Fact Sheet

Cogito Group

Ministry of Health - Vaccine Passport

Vaccine Passport Requirements

New Zealand's Ministry of Health (MoH) required an authentication solution for creating digital COVID-19 health certificates. At a high level this involved:

- Technology and infrastructure to generate compliant digital certificates, initially aligned to the EUDCC credential format.
- Integration with the New Zealand CSCA infrastructure and the ICAO PKD.
- Development or integration into the EUDCC gateway
- Operational support for any technical solution, including hosting, proactive and reactive maintenance, incident and event management, and key management.

Cogito Solution

Cogito Group offered a solution for MoH digital health certificates that included:

- integration with APIs for the retrieval of data of the information required to create the certificates
- the signing of those certificates by the trusted PKI
- an auditable solution allowing a high trust environment to be established that will allow the created digital certificates to be recognised and trusted internationally

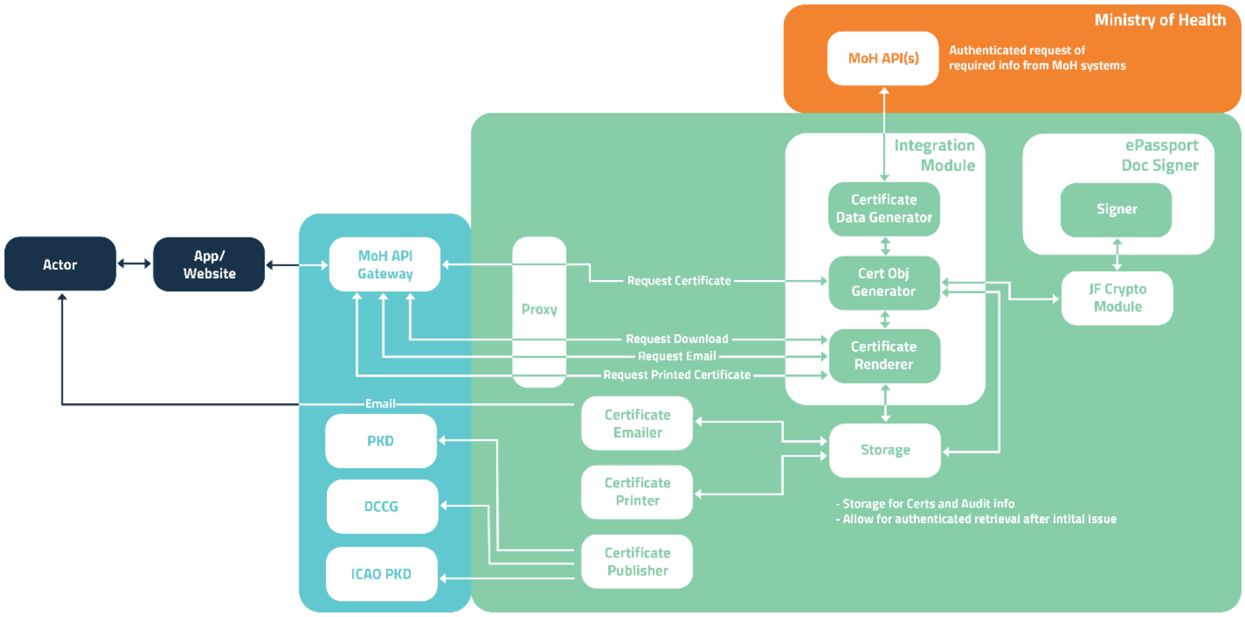
Importantly, Cogito was able to provide a solution that ensured a secure way for citizens to get or request a copy of their vaccination certificate that:

- Prioritises self-service over assisted service, to reduce operational impacts on the health system
- Provides a way to get a health certificate via non-digital means.

Cogito was also able to leverage their existing capability, already used for submitting requests for signing for DIA ePassports using document signing certificates issued from the existing NZ CSCA, to provide publication of the Health Certificate signing certificates to the existing ICAO PKD and extend this capability where required to integrate with another PKD or the Digital COVID Certificate Gateway (DCCG). Cogito has established technology and infrastructure to:

- Create EUDC-compliant digital health certificates; and
- Integrate with NZ CSCA and ICAO PKD

High level overview of the solution



Steps:

