947606

INTERNATIONAL DIGITALLY VERIFIABLE COVID-19 CERTIFICATES
/FOR TEST-RESULTS & VACCINATIONS

BRIEF V1
OCTOBER 2020

Note: Information in this document is preliminary and subject to change without prior notice.

BACKGROUND

The Covid-19 pandemic has revealed an urgent need for a global and cross-sector response to mitigate the spread of communicable diseases with severe global impact.

While the restrictions on social interaction and travel have been accepted so far, as the main and most effective implemented measures to protect public health, these have caused tremendous social and economic harm.

Increasingly accepted practice is facilitate modified movement restrictions with reliable information about negative Covid-19 test result or in the future a valid vaccination against the virus.

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.

Thus, a reliable verification of being effectively Covid-negative or immunized has also become clearly relevant.

Guardtime (Estonia) together with its partner SICPA (Switzerland) have build and deployed a system that can make **digitally verifiable Covid-19 test results or vaccination certificates.**
Such certificates are respecting the **ethical rules and the protection of privacy**, without creating new unforeseen cases of fraud, misuse or discrimination

Guardtime/SICPA system **stands out from the others** by meeting all the required criteria of a workable solution to address the current Covid-19 epidemics:

- ✓ No need to create a new database to keep individual health information;
- ✓ Suits with the varying needs of countries worldwide with uniform security;
- ✓ Works both with paper and modern digital certificates, regardless of the country's level of digital development;
- ✓ Is easily compatible with existing various IT systems;
- ✓ Is implementable within 3-6 months globally.

The solution has been agreed to be piloted for support of effective implementation of the Covid-19 vaccination program (COVAX).

For this, Guardtime has partnered with the Estonian Government and WHO to pilot a **digitally verifiable international vaccination certificate** ("Smart Yellow Card").

DIGITALLY VERIFIABLE CERTIFICATE

Covid-19 certificate should provide assurance that the individual has given a negative Covid-19 test with accepted method or has been vaccinated (should the vaccine become available).

To do this, there must be a reliable link between:

- ✓ **The identity of the Patient** (or the link to his/her National ID)
- ✓ **The result of a reliable Covid-19 test** (e.g. PCR from swab/saliva, Anti-body, ...) or **Vaccine** (Manufacturer + Lot No)
- ✓ **The signature of the Issuing Authority** (accredited healthcare institution) where the test or vaccination was performed

These three information artefacts are secured by the KSI Blockchain[1], which makes it unforgeable and universally verifiable, by anyone with a smartphone or a computer.

The issuing process is also secured with a Process Integrity solution, secured itself on the KSI Blockchain.

Important the trust anchor is the Issuing Authority which can be managed by public entity via pre-authorisation (combined with the accreditation to perform relevant medical procedure according to applicable law)

