guardtime

GUARDTIME /VACCINEGUARD

VERIFY COVID-19 STATUS OF INDIVIDUALS.
MAINTAIN ACCURATE OVERVIEW OF
VACCINATION PROGRAM EFFECTIVENESS.

OCTOBER 2020

5.1.2e e | Chief Medical Officer
5.1.2e @guardtime.com

DIGITAL COLLABORATION
/ BETWEEN ESTONIA AND THE WORLD HEALTH ORGANISATION

- In October 2020, Estonian Prime Minister Jüri Ratas and WHO Director-General Dr Tedros Adhanom Ghebreyesus signed a **Memorandum of Understanding to share the experience of Estonia** and its companies in healthcare digitization using distributed information architecture and interoperability with WHO and its member states.
- The first pilot will be a **digitally verifiable international vaccination certificate („Smart Vaccination Certificate")**, which could potentially support the effective implementation of the Covid-19 vaccination program.
- **The technical leader of the project is Guardtime**, an Estonian-born cybersecurity company leveraging the EU eIDAS-accredited trust service KSI-blockchain in its solution for tamper-proof digital certificates. The collaboration also involves Nordic Institute for Interoperability Solutions (NIIS), SICPA and potential other partners.

FUNCTIONAL GOALS
/ OF THE PILOT IMPLEMENTATION

guardtime

Provide proof of Covid19 tests & vaccination (certification)

Provide independent verification of the certificates

Monitor vaccine uptake among target population

Collect insights about supply chain integrity and pharmacovigilance

KEY ASSUMPTIONS FOR A COVID-19 /TESTING & VACCINATION CERTIFICATE SOLUTION

guardtime

- **No need to create a new database** to keep or exchange individual health information;
- **No need to build new IT infrastructure** locally or centrally (compatible with existing systems and workflows)
- Works with **paper and modern digital applications**, regardless of the country's level of digital development;
- Provides **a minimum universal security principles** that can be adjusted to the needs of countries worldwide;
- Is implementable **immediately,** globally.

PRAGMATIC APPROACH TO
/ SMART VACCINATION CERTIFICATE

EXISTING OFFLINE STANDARDS FOR PATIENT IDENTTY

EXISTING UNIQUE VACCINE MARKING STANDARDS (GS1)

INTRODUCING GLOBAL LIST OF **AUTHORISED ISSUERS** (HEALTHCARE PROVIDERS)

EXISTING VACCINATION DATA STANDARD (IHR / FHIR)

