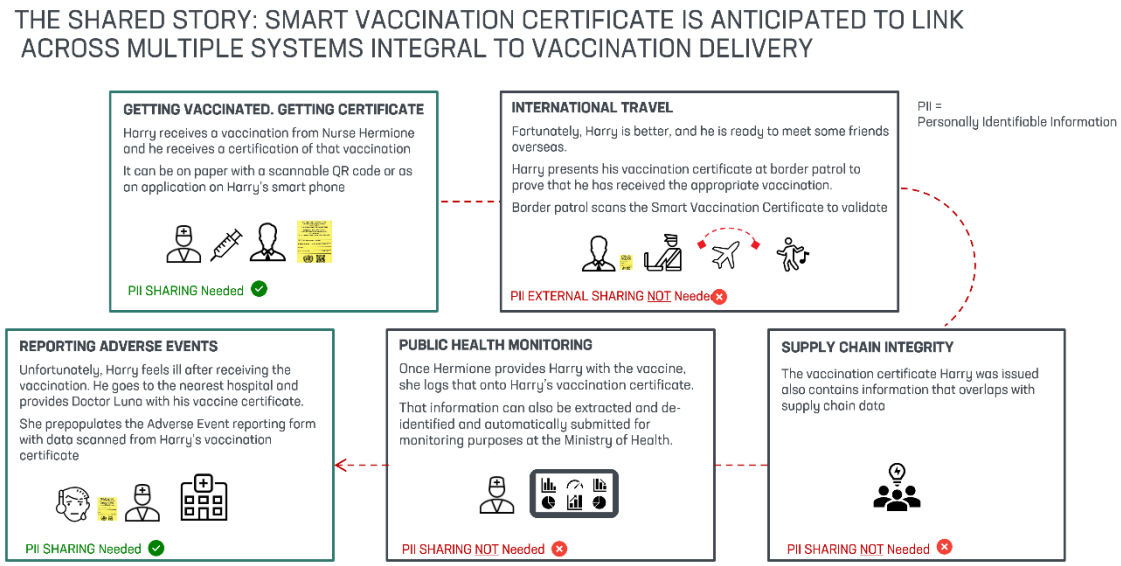
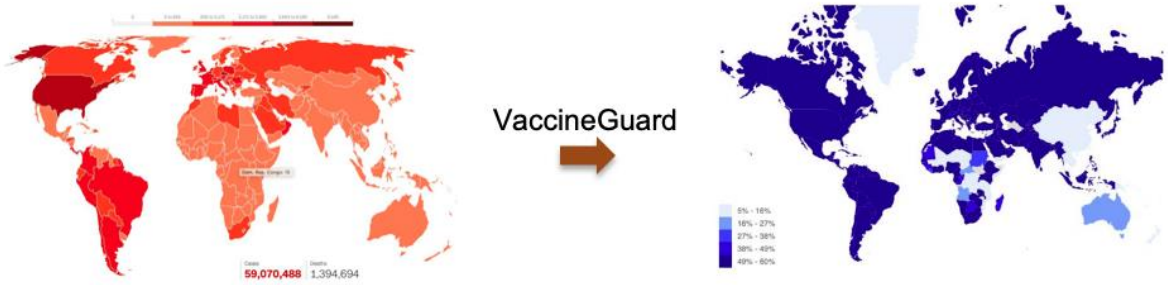


Figure 1. Smart Vaccination Certificate and the link between various components of vaccine delivery (Slide courtesy by Natschja Ratanaprajul from WHO)

Figure 1 demonstrates how the medical procedure of vaccine administration is linked with the issuance of a trusted certificate about the fact. Next, this certificate can be used worldwide to verify vaccination status, e.g., if this is required to cross the border or access a high-risk facility. Importantly, vaccine distribution (supply-chain) requires up-to-date information to avoid shortages or discover counterfeits. Further, public health reporting is vital to coordinate effective and equitable vaccination campaign roll-out. Eventually, all the previous information needs to be available for investigation of rare but important discovery of unwanted adverse events.

Following this approach, vaccination programs can operate based on real-time field intelligence, gradually replacing the "Covid19 incidence map" with the "Covid19 vaccination map".



How does VaccineGuard help?

VaccineGuard is designed to connect multiple systems that are all integral to vaccination delivery. The solution allows different interlinked stakeholders to execute their tasks and for the companies and governments responsible for managing the rollout to obtain real time insights on the plan's performance based on reliable information. At the same time, VaccineGuard maintains the highest level of security and privacy protections for sensitive data while supporting each respective role - individuals, public authorities or manufacturers - in their tasks with single version of reliable information.

VACCINEGUARD: CERTIFICATE FOR TRAVEL EFFECTIVENESS AND SAFETY UPDATES

+ Providing proof of Covid19 tests and vaccination (certification)
+ Providing independent verification of the certificates
+ Notification on vaccine effectiveness. Warning about counterfeits
+ Monitoring supply chain integrity and vaccine quality

FOR PEOPLE VaccineGuard provides a globally valid digitally verifiable vaccination certificate to enable safe travel and confidence in the authenticity of the vaccine used, but also a rapid feedback during vaccine's quality monitoring / pharmacovigilance period (for example, notification when new information about the vaccine's effectiveness becomes available, etc.).

FOR PUBLIC HEALTH AUTHORITIES that are responsible for the vaccination campaign, VaccineGuard provides an operational overview of the implementation of the vaccination campaign within their jurisdiction, but also internationally for effective collaboration (imagine a map with vaccination uptake instead of infection incidence).