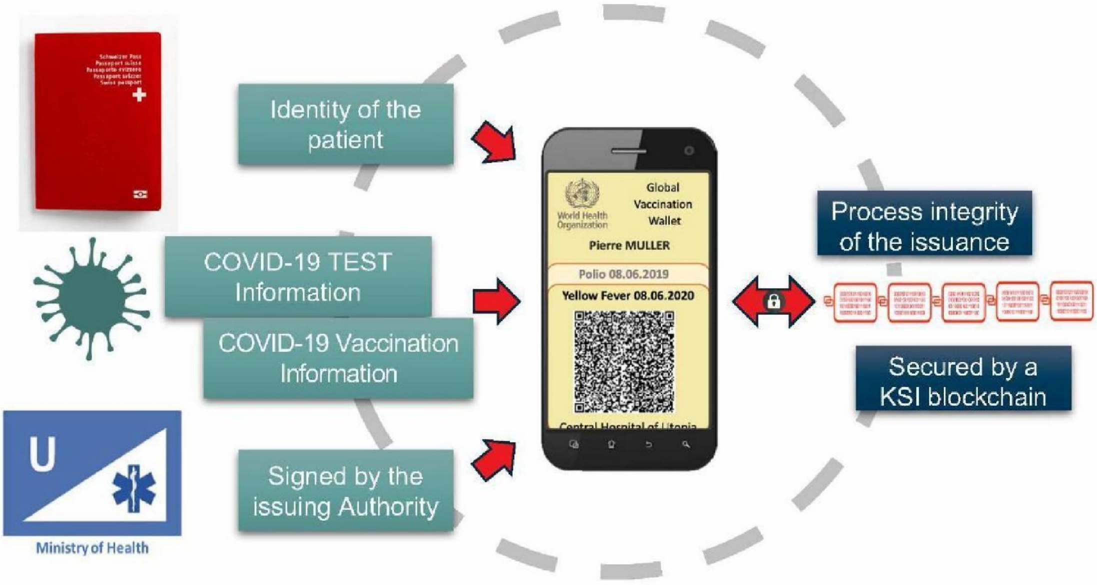

Identity of the patient
COVID-19 TEST Information
COVID-19 Vaccination Information
Signed by the issuing Authority
World Health Organization
Global Vaccination Wallet
Pierre MULLER
Polio 08.06.2019
Yellow Fever 08.06.2020
Central Hospital of Litonia
Process integrity of the issuance
Secured by a KSI blockchain
Ministry of Health

Figure 1: Covid Certificate concept

[1] – *KSI is a blockchain technology designed in Estonia and used globally to make sure networks, systems and data are free of compromise, all while retaining 100% data privacy.* https://e-estonia.com/solutions/security-and-safety/ksi-blockchain

GLOBAL SOLUTION OVERVIEW

The proposed solution (*Figure 2*) addresses the issuance and management of new **COVID-19 Certificates** to serve as the basis for near real-time trusted awareness of one's a Covid-19 status.

Testing or vaccination is entrusted to specific **healthcare facilities** that have been authorized to to perform such clinical operations in each country. Such providers shall be registered with the relevant state Certificate Issuer and given permission to issue digital certification credentials.

To ensure privacy, health information with personal data is stored only in a health care institution and on the certificate issued to **the patient (Certificate Holder)**.

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.

Only the Certificate Holder has the option to show the Vaccination Certificate on paper or on a mobile screen to an Authorised Verifier (thus **consenting to be verified**). The Certificate can be checked via its QR Code (containing the cryptographic seal), which can be scanned with either a smartphone or a computer camera.

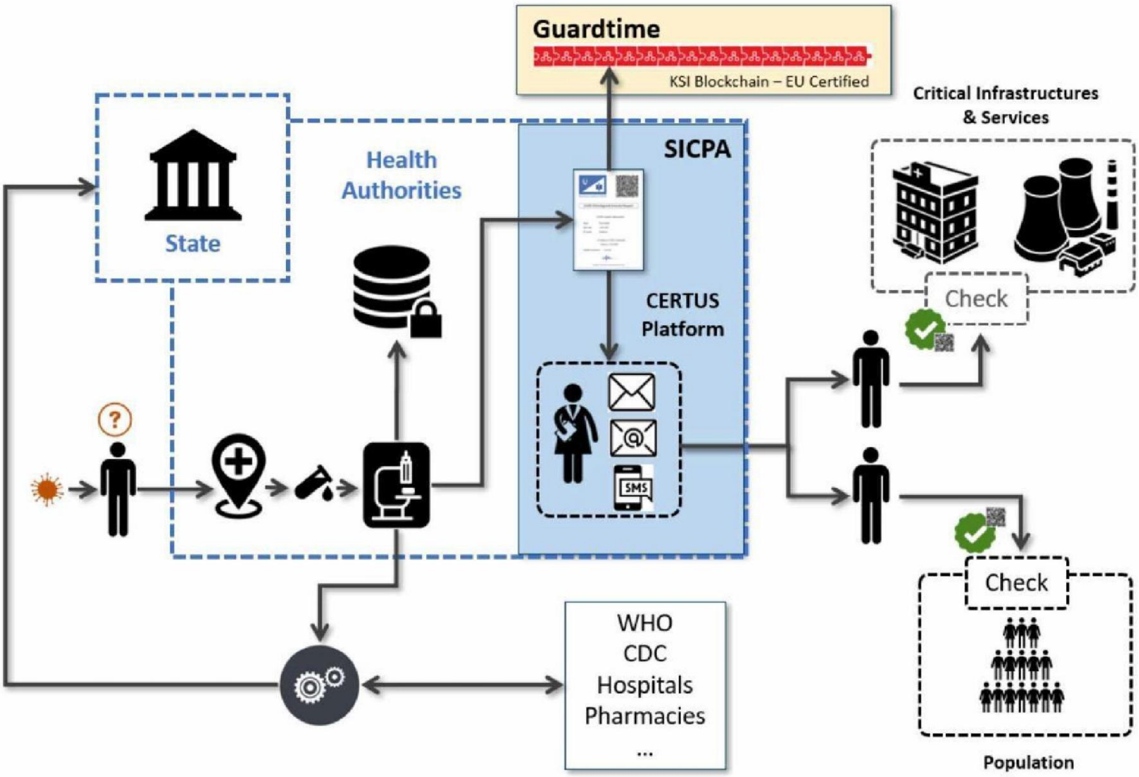


Figure 2: The solution as part of simplified Covid-19 testing/vaccination and verification workflows