Cryptographic seal for verification

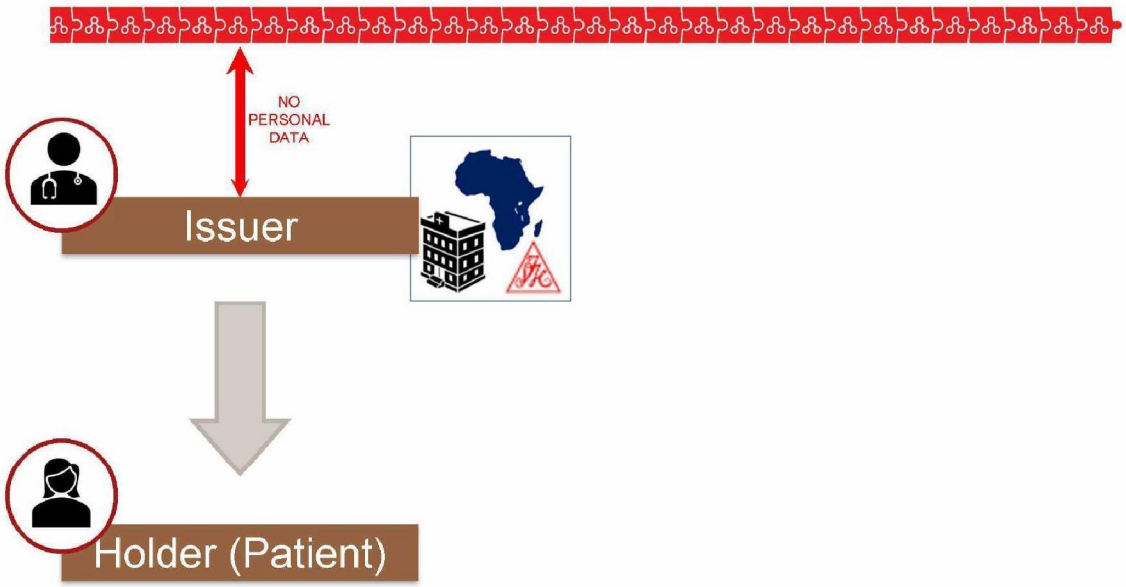
Secured by KSI blockchain

NO PERSONAL DATA

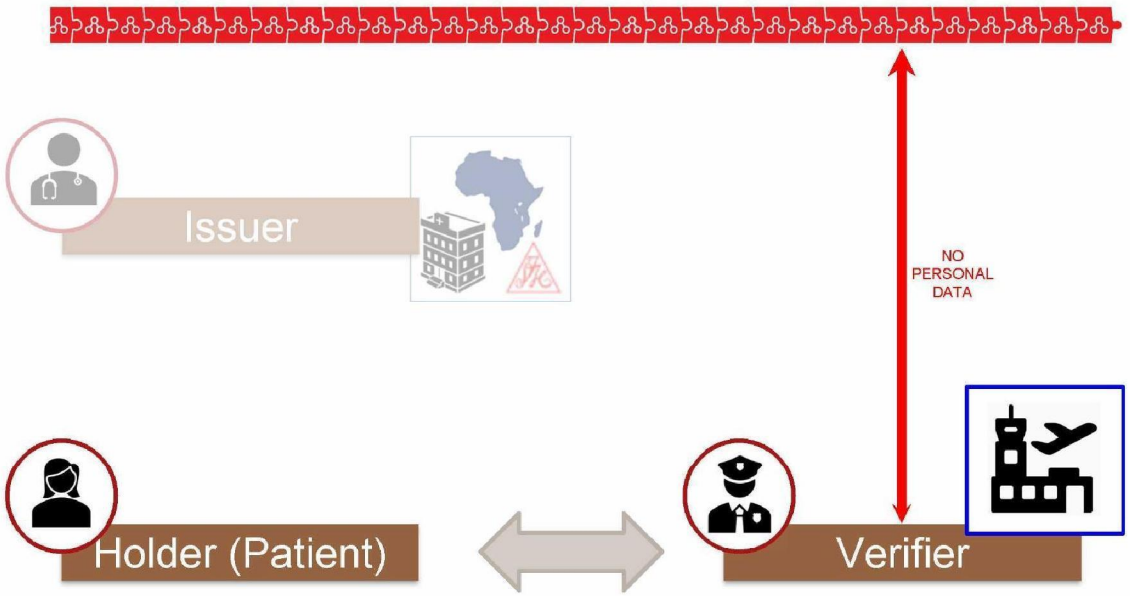
Process integrity is guaranteed

guardtime

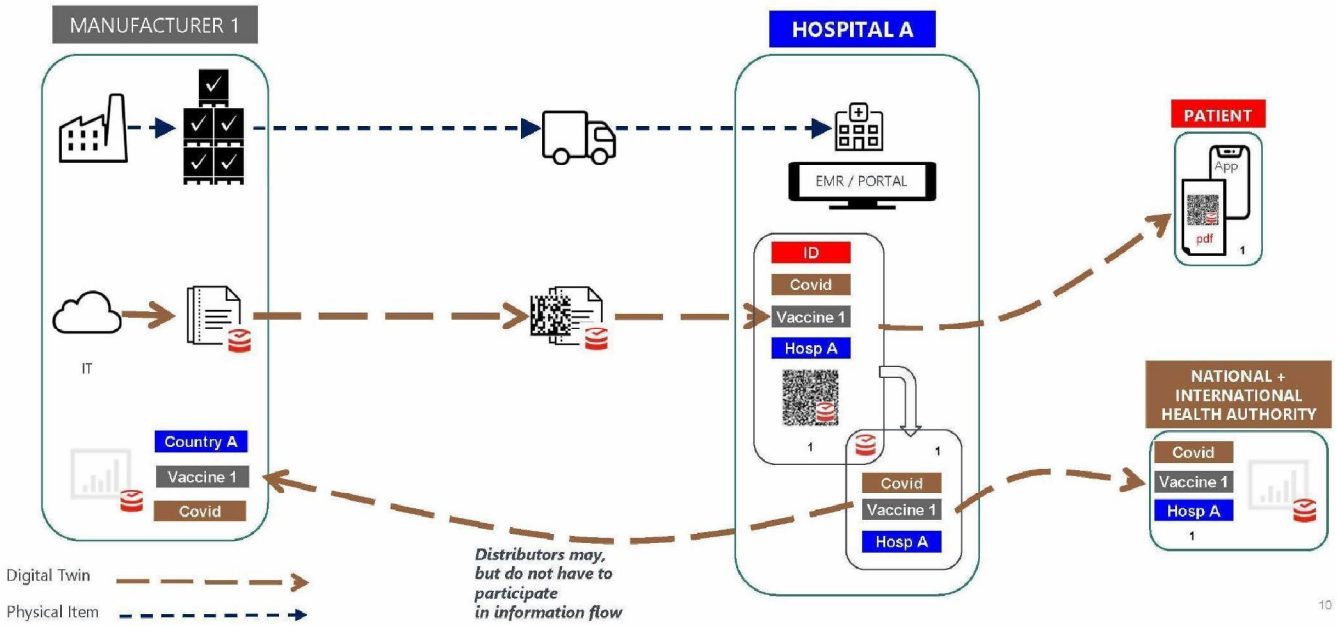
SMART VACCINATION CERTIFICATE SERVICE USES / PERSONAL CONTROL OF MY HEALTH DATA



SMART VACCINATION CERTIFICATE SERVICE USES / PERSONAL CONTROL OF MY HEALTH DATA



VACCINEGUARD BY GUARDTIME
/LINKING CERTIFICATE WITH VACCINATION SUPPLY CHAIN



TECHNOLOGY & STANDARDS

guardtime.com

guardtime

SECURITY STANDARDS AND PRINCIPLES OF / SMART VACCINATION CERTIFICATE SOLUTION

- ✓ **eIDAS accredited trust service - KSI blockchain** (private permissioned blockchain)
  - ✓ Data + process integrity
  - ✓ Lifetime universal verification process
  - ✓ No need for a holder to manage cryptographic keys
- ✓ **X-road based permissioned system for Issuers**, with a decentralized accreditation management (built-in chain of trust) with open-source protocols for:
  - ✓ Message & service metadata (SOAP / REST)
  - ✓ Environmental & operational monitoring
  - ✓ Management services
  - ✓ Online Certificate Status – OCSP (RFC 6960)
  - ✓ Time-Stamp Protocol – TSP (RFC 3161)

PRIVACY STANDARDS AND PRINCIPLES OF / SMART VACCINATION CERTIFICATE SOLUTION

- ✓ **GDPR / HIPAA compliant**
  - ✓ The certificate is fully in the control of the Holder
  - ✓ Nobody else than the Holder can disclose a Certificate (consent by design)
  - ✓ No database with PII needed for verification
  - ✓ Fully inclusive (including paper copies, as no electronic device are mandatorily needed)