VACCINEGUARD: GLOBALLY VERIFIABLE CERTIFICATES AUGMENTING VACCINATION CAMPAIGN EFFECTIVENESS

+ Providing proof of Covid19 tests and vaccination (certification)
+ Providing independent verification of the certificates
+ Monitor vaccine uptake among population in real time
+ Collect insights about supply chain integrity and pharmacovigilance

VACCINEGUARD: END-TO-END SUPPLY-CHAIN VISIBILITY USING REAL TIME VACCINATION DATA

+ Proof that 1 vaccine has been used to vaccinate 1 individual
+ Proof that the vaccine has been used where it was sent
+ Real time overview of vaccine uptake among population. Everywhere
+ Real time alerts on counterfeits and pharmacovigilance

Similarly, **VACCINE MANUFACTURERS** will receive anonymous real time insight about supply-chain effectiveness (where are vaccines admitted, level of available stocks) as well as early warning on diversion (when vaccines intended for one country surface in another place) or counterfeit (when vaccinations are performed with non-authentic vaccines).

For all the involved parties, VaccineGuard provides effective quality monitoring and mitigation support by facilitating high accuracy pharmacovigilance data collection, analysis as well as rapid distribution to the relevant entity. Public Health Authorities will receive early warning that can be communicated to the manufacturers for rapid mitigation measures; citizens will get timely notifications if new information will become known about their vaccination appointments.

This will be achieved by anonymous reporting that is securely linked to the unique vaccination record and supply chain process artefacts using the same cryptographic method that protects the reliability of certificates as well as the privacy of individuals.

VaccineGuard has the unique capability to link independent records that are created during vaccination campaign implementation by independent players (manufacturers, distributors, vaccination campaign managers, vaccinating clinics, public health agencies, citizens, certificate verifiers, agencies responsible for pharmacovigilance) into a reliable graph of knowledge based on undisputable attestations. VaccineGuard helps to know when, where and what took place and equip every citizen with a certificate to prove their Covid19 vaccination status anywhere in the world and also build from the same source data anonymous aggregated analytics for vaccination program managers.

KEY UNIQUE FEATURES OF VACCINEGUARD ARE:

+ Creation and privacy-preserving verification of globally reliable Covid19 certificates.
+ Monitoring of each individual vaccine flow throughout the supply chain to the individual person and location of vaccination.

The combination of these two on a single globally accessible secure and independently auditable digital platform gives VaccineGuard its functional value. Similarly, each feature is highly valuable if implemented separately or gradually while adjusting with existing workflows. If necessary, VaccineGuard can be implemented in a modular fashion.

An important aspect of VaccineGuard is the potential to combine paper-based and digital documents into a single issuance and verification process, enabling the interoperability of an implemented system worldwide, including in resource constrained settings.

VaccineGuard provides various deployment models to make it easy to start participating and to keep data safe while abiding to local compliance principles and regulations. Ranging from no infrastructure to on-premise deployments, VaccineGuard can provide customers with what they need to fit their technological, legal and organizational preferences.

What is VaccineGuard?

VaccineGuard is a digital platform that provides end to end attestation and verification of data and actions across the many systems involved in vaccination delivery. The overall goal of the product is to enable travel both within and across national borders and reduce restrictions to social interactions.

In order to successfully deploy the Covid vaccination program and equip citizens with trustworthy Certificates, authorities overseeing, and companies involved in the vaccine distribution and administration need trusted and real time situational information and assurance about:

1. The creation of each Vaccine Certificate for an identifiable person
2. The authenticity of vaccines being used
3. That Vaccine Certificates are being based on authentic vaccines
4. Progress to target vaccination goals
5. Possible Overuse of an authentic vaccines for counterfeit Certificates

VaccineGuard delivers these goals via a set of functional components to help different actors throughout the value chain as all of them benefit from the same distributed data management platform. These components empower each other significantly when working together, but each module is also valuable independently. The components are described further below.

Globally verifiable Certificate with reliable data

The first differentiator of VaccineGuard Certificate is that critical data accuracy is protected at the moment when the Certificate is created:

1. The provider of vaccination services as well as the issuer of Vaccination Certificate is an authorized healthcare or health data service provider. Such institutional authorization is provided by a government or other internationally recognized entity. VaccineGuard Certificates can only originate from an Issuer that belongs to a trusted list, which can be digitally verified (Trust Framework).
2. The vaccine used for immunization and creation of Vaccination Certificate is verified against an authentic vaccine data repository. This is done using the “digital twin” of each vaccine created together with the physical vaccine vial, which are defined via unique serial numbers (see below). VaccineGuard Certificates can only be issued with the reference to a unique authentic vaccine, which can be digitally verified.
3. Vaccine recipient is authenticated by the healthcare provider using existing photo-ID that is cryptographically linked to the Vaccination Certificate. Thus, VaccineGuard Certificate can only be issued with a reference to a unique individual, which can be digitally verified. If needed, also verification of a person against prioritization and eligibility database can be facilitated.

To summarize, each Vaccination Certificate creates a reliable link between a specific individual, an authentic vaccine dose and a trusted healthcare institution. No vaccine can be marked as used unless an authenticated unique individual is attached to it and no individual can be marked for being vaccinated unless an authentic unique

vaccine is attached to it. At the same time VaccineGuard is only complementing the trust guarantees that already exist, instead of building its own universe. This facilitates easier and more efficient adoption globally.

First, the "whitelist" of trusted healthcare providers that are authorized to perform vaccinations is expected to be licensed or accredited to do so by a public body or some internationally recognized organization. VaccineGuard extends access to its services for the digital certificate attestation only if authorized to do so by an above mentioned public or international body, who gives its guarantee that Vaccination Certificates can only originate from a trusted source. A dedicated digital "trust framework" facilitates this component.