CERTIFICATE ADVANTAGES

The proposed COVID-19 Certificate has the following advantages:

- ✓ Impossible to counterfeit (to avoid false certification);
- ✓ Can only be issued by an Authority;
- ✓ Can be a paper document or in Digital form (PDF file, mobile wallet file etc) – all with the similar security and immutability guarantee;
- ✓ Universally verifiable with a simple smartphone or computer (via a Web application or a Mobile App), including off-line;
- ✓ Compliant with GDPR: no personal information – PII – is ever disclosed from any database; no need to access a database for the verification process;
- ✓ No need for any additional installation of infrastructure or software by the Authority to issue the Covid-19 Certificates;
- ✓ Easy to deploy and use, without the need for a central system (nor a central database) for the issuance – can be issued by each Authority, independently from the others;
- ✓ Can be easily integrated into the Authority's computer systems, via API calls;
- ✓ No need to have a specific means to manage the identity and authentication of the beneficiaries (because the certificate is linked to a person through his/her identity card, social insurance card, passport or any other official identification document).

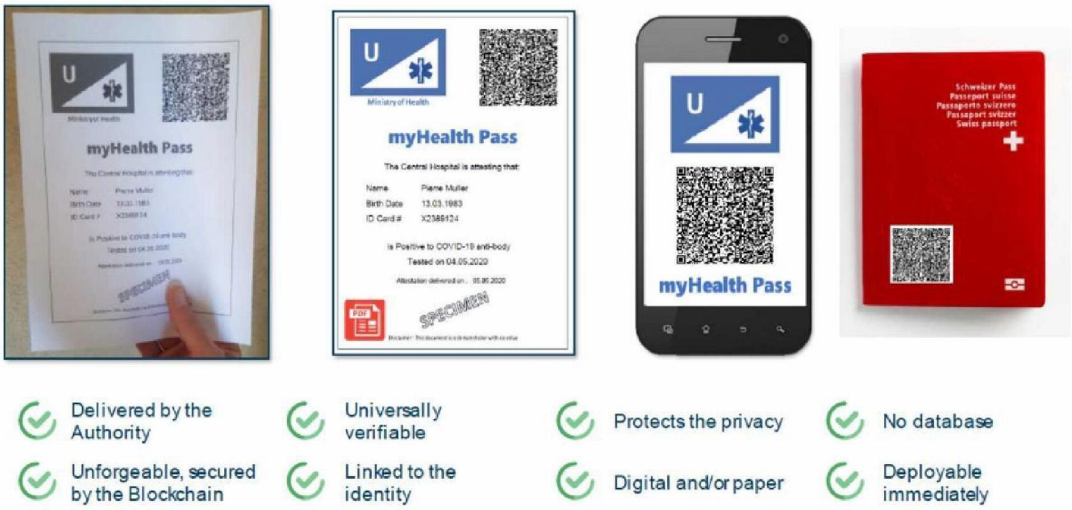
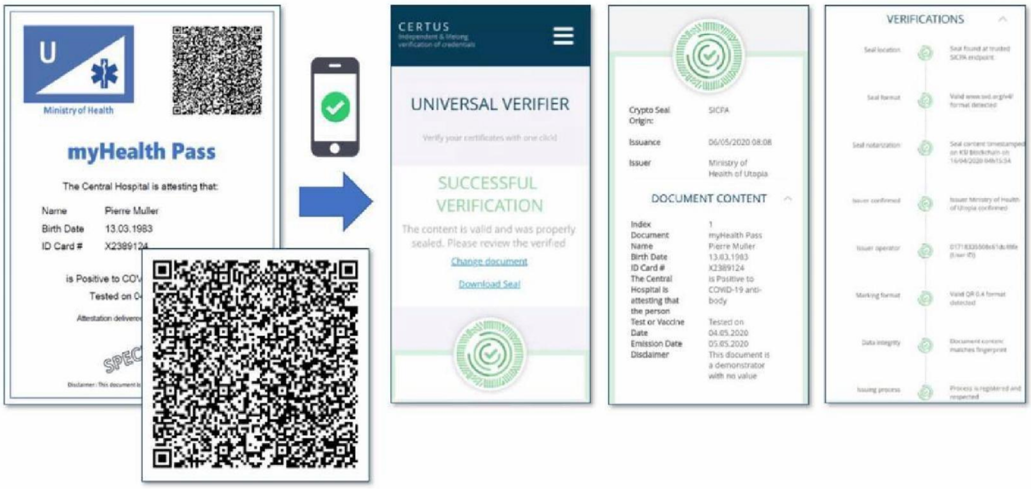


Figure 3: Main features of the solution & the Certificates in their various forms

VERIFICATION

When a holder shows the COVID Pass to an authorised verifier (thus consenting to be verified), the Pass can be checked via its QR Code. This secured QR code can be scanned with either a smartphone - see *Figure 4* - or a computer - see *Figure 5*.