  - ✓ Fully decentralized architecture
  - ✓ Fully sovereignty and independence of States about issuance & verification

AUTHENTICATION AND MEANS OF IDENTIFICATION FOR / SMART VACCINATION CERTIFICATE SOLUTION

- ✓ Existing off-line standard documents for identification
- ✓ Initial authentication performed by authorised healthcare provider (as part of vaccination service)
- ✓ Unforgeable link between the Certificate and an official ID (KSI signatuure)
- ✓ Possibility to include a Photo (as a Photo ID) and/or the biometry

DATA FORMATS AND PRINCIPLES FOR / SMART VACCINATION CERTIFICATE SOLUTION

- ✓ Compatible with any data standard and terminology formats
- ✓ Pilot is focusing on combination of IHR and FHIR (subset)
- ✓ GS1 standard for vaccine marking (Batch/lot, serial number, expiration date)

INTERFACE STANDARDS AND PRINCIPLES FOR / SMART VACCINATION CERTIFICATE SOLUTION

- ✓ Very low requirements in terms of standards
- ✓ Can be coupled with any IT system, through a set of open API's
- ✓ No need to have compatible systems installed on both sides (of Holders & Verifiers)
- ✓ No need for an App for a Certificate Holder or Verifier
- ✓ No need for a Holder to manage Apps and Private Keys
- ✓ No need to have any electronic device, using a Paper version, without compromise on security, privacy, integrity and verifiability
- ✓ Built-in possibility to have an off-line verification

SCALABILITY AND READINESS OF / SMART VACCINATION CERTIFICATE SOLUTION

- ✓ Solution is in operation at industrial scale
- ✓ Immediately scalable to billions of certificates
- ✓ The KSI Blockchain allows to secure 10^{12} transactions per second