Second, the data describing vaccination of an individual - personal details, administered vaccine, relevant contextual information - is captured by this trusted healthcare provider, who will guarantee that the data entry is accurate.

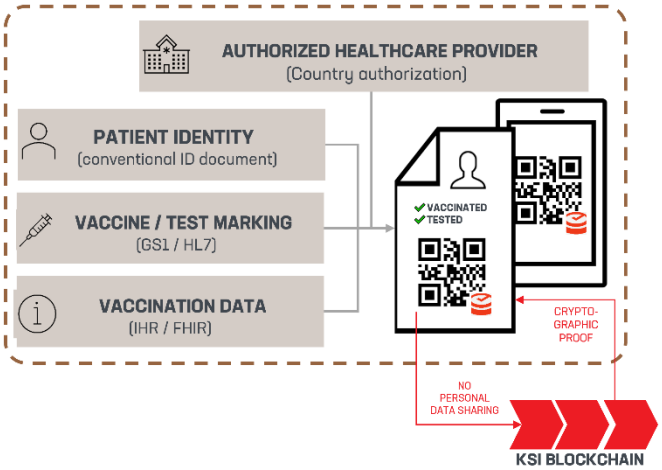


Figure 2. VaccineGuard adds immutable attestation to the Certificate

VACCINEGUARD PROVIDES IMMUTABILITY GUARANTEE to the Vaccination Certificate with the help of the eIDAS accredited KSI blockchain so that if a single data point in any of the certificates fails verification it is possible to trace back the information on the issuer or the vaccine that is causing disqualified verification.

This is possible even without keeping a centralized registry of all vaccinations and without processing personally identifiable information.

Such immutability guarantee assures reliability of both the data and process that was used to generate it for any later use of this information by Vaccination Certificates or supply chain monitoring.

Because the three components of the vaccination attestation are processed independently - and can be separated from the attestation document itself - they can be used for legitimate revocation of vaccination attestation. Examples include: if a vaccine batch appears to be ineffective or the medical facility loses its accreditation. This information can be made available for verification of the vaccination attestation without the need to maintain the list of individuals who received the invalidated vaccination.

Privacy-preserving Certificate verification

Global verification of VaccineGuard Certificates is possible in a maximum privacy-preserving way compliant with GDPR or other strict legal frameworks:

1. Once created the Vaccine Certificate is issued by healthcare provider as printout or sent via e-mail / mobile phone to the patient. Only the issuer and the patient have a copy of the Certificate – no central database is required for this. VaccineGuard will store only hashed verification data.
2. Only the patient is carrying and transporting the Certificate. All health and personally identifiable data are processed at her consent and no sharing is needed between the original issuer and the Verifier.
3. Verifier will receive personal information like photo-ID accompanying with the Certificate directly from the patient at her consent. Only proof of authenticity and hashed non-personal certificate data is verified against KSI blockchain and VaccineGuard.

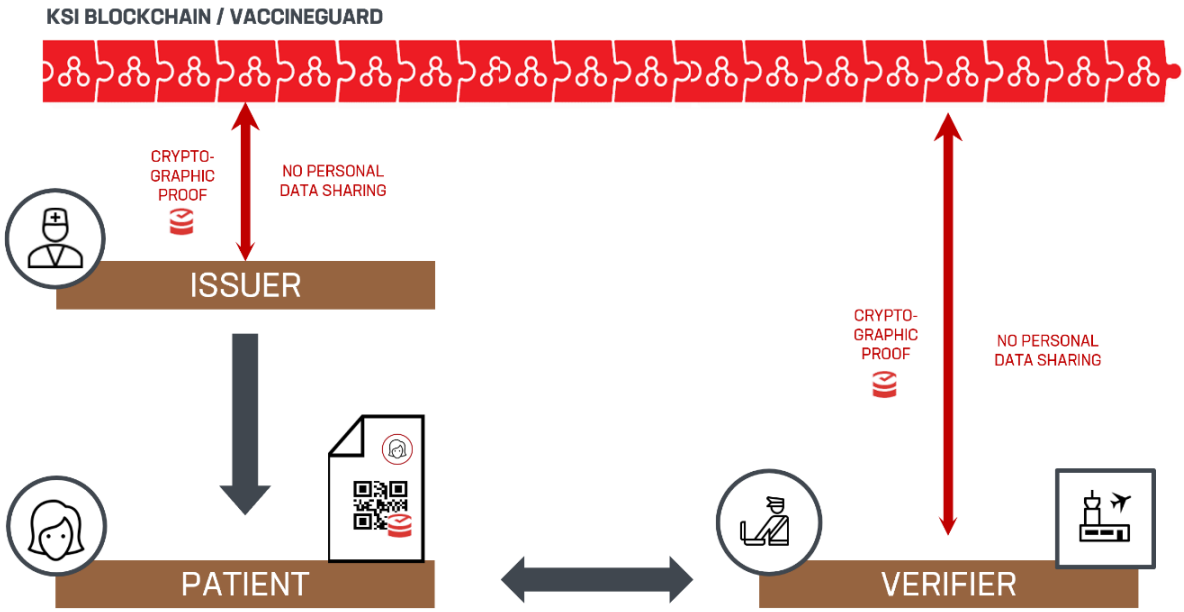


Figure 3. Workflow of the Certificate, demonstrating Patient's control of her personal and health data to protect privacy.

In such a way VaccineGuard's globally verifiable certificate solution facilitates personal control of health data, while providing assurance of the reliability of data on the Certificate and that it applies to the same person possessing the connected photo-ID.