The Certificate Issuer and the Verifier are not required to have any relationship with each other – no data exchange is needed apart from what the individual consents to demonstrate from the Certificate..



U

Ministry of Health

myHealth Pass

The Central Hospital is attesting that:

Name	Pierre Muller
Birth Date	13.03.1983
ID Card #	X2389124

is Positive to COV

Tested on 0

Attestation delivere

SPEC

Disclaimer: This document is

CERTUS
Independent & lifelong verification of credentials

UNIVERSAL VERIFIER

Verify your certificates with one click!

SUCCESSFUL VERIFICATION

The content is valid and was properly sealed. Please review the verified

Change document

Download Seal

Crypto Seal Origin:	SICPA
Issuance	06/05/2020 08:08
Issuer	Ministry of Health of Utopia

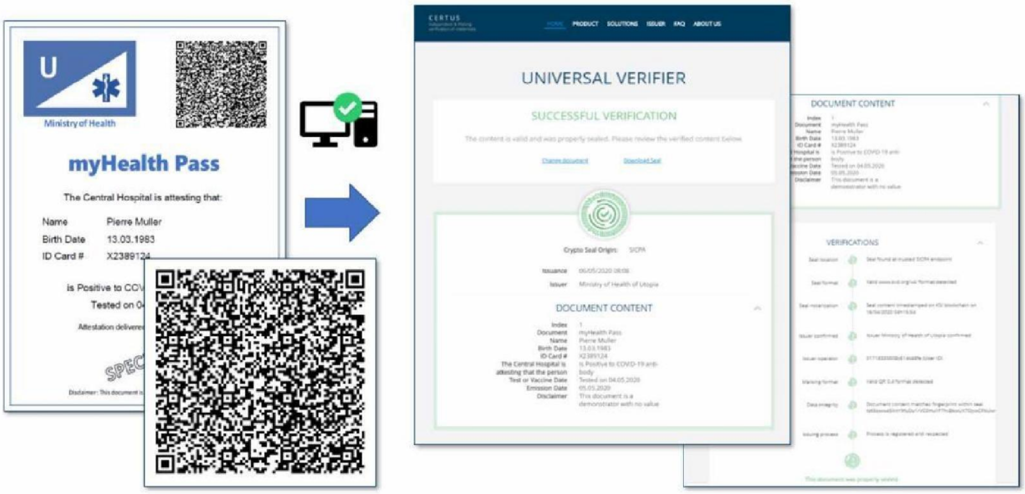
DOCUMENT CONTENT

Index	1
Document	myHealth Pass
Name	Pierre Muller
Birth Date	13.03.1983
ID Card #	X2389124
The Central Hospital is attesting that the person	is Positive to COVID-19 anti-body
Test or Vaccine Date	Tested on 04.05.2020
Emission Date	05.05.2020
Disclaimer	This document is a demonstrator with no value

VERIFICATIONS

Seal location	Seal found at trusted SICPA endpoint
Seal format	Valid www.sed.org/v4/ format detected
Seal notarization	Seal content timestamped on KSI Blockchain on 16/04/2020 04h15:54
Issuer confirmed	Issuer Ministry of Health of Utopia confirmed
Issuer operator	[illegible] (User ID)
Marking format	Valid QR 0.4 format detected
Data integrity	Document content matches fingerprint
Issuing process	Process is registered and respected

Figure 4: Universal verification, with a Smartphone, using a WebApp (https://www.certusdoc.com)



U

Ministry of Health

myHealth Pass

The Central Hospital is attesting that:

Name	Pierre Muller
Birth Date	13.03.1983
ID Card #	X2389124

is Positive to COV

Tested on 0

Attestation delivere

SPEC

Disclaimer: This document is

CERTUS

UNIVERSAL VERIFIER

SUCCESSFUL VERIFICATION

The content is valid and was properly sealed. Please review the verified content below.