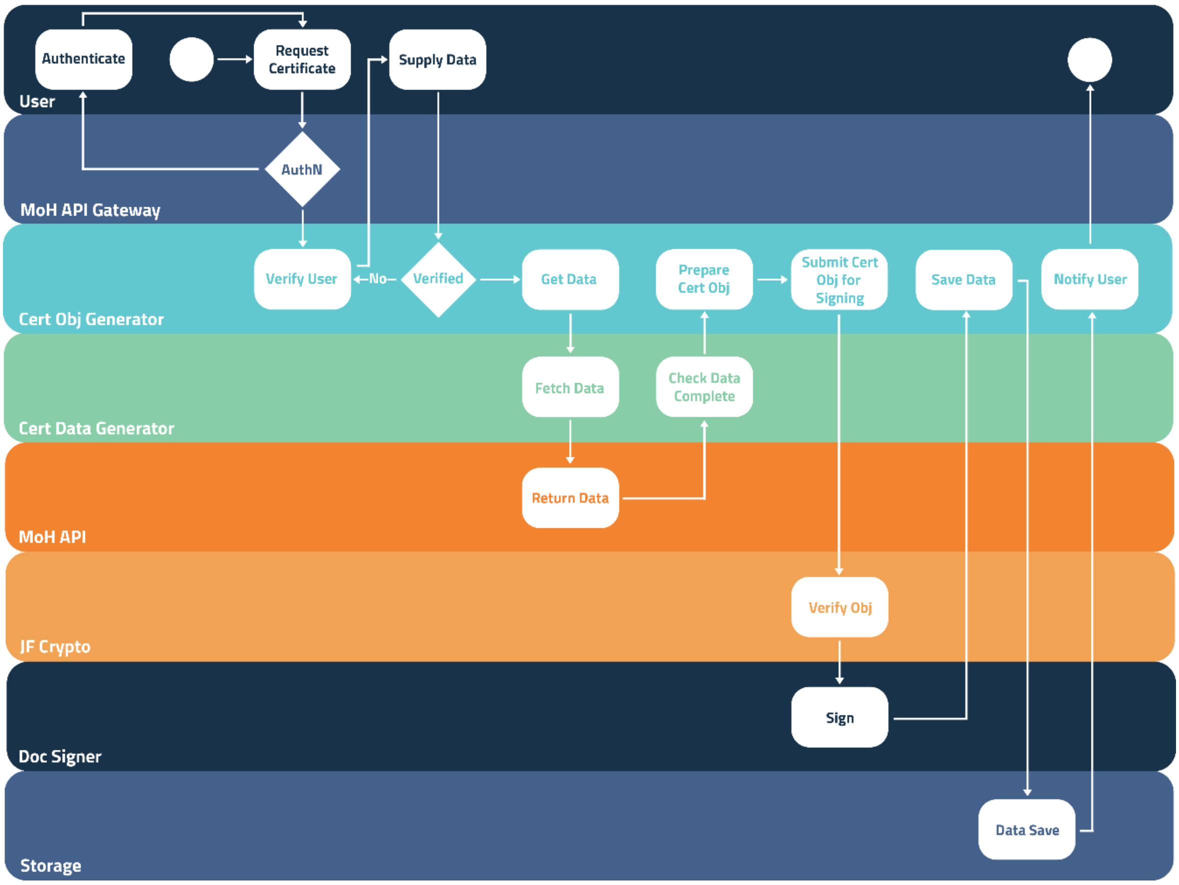
- An appropriately authenticated and authorised user of the service would be able to request the creation of a Health Certificate from their application or website.
- The authentication and authorisation process to access the required services for the certificate creation would be performed by the MoH API gateway utilise existing MoH authentication and authorisation methods.
- When a certificate request is made, the details of the user would need to be gathered and verified/validated.
- The Integration module contains the required implementations to:
  - generate the Health Certificate object (Cert Obj Generator);
  - request the required details for the certificate based on the user details and the type of Health certificate required from MoH data sources via existing APIs or new APIs where the existing capabilities are unable to provide the required data (Certificate Data Generator)
  - render the generated certificate (Certificate Renderer)

Certificate Issuance Process

To initiate the Certificate issuance process, the requestor would be required to be authenticated. This authentication process would use the authentication processes currently required by the MoH API Gateway. When authenticated the user will present their details required for the creation of the Health Certificate being requested. The presented data will be used to fetch the required details from MoH datastores via available APIs. Data returned from the MoH APIs will be checked to ensure it is complete for the type of certificate that is to be issued. If correct, the data will be placed into the correct format and submitted for signing.

Cogito's Jellyfish Crypto module will verify the validity of the object and submit it to the Document Signer to be signed. Once signed, the returned certificate can be saved to storage to allow it to be retrieved later to allow reissue. This is crucial in the event that the certificate becomes lost or damaged following retrieval by the Requestor. Once stored the requestor will be notified and presented with the options such as to print, download or to save in a wallet.