End-to-end visibility of authentic vaccines supply chain

Creating a vaccination record and respective Vaccination Certificate by a trusted healthcare provider marks also the "magic moment" of linking a vaccine supply chain with that of a physical person. This enables VaccineGuard to anchor an immutable artefact of a unique vaccine used for concrete vaccination using its unique serial number.

Thus, vaccination record or Vaccination Certificate will contain valuable information about the last mile of the vaccine use - where, when and which specific vaccine was used.

VaccineGuard is flexible in terms of allowing the Certificate document to carry only the information that is deemed necessary and appropriate from privacy protection standpoint. Thus, it is possible to add cryptographic proof to the existing quite extensive data model suggested for the Yellow Card or keep only the patient's ID and cryptographic verification proof.

However, since the information about the last mile of the vaccine supply chain is cryptographically sealed for immutability, it is possible to aggregate the counts and other relevant information about individual vaccinations, without harvesting personal information (see below), with high accuracy and in near real-time.

Figure 4: Vaccination Certificate and the "last mile" data about a vaccine

VaccineGuard supply chain information management platform is an extremely flexible and powerful tool that enables end-to-end verifiable connections between all individual activities performed by various system participants, all following their autonomous but intertwined workflows.

VaccineGuard uses a "digital twin" of every individual vaccine. This can be created at the time when a vaccine is prepared for shipment out of manufacturing site or when it enters a country, for example by a Public Health Authority responsible for the vaccination Campaign.

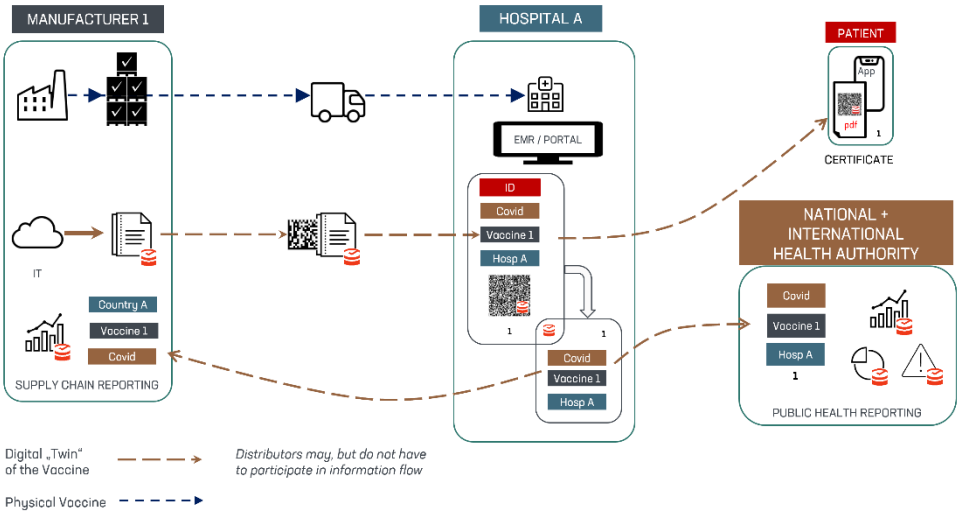


Figure 5. VaccineGuard links vaccination records and Certificates with end-to-end vaccination flow and anonymous reporting to public health authorities and manufacturers using the "digital twin" of every unique marking (GS1 serial number) of a vaccine.

VaccineGuard is accompanied with mobile application or web UI that enable fast capture of unique GS1 serial number from a package and verify it to "upstream" artefacts recorded by VaccineGuard about the origin and supply chain history of the given vaccine. The flexibility of the solution allows to connect just two end-points (for example the manufacturer's repository and the vaccination site without the need for any wholesaler to participate) and already enable real time awareness, while gradual onboarding of more participants in the supply-chain increases the value of the platform to all participating entities.

As vaccine count and allocation are captured by individual vaccinations, the counterfeit or diversion of vaccines is very easily discoverable. The ease of revoking attestations of vaccination that are administered improperly will discourage individuals from seeking them out, and medical suppliers from providing them. Furthermore, while a vaccination attestation contains personal information, such information is not necessary for the management of supply chain integrity. Any misbehavior within the supply chain, before the vaccination procedure, can be traced, after the fact, to those end recipients affected, since the individual vaccination certificates may be revoked. Individuals who are affected in this manner, will be aware, and can seek redress. This also allows anonymous monitoring of batch allocations. This mechanism provides sufficient means to control the supply chain and ensure transparency from all sides.

Real-time insights for vaccination program steering

The next layer of VaccineGuard's value proposition lies in the real-time reporting and aggregation information for decision makers while protecting patient privacy. This is provided via secure, distributed and privacy-preserving data exchange service between VaccineGuard network participants that is flexible for local, regional, national or supranational aggregation levels.
VaccineGuard facilitates data collaboration across various organizations operating in various geographical and legal contexts.

The unifying component for all participating entities is the single version of truth about data, its origin and genealogy, while rules and policies on how and what data can be shared are configurable according to the individual or collective agreements.