PILOTING

guardtime.com

guardtime

MAIN FEATURES /OF THE CONCEPT

1. Vaccination is entrusted to **specific healthcare facilities** that have been authorized to vaccinate in each country.
2. Healthcare providers that have received such a right shall be **registered by the relevant state authority** and given permission to issue digital certification credentials.
3. To ensure privacy, vaccination information with personal **data is stored only in a health care institution** and the patient is issued a vaccination certificate.
4. The only information **stored centrally is an independent digital authenticity certificate** - this ensures that the vaccination attestations issued by each healthcare institution cannot be falsified or subsequently altered.
5. The certification confirmation - **QR code - can be verified from paper, as well as from pdf or mobile app** versions of the vaccination attestation. Thus, the transfer/sharing of personal data takes place only by the person himself and under his control, no central health database is required for the purpose of verification.
6. For other countries, in addition to checking the attestation and verifying the certificate, only information about the respective country authority that issues the accreditation for vaccination is needed; in case of doubt, it is possible to make a further inquiry to the competent authority as to whether a particular healthcare provider is authorized to vaccinate.

How to become a user?

Through a collaboration with the Government of Estonia we are actively engaging with all countries that are interested in becoming users of the solution to facilitate faster and more efficient response to Covid-19 risk mitigation through smart travel restriction management.

CONTACT Solution Manager:

5.1.2e

Chief Medical Officer | Guardtime

5.1.2e @guardtime.com

+372 50 63619

How to become a user?

The solution is currently ready for immediate deployment.

To launch a successful Covid-19 Certificate issuing and verification service, it may be desireable for healthcare providers to integrate issuance into an Certificate Issuer's existing business processes, and for National Entities to accommodate the Certificate verification procedures by the appropriate National agencies (boarder guards, etc).

Given the multiple stakeholder nature of the solution, we recommend deployment in four phases to achieve overall acceptance.

Phase 1: Demonstrator / Proof Of Concept

Phase 2: First Pilot

Phase 3: Multi-sites Pilot

Phase 4: Nationwide Deployment

How to become a user?

Phase 1: Demonstrator / Proof Of Concept
Set-up and run a Demonstrator (or Proof of Concept - PoC) to show to the different actors and decision makers that the solution works, to test social acceptance and to gain full support.
2 - 4 weeks

Phase 2: First Pilot
Set-up and run a first Pilot in one health care provider (Certificate Issuer) and one Authorised Verifier carrying out routine vaccinations to confirm the validity of the solution: that it is well integrated into the business processes to be scaled.
8 – 10 weeks

Phase 3: Multi-sites Pilot
Extend the Phase 2 Pilot to multiple sites and multiple use cases. Phase 3 should also include a communication and information campaign from the National Entities.
8 - 12 weeks

Phase 4: Nationwide Deployment
Extension to the general population (incl setting-up and adapting the National Entities' IT systems to manage such information, as well as setting-up relevant processes in participating administrations).
2+ months

THE COMPANY

guardtime.com

guardtime

The leading trust technology company

COMPANY SUMMARY

FOUNDED: 2007 in Tallinn, Estonia

GLOBAL HQ: Lausanne, Switzerland

FOUNDER AND CEO: 5.1.2e

PERSONNEL: 150 FTE, offices in US, EU and Asia

PRODUCT: Full stack infrastructure for building zero-trust systems and software applications. EU-EIDAS, NSA NIAP, 公安部 (China) accreditation

INTELLECTUAL PROPERTY: 50+ issued patents for zero trust systems

2019 REVENUE: US GAAP 36M USD

REFERENCE CLIENTS & PARTNERS:

Republic of Estonia Government · verizon · MÆRSK · Bank for International Settlements · Roche · esa · Lockheed Martin

GUARDTIME HEALTH

LEADERSHIP TEAM: leaders in trust technology, well resourced team with backgrounds in corporate development and management.
5.1.2e, MD MPH, Chief Medical Officer

TECHNOLOGY: recognized technology leaders with a proprietary trust computing stack (patent protected)

APPLICATIONS: core technology is 'horizontal' in nature, can be applied to large number of solutions and products, ensuring the total addressable markets are significant

PRODUCTS:

- Real World Data Engine for Market Access
- VaccineGuard
- Drug Shortage Manager
- Data Access and Governance Manager

ACCREDITATION: technology has been accredited by US, EU and China regulators for deployment on to government networks

CONTACTS

guardtime

5.1.2e

5.1.2e 5.1.2e

REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

5.1.2e

5.1.2e