Change document

Download Seal

Crypto Seal Origin:	SICPA
Issuance	06/05/2020 08:08
Issuer	Ministry of Health of Utopia

DOCUMENT CONTENT

Index	1
Document	myHealth Pass
Name	Pierre Muller
Birth Date	13.03.1983
ID Card #	X2389124
The Central Hospital is attesting that the person	is Positive to COVID-19 anti-body
Test or Vaccine Date	Tested on 04.05.2020
Emission Date	05.05.2020
Disclaimer	This document is a demonstrator with no value

VERIFICATIONS

Seal location	Seal found at trusted SICPA endpoint
Seal format	Valid www.sed.org/v4/ format detected
Seal notarization	Seal content timestamped on KSI blockchain on 16/04/2020 04h15:54
Issuer confirmed	Issuer Ministry of Health of Utopia confirmed
Issuer operator	[illegible] (User ID)
Marking format	Valid QR 0.4 format detected
Data integrity	Document content matches fingerprint within seal [illegible]
Issuing process	Process is registered and respected

This document was properly sealed

Figure 5: Universal verification, with a computer (desktop – laptop), using a WebApp (https://www.certusdoc.com)

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.

Below is the brief roadmap to become a user. For contacts see back of the brief.

The Guardtime/SICPA 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

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

guardtime

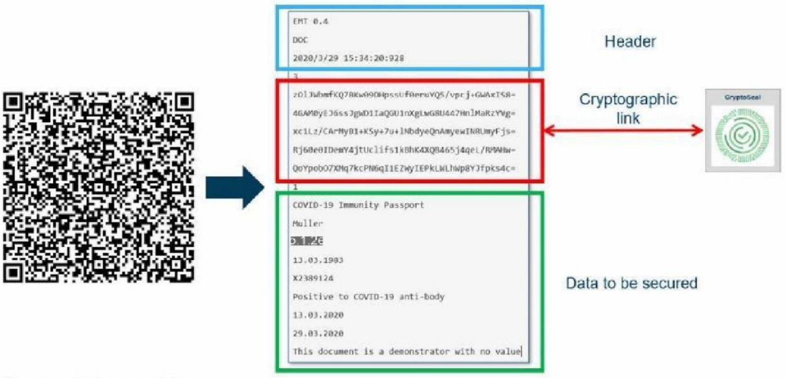
SICPA

TECHNICAL ANNEXES

SICPA/GUARDTIME "CERTUS" CryptoSeal

The CERTUS Platform generates CERTUS Documents (thus COVID Pass) in batches. The content of each document is secured by a QR code. Each QR code contains the data to be secured in the document - green frame.
The cryptographic signature is a unique and unforgeable link between the Data in the document and the corresponding CryptoSeal of the batch.

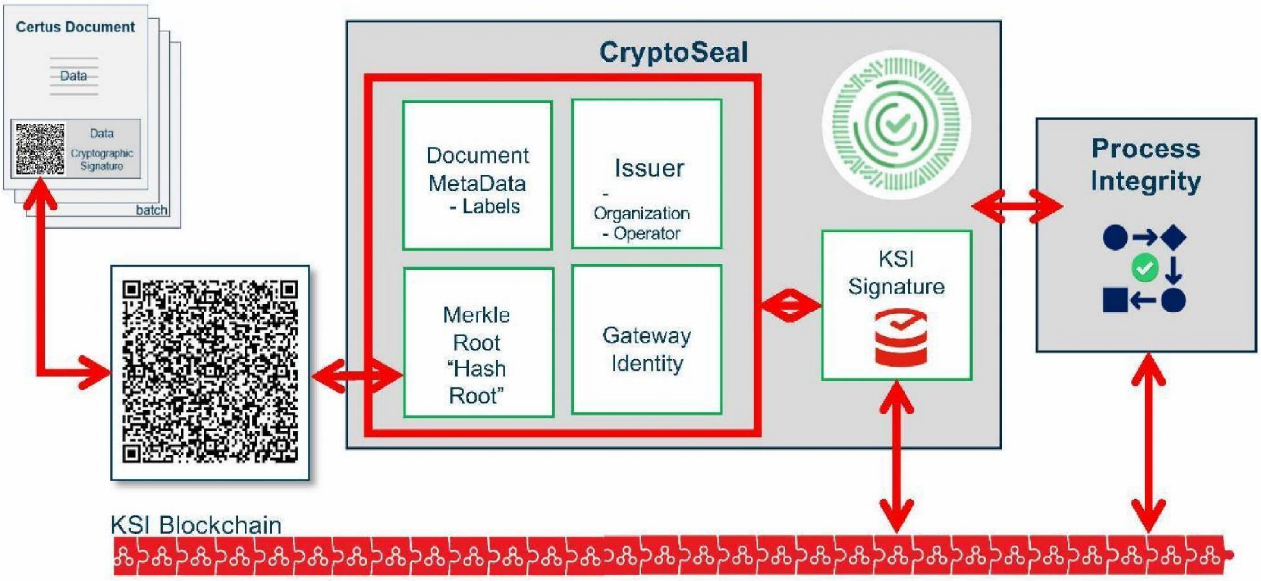
The CryptoSeal secures all documents in the batch. It also contains the name of the issuer, some metadata about the batch (e.g. issuance date, the Gateway used for the document generation, ...) and the Hash Root.



```
EMT 0.4
DOC
2020/3/29 15:34:20:928
3
zDl3WbmfKQ7BKw09DHpssUf0eruYQS/vpcj+GWAxTS8=
4GAM0yEJ6ssJgWD1IaQGU1nXgLwG8U447HnlMaRzYVg=
xc1Lz/CArMyB1+K5y+7u+lNbdyeQnAmyewINRUmyFjs=
Rj60e0IDemY4jtUclifs1k8hK4XQ8465j4qeL/RMAHw=
QoYpobO7XMq7kcPN6qI1EZWyIEPkLWLhWp8YJfpks4c=
1
COVID-19 Immunity Passport
Muller
[redacted]
13.03.1983
X2389124
Positive to COVID-19 anti-body
13.03.2020
29.03.2020
This document is a demonstrator with no value
```