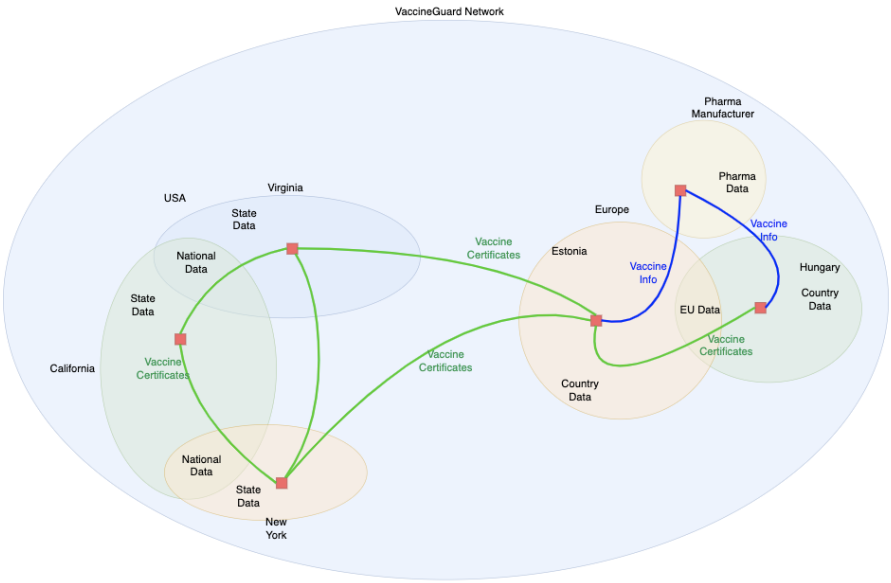


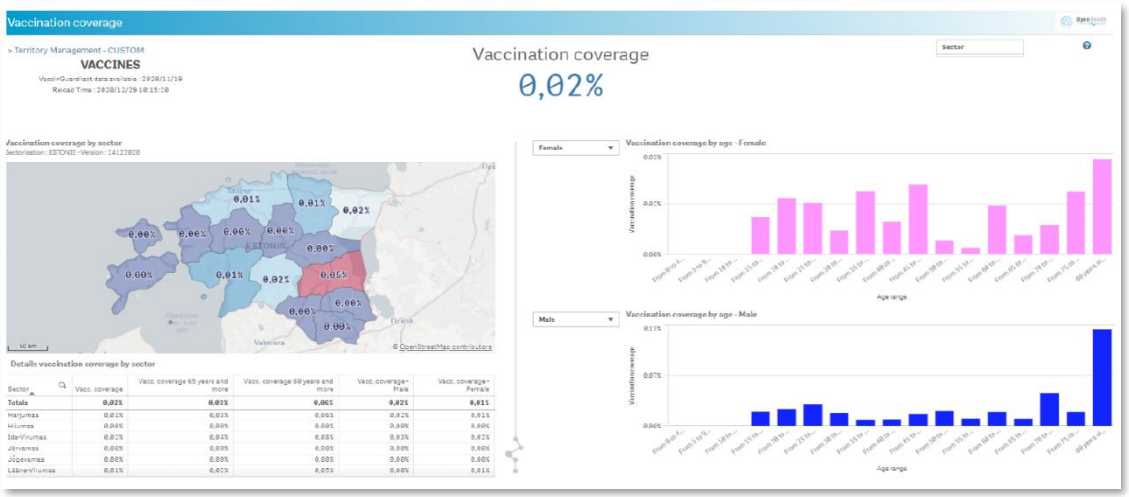
Figure 6. Example of VaccineGuard global ecosystem, that enables real-time flexible distributed collaboration, which is all based upon data sovereignty and cryptographically provable reliability of individual as well as aggregated information.

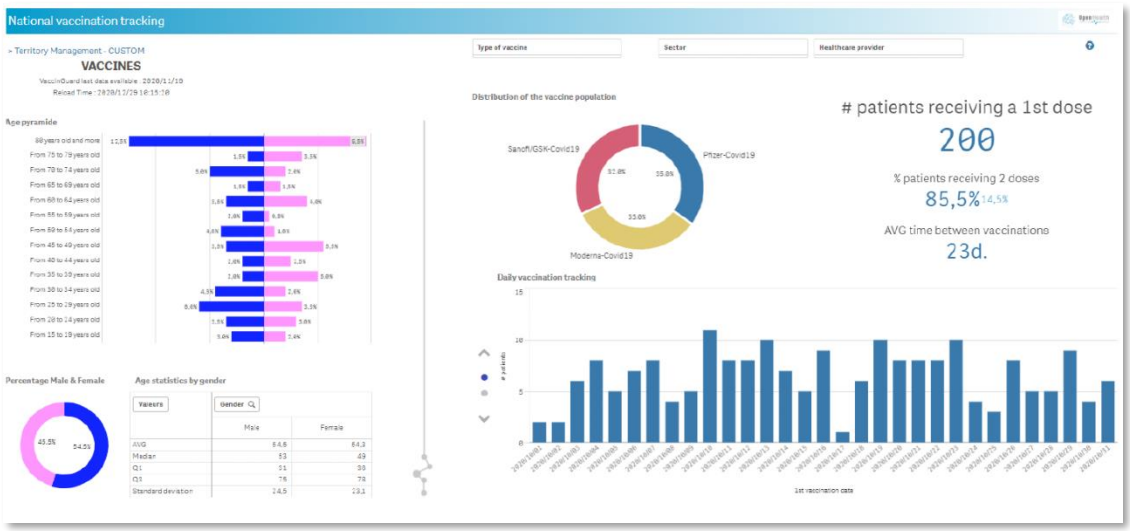
Steering of vaccination campaigns as well as coordination of supply and inventory management at different levels as well as between public and private entities in the network.

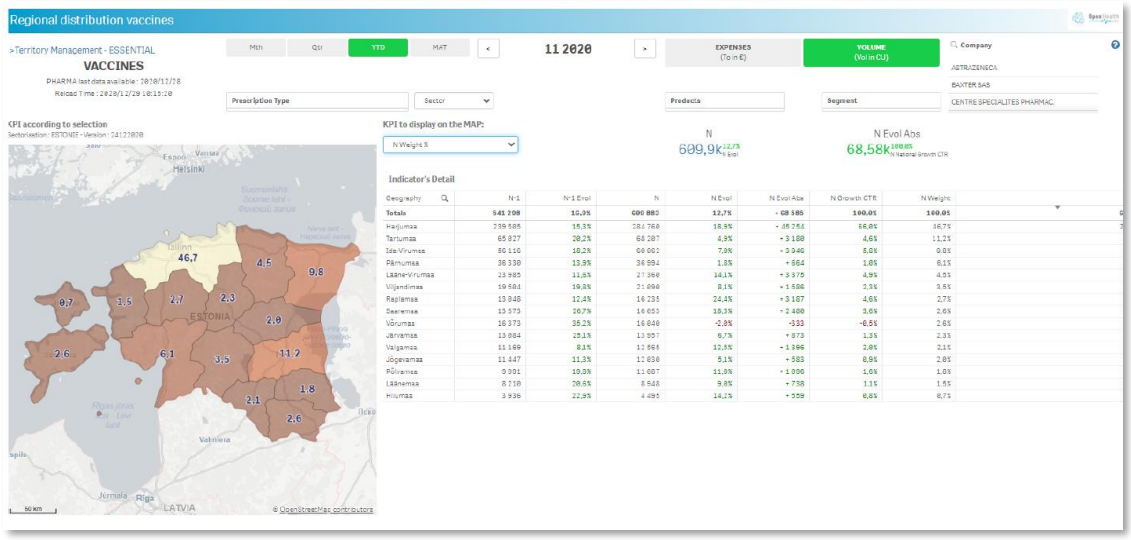
1. Vaccination campaign managers at different levels have access to a dashboard with real-time insights on vaccination targets based on automated aggregated reports from each vaccination provider.
2. Vaccine inventory overview and demand analytics are enabled via automated monitoring of stock and vaccinations for public health authorities as well as suppliers, if considered appropriate.
3. For Covid19 vaccinations campaigns eligibility management for public health prioritization is possible by linking respective category data with the individuals deemed for and willing to get vaccinated.

The demographic or reporting information can be adapted as needed, as the system provides a flexible data model approach. This data can be captured using manual or semi-autonomous methods and automatically exchanged with the necessary reporting entities. VaccineGuard provides the ability to cryptographically link each reporting data point to an authentic vaccination record or Certificate; in this case, it protects data privacy by including no identifying information.

In the end the goal of VaccineGuard is to replace the Covid19 incidence map with that of vaccination coverage map and up-to-date reliable intelligence on the situation.







Figures 7-9. VaccineGuard provides real-time insights on vaccination uptake for public health authorities, enabling a faster and reliable pandemic response. Automated aggregated reports provide insights to vaccination coverage, regional distribution of vaccines, and enable national vaccination tracking.

Pharmacovigilance and other post-vaccination monitoring

Lastly, the approach to securing Vaccination Certificates can be flexibly integrated with the workflows of vaccine adverse reaction monitoring (pharmacovigilance) to improve its efficiency and accuracy significantly.

Reports of adverse events associated with a vaccination can be first supported with the accurate association of the vaccination context (healthcare provider) and specific vaccine regardless of the place where the patient turns for medical help if the condition related to the vaccination develops.

Furthermore, VaccineGuard facilitates anonymously quick and automated aggregate reporting of such encounters across the continuum of relevant bodies without losing the precision about which vaccine they apply to. In the case of COVID-19 vaccination programs, this is of extreme importance, as the time for testing the new vaccines has been unprecedentedly brief.

VaccineGuard has the potential to strengthen the quality and efficiency of vaccine quality management in both high and low resource settings.

Key technical aspects

Following is an overview of the key technical aspects of VaccineGuard. For more in-depth information a technical documentation is available on demand.

General service design and architectural criteria

The solution is designed with the following general criteria and principles as suggested by the World Health Organization on Smart Vaccination Certificate to the respective working group:

+ INCLUSION BY DESIGN: it has to be possible to read Vaccination Certificate information manually. The Certificate Holder must be able to confirm with some level of assurance that he/she has had the vaccine, without a permanent connection to the internet and/or the availability of any servers outside the jurisdiction of the validating Certificate Issuer.
+ COMPLEMENTARITY BY DESIGN: it has to be possible to issue the Vaccination Certificate without the need for any additional installation of infrastructure or software by the Certificate Issuer (e.g., it is possible to instead use a Software-as-a-Service platform (SaaS)). However, it should also be easily integrated into the Certificate Issuer's computer systems (e.g., via API calls).
+ It must be possible to assume that the healthcare providers certified/authorized for the medical procedure of vaccination can also act as Trusted Certificate Issuers, to the extent that any Certificate Verifier may assume that both the medical procedure and Vaccination Certificate confirming it are true.
+ PRIVACY BY DESIGN: it has to be possible to verify the authenticity of the Vaccination Certificate with a simple smartphone or computer (via a Web application or a Mobile App) but without any need to access databases containing personal and/or medical information - or even through a trusted third-party (i.e., Vaccination Certificate data is presented "off-line"); any personal data processing must respect individual privacy and consent.
+ VALIDITY BY DESIGN: it must be possible to validate a Vaccination Certificate universally (across businesses, and national and geographic boundaries) and independently from the Certificate Holder, Issuer or Verifier, using trusted electronic and governance solutions.
+ TRUST BY DESIGN: it has to be possible to secure and audit the integrity of both the Vaccination Certificate data and its issuance process by a technology - not by human activity - to prevent any counterfeit or fraud of either digital or paper documents.
+ It must be possible to change Vaccination Validity Information post factum: nurses can turn out to be fraudulent, batches of the vaccine can turn out to be faulty or ineffective, or the immunization period can change, for example.
+ RESILIENCE BY DESIGN: it must be interoperable and adaptable with and between the existing technological solutions operated by any system, organization, country, culture or environment, without the need to build new IT infrastructure; it must be possible to govern issuance of the credentials locally without the need to rely on a globally centralized technological solution.