© SICPA, Guardtime – October 2020

The CryptoSeal is signed on the Blockchain once the batch is activated. The figure below shows how a batch of documents is secured by the Blockchain, via the CryptoSeal.



© SICPA, Guardtime – October 2020

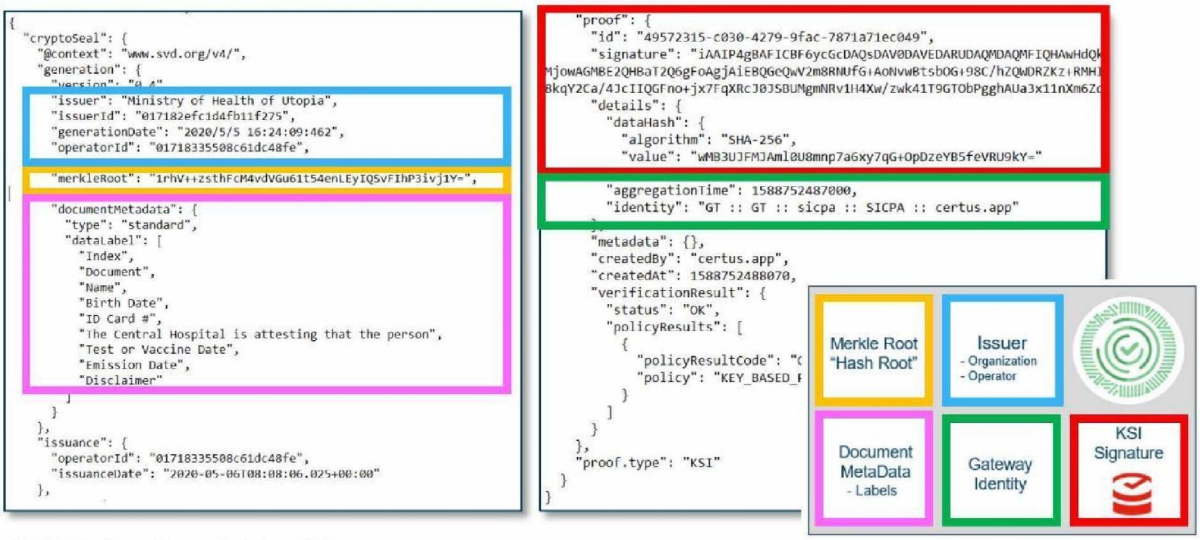
CryptoSeal integrity and verification

The integrity of each CERTUS document can be checked independently, with the CryptoSeal. The validity of the CryptoSeal can itself be checked through its KSI Signature on the Blockchain (independently from the CERTUS Platform).
As neither the CryptoSeal, nor the Blockchain, are hosting any data from the CERTUS document, it fully preserves the privacy of the beneficiaries.