+ Identity management is not included in the scope of the current solution. We assume that a healthcare worker performing the vaccination has authenticated and verified the Certificate Holder . We also assume that the Subject will use the same identifying documents when presenting the proof of vaccination and when getting the vaccination.

Privacy management

Where is data stored and processed?

The data resides wherever the data owner chooses. It is related with the VaccineGuard preferred deployment model of VaccineGuard (see below). The data can be kept locally on a commercial computing device, such as a smartphone or laptop or a database within the Hospital network; or it can be hosted in a specific and acceptable cloud service provider. So, eventually the customer chooses, but resides within one of the specific regions where GDPR or other privacy regulation compliance is acceptable.

What follows is the description of a traditional model, where all personal and health data processing takes place within the existing IT infrastructure of a healthcare provider or by an authorized personal health data holder (for example an electronic medical record vendor or national health information system).

VaccineGuard solution manages three types of data or data objects.

Vaccination Records and **Vaccination Certificates**	These are created by authorized healthcare organizations to prove events of vaccination administration and full vaccination status. Vaccine Records stored by Health Organizations for record keeping and verifying vaccination progress while Vaccine Certificates are given to citizens. Vaccination Certificates do not contain personally identifiable information but do contain a mechanism to link the Vaccine Certificate to a valid Vaccine and an authenticated Citizen.
Vaccine Data	Vaccine Data provides proof of validity for the specific Vaccine and specific contextual information such as how many doses the specific serial number stands for or how many vaccine doses are required to reach adequate immunity. This includes possible counterfeits and the inventorying or rejection of Vaccine Chain of Custody.
Vaccination Reporting Data	Vaccine Reporting Data is anonymous information about a vaccination event that does not contain any reference to a physical person; only a cryptographic link to a unique event that prevents double counting. This is used in aggregated Vaccination Reports.

DATA CAN BE PROCESSED BY:

- Healthcare Organizations
- Public Health Authorities
- Citizens/patients
- Verifiers

HEALTHCARE ORGANIZATIONS that are authorized (see above) to have a VaccineGuard account can use the software to certify Vaccination Records and generate Vaccination Certificates. The data is created on the machine, which is controlled and managed by the Organization (for example within a single physical network), and it is also stored within the Health Organization's digital infrastructure. It is also important that the data of the Vaccine Certificate does not ever need to be stored centrally, nor is it kept in the blockchain. The Certificate can be sent directly to the patient by the Healthcare Organization or exchanged with national authorized entities, if relevant - this data processing takes place outside the VaccineGuard.

PUBLIC HEALTH AUTHORITIES may receive via VaccineGuard the Vaccination Reporting Data according to the predefined rules. Aggregation can be facilitated at different levels from a hospital to regional or national authorities to supranational entities. While the Reporting Data is based on a unique count of a vaccination event, it does not contain any personally identifiable data and is also used in an aggregated form.

CITIZENS/PATIENTS can have sent by the Healthcare Organization a copy of their Vaccination Certificate, which is linked to their photo-ID or personal ID-number that was used for authentication by the Healthcare Organization. It must be emphasized that the Vaccine Certificate doesn't contain any PII, but only a cryptographic guarantee for its integrity (data has not been tampered) and validity (data belongs to a specific individual). This allows for confident and confidential exchange of the Vaccine Certificates to enable on-demand verification.

VaccineGuard protects Data Privacy by following industry standards for protecting PII. Vaccine Certificates and Records require the ability to be uniquely tied to an individual. To provide the utmost Data Privacy while still achieving this goal, VaccineGuard uses salted hashes associated with the citizens unique, government issued, identity credential. This can be in the form of a Government Issued Passport number, national ID card or personal ID-number. An illustration showing the relationship is below.

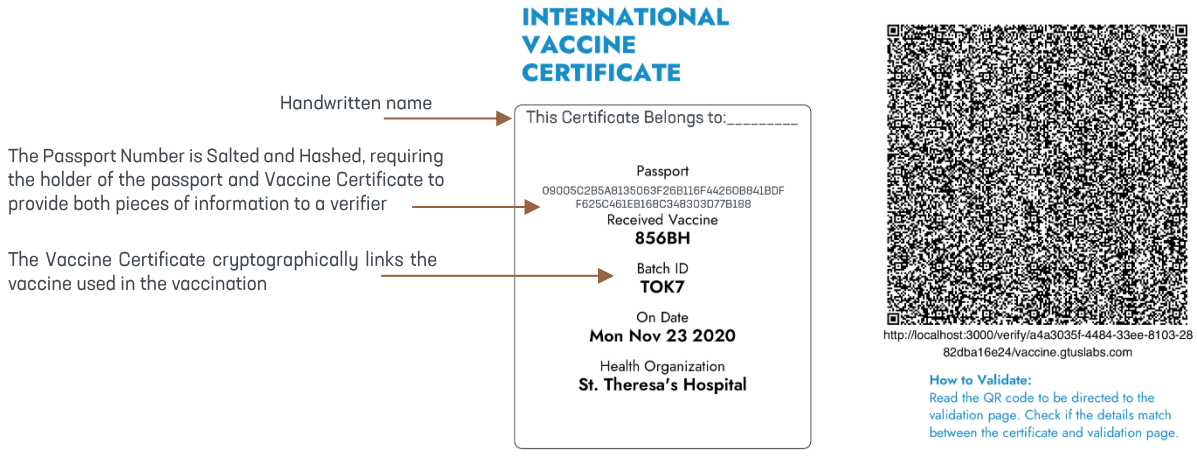


Figure 10. Privacy preserving features of the Vaccination Certificate (document)

How is the verification facilitated?

Eventually the Citizen/patient will want to prove vaccination to a Verifying Entity. To do this, only the barcode on the digital PDF or the physical PDF is required. One does not need access to any personal information or a centralized database, and, in particular, there is no need to access the Certificate Issuer's original records at the Healthcare Organization, where the original data in the Certificate might be held.

Once the citizen presents the certificate to the Verifying Entity, the Verifying Entity scans the QRCode(s) associated with the Vaccine Certificate and reassembles the Digital Twin associated with the Vaccine Certificate. This will provide the data, signature, and 'salt'. The Verifying Entity then enters the passport number from the Government Issued Passport belonging to the Citizen. All must match in order for the Vaccine Certificate Verification to be successful.

Here, the Verifying Entity will validate the cryptographic evidence locally on the Verifying Entity Device. The Verifying Entity will validate the authenticity of the Certificate using the KSI Signature. This process does not require data exchange with IT systems or key exchanges across organizations. The verification takes milliseconds, and the Verifying Entity can do it independently of any server assisted responses. The KSI Signature is validated using the KSI Blockchain where Verifying Entities can retrieve the distributed blockchain proving authenticity of the Signature and in turn the Vaccine Certificate. This does not require exchange of data, but instead cryptographic blocks, or hashes.

Getting Started with VaccineGuard

The VaccineGuard Network provides organizations with a Network of interconnected participants to create a secure and trusted vaccination value chain.

The VaccineGuard Network connects Vaccination Value Chain Participants. These include Vaccine Manufacturers, State and National Governments, and Health Organizations, testing and working together to strengthen the Vaccination Value Chain. Once on-boarded, you can exchange data in real time with other participants.

What do I Need?

VaccineGuard aims to be inclusive and provides different avenues to participate depending on customer needs. These different avenues allow customers to choose the right fit for them when looking at data storage requirements, GDPR, IT Staffing Budget and functionality needed. These are explained in more detail below.

1. No-Premise Deployment

WHY USE THIS?

This is primarily used for customers or individual contributors who want to:

1. participate without the ability to install other VaccineGuard components
2. do not have any IT infrastructure
3. perform basic tasks along the value chain

WHAT IS REQUIRED?

A mobile device or personal computer with the ability to install an application.

WHAT DO I GET?

Customers choosing this option will be provided a secure download link once on-boarded. This will provide an installation file they can use to install the VaccineGuard app.

2. On-Premise Deployment

WHY USE THIS?

This is primarily used for customers who require more robust data storage, data exchange, and workflows and want to:

1. store any data locally within their walls
2. only send data outside of their walls to exchange data explicitly with the network
3. have basic IT infrastructure to install the components.

WHAT IS REQUIRED?

Any Linux of Windows Server that can run software installations and basic networking.

WHAT DO I GET?

Customers choosing this option will be provided a secure download link once on-boarded. This will provide an installation file they can use to install the VaccineGuard components.

3. Subscription

WHY USE THIS?

This is primarily used for customers who require more robust data storage, data exchange, and workflows and want to:

1. leverage the VaccineGuard features in a Software as a Service model
2. eliminate the need for installation and infrastructure on their premises.

WHAT IS REQUIRED?

Users will receive access to the VaccineGuard portal upon completion of the signup process. Users can access this through a web browser and mobile app.

Pilot Engagement

The VaccineGuard Pilot Network provides organizations with a Network for Proof of Concepts and Pilots. This network mimics the production VaccineGuard Network, but does not include sensitive data, real names of organizations and production SLAs.

WHY PARTICIPATE IN THE PILOT NETWORK?

The VaccineGuard Pilot Network connects actual Vaccine Value Chain Participants for trials, Proof of Concepts, and tests. These include real Vaccine Manufacturers, State and National Governments, and Health Organizations, testing and working together to strengthen the production VaccineGuard MobileFirst Network. Once on-boarded, you can exchange data with actual participants.

HOW TO GET ACCESS?

Enrollment is as simple as providing a desired organization name, emails, and the type or types of Roles requested.

WHAT WILL YOU EXPECT?

Once processed, the requester of the Pilot Network email will receive the information for your new VaccineGuard instances. This will include a dedicated instance for your organization for each the various Entity Types requested.

Logins and URLS will be provided as well as a welcome document and how to start participating in the video.

Once logged in, participants can begin right away, with pre-populated data and a live Network with constant data exchange.

Participation with other organizations is easy, as data can be exchanged with each organization and the list of participants constantly updated as new organizations join.

WHAT DO I NEED?

A web browser - The VaccineGuard Pilot Network allows organizations to start participating as quickly as possible with no setup time or infrastructure to create. For more involved trials, such as on-premise installations, VaccineGuard can be set up to support this as well.

HOW LONG DO I GET ACCESS?

The standard Pilot lasts 30 days. This provides enough time for participants to feel comfortable with the platform and provide feedback for the production version.

WHAT DO I DO AFTER THE PILOT?

After the Pilot, transitioning to the production version is simple and straightforward. The participants will be on-boarded in a very similar way and gain access to the production network.