The CryptoSeal is a JSON file, as shown on the Figure below. It contains the four components outlined in yellow, blue, pink and green, as well as the KSI Signature (outlined in red), which seals the whole CryptoSeal and which can be verified with any smartphone or computer.

As it can be seen, the CryptoSeal doesn't contain any PII (Personally Identifiable Information), it is fully GDPR compliant.

The CryptoSeal contains only MetaData, the Issuer's information and a cryptographic signature on the KSI Blockchain. No Data about the QR code content is included in the CryptoSeal



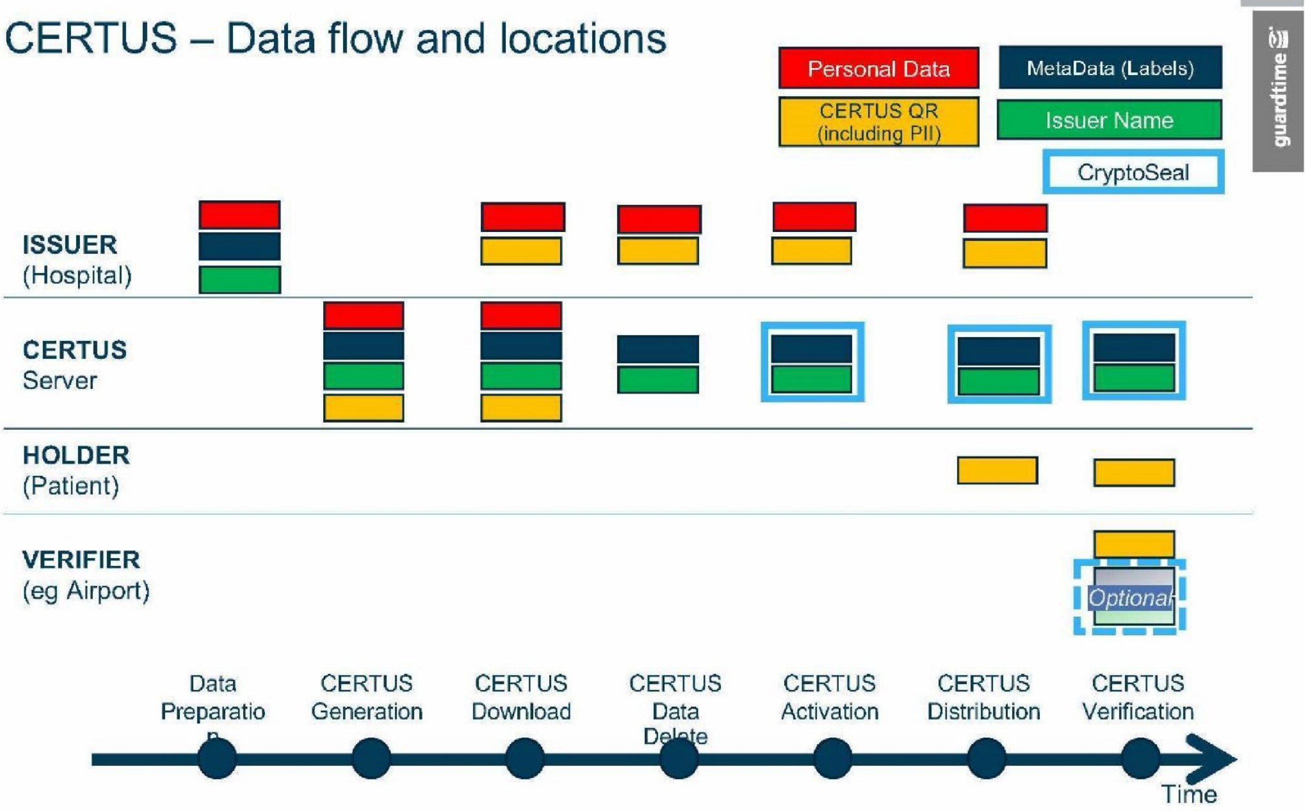
```
{
  "cryptoSeal": {
    "@context": "www.svd.org/v4/",
    "generation": {
      "version": "0.4"
      "issuer": "Ministry of Health of Utopia",
      "issuerId": "017182efc1d4fb11f275",
      "generationDate": "2020/5/5 16:24:09:462",
      "operatorId": "01718335508c61dc48fe",
      "merkleRoot": "1rhV++zsthFcM4vdVGu61t54enLEyIQSvFIhP3ivj1Y=",
      "documentMetadata": {
        "type": "standard",
        "dataLabel": [
          "Index",
          "Document",
          "Name",
          "Birth Date",
          "ID Card #",
          "The Central Hospital is attesting that the person",
          "Test or Vaccine Date",
          "Emission Date",
          "Disclaimer"
        ]
      }
    },
    "issuance": {
      "operatorId": "01718335508c61dc48fe",
      "issuanceDate": "2020-05-06T08:08:06.025+00:00"
    },
```

```
    "proof": {
      "id": "49572315-c030-4279-9fac-7871a71ec049",
      "signature": "iAAIP4gBAFICBF6ycGcDAQsDAV0DAVEDARUDAQMDAQMFIQHAwHdQk
MjowAGMBE2QHBaT2Q6gFoAgjAiEBQGeQwV2m8RNUfG+AoNvwBtsbOG+98C/hZQWDRZKz+RMHI
8kqY2Ca/4JcIIQGFno+jx7FqXRcJ0JSBUMgmNRv1H4Xw/zwk41T9GTObPgghAUa3x11nXm6Zc
      "details": {
        "dataHash": {
          "algorithm": "SHA-256",
          "value": "wMB3UJFMJAml0U8mnp7a6xy7qG+OpDzeYB5feVRU9kY="
        "aggregationTime": 1588752487000,
        "identity": "GT :: GT :: sicpa :: SICPA :: certus.app"
      },
      "metadata": {},
      "createdBy": "certus.app",
      "createdAt": 1588752488070,
      "verificationResult": {
        "status": "OK",
        "policyResults": [
          {
            "policyResultCode": "(
            "policy": "KEY_BASED_F
          }
        ]
      }
    },
    "proof.type": "KSI"
  }
}
```

© SICPA, Guardtime – October 2020

Guardtime/SICPA global verifiable Covid certificate data flow (version 1.1)

CERTUS – Data flow and locations



1. ***DATA PREPARATION:*** *During the emission process, the ISSUER will upload all the input data (i.e. with the PII - personal information, as it will appear on the myHealth Pass) in an encrypted form to the CERTUS SaaS*
2. ***CERTUS GENERATION*** *takes place on the CERTUS SaaS using the uploaded documents – a unique QR will be generated.*
3. ***CERTUS DOWNLOAD*** *phase means that the ISSUER will download the unique QR code (that contains PII) onto its system (data in transit is encrypted)*
4. ***CERTUS DATA DELETE*** *phase means that before the activation of the CERTUS documents, all these input data, as well as the generated CERTUS documents are deleted from the CERTUS SaaS.*
5. ***CERTUS ACTIVATION*** *for a given batch of certificates can NOT be made if the data have not been deleted before. This is guaranteed by the "Process integrity" engine (powered by KSI-VBP). Thus, we can guarantee that no data are stored on the CERTUS SaaS, except the Cryptoseal.*
6. ***CERTUS DISTRIBUTION*** *is the phase when the ISSUER will send the QR code to the HOLDER (patient) – only the latter can share the QR code with outside parties (eg with the VERIFIER)*
7. ***CERTUS VERIFICATION*** *can be performed with the a) Certus WebApplication or b) Certus MobileApplication.*
   1. *During the verification the personal data in the QR code are encrypted by Front-end (WebApplication) or on the MobileApplication only and never send to the server. Verification is done in three times:*
      1. *Request label of corresponding Cryptoseal to CERTUS Server*
      2. *Compute locally required hashes for verification*
      3. *Send it the CERTUS server for verification with the Cryptoseal (data integrity, KSI signature). Answer contains : Valid/Not valid including status/error message; Issuer Name; Operator ID ; issuance date, KSI timestamp date and time, seal format and labels*
   2. *An "off-line" verification mechanism can be available for MobileApplication where the Cryptoseal are download (included KSI signature validation) on the phone and all verification are done locally*

As all the PII are directly in the CERTUS document itself, the verification is not looking for any PII from any database as no PII leave the device which perform the checks.. In Estonia, we assume that the PII and medical data are stored in the Digital medical patient record, but these records will never be accessed to verify a CERTUS Pass. Thus CERTUS is not creating any risk for the patient records database of Estonia.

FUTURE PLANS:

- *A new version of the solution is under development for computing locally the claim hashes required for generating the CERTUS credentials which will be sent to CERTUS SaaS in order to build and secure the Cryptoseal; without dispatching to the CERTUS SaaS any PII, even temporary. This is targeted to become available by Q1-2021.*

guardtime

SICPA

www.guardtime.com | www.sicpa.com

Global Digitally Verifiable Vaccination Certificate

CONTACT Solution Manager:

5.1.2e

5.1.2e

5.1.2e