Request Certificate



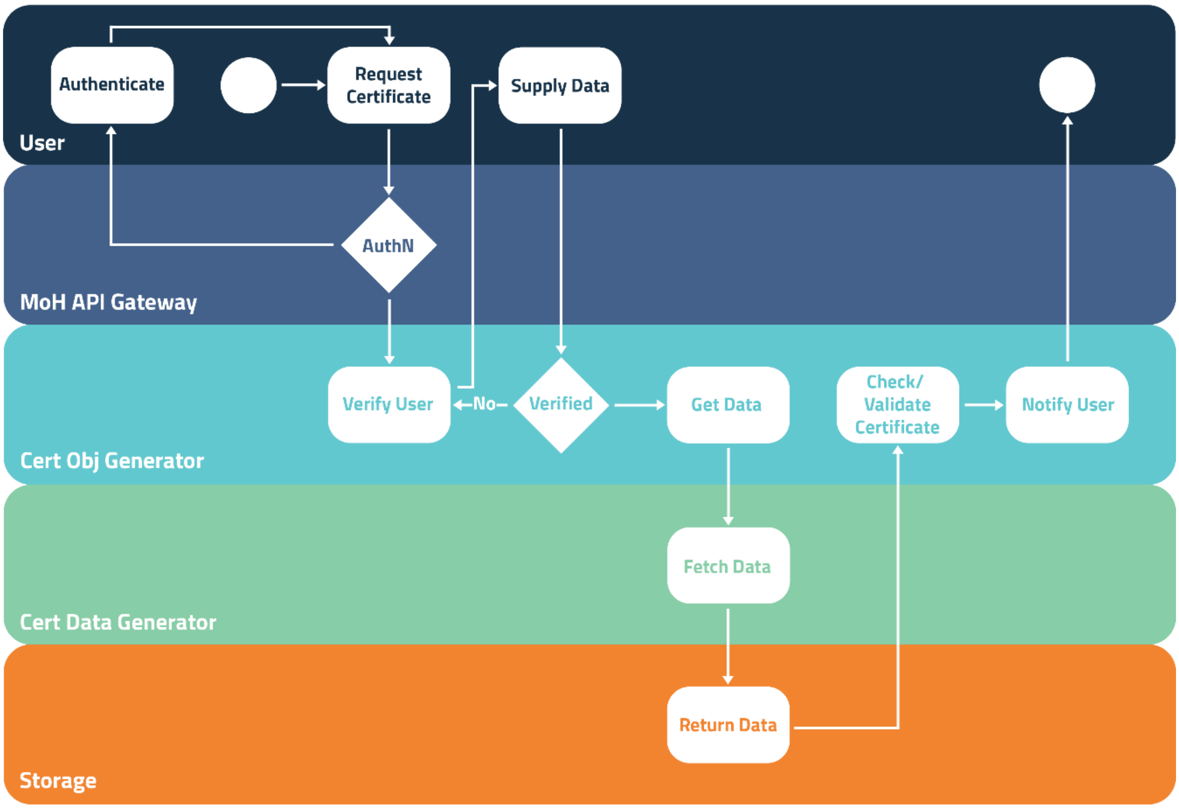
Reissue Certificate Process

The individual requesting the reissue of the previously issued certificate, would first be required to login to the system, utilising the authentication processes in use for the MoH API Gateway.

Once authenticated the requestor will be able to request the reissue and will need to verify that the certificate was previously issued to them.

At the completion of the verification, the certificate will be fetched from storage, checked and validated to ensure it is still a valid certificate, the user notified and presented with the options available for them to download, print or save the certificate.

Reissue Certificate

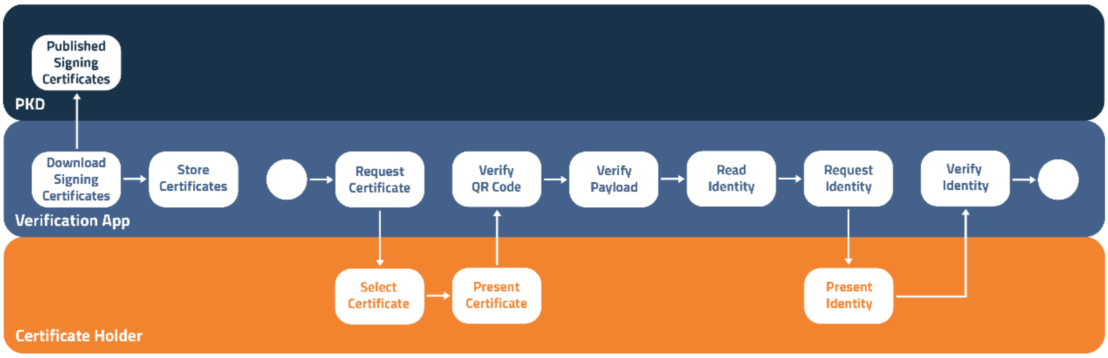


Offline Variation Process

Where the verification process is performed using an offline process, the published signing certificates would be downloaded from a publication point, in this case the PKD and then stored within the verification application.

When a certificate holder presents to have their Health Certificate verified the holder would be required to present their certificates QR code for validation (paper or electronic). When the QR code is verified, the verification application will verify the payload of the certificate and read the identity details. If required, the Verifier can request the Holder for an identity document that contains the identity details contained within the certificate, DOB and name, such as a drivers license or passport and then verify that the Holder is the person represented by the Health certificate.

Offline Verification



Revocation Process

The process or revocation of a Health certificate is similar to the process by which a passport would be made untrusted. Should a Document Signing server signing X.509 certificate become compromised, the revocation of this certificate and publishing of a new CRL would remove any trust and invalidate all Health certificates signed by that Document Signing X.509 certificate.

Audit Logging

Audit and logging information will be captured as part of the certificate creation process and also where the certificate has been reissued as a replacement. The full details of logging can be finalised as part of the final initial implementation requirements to ensure that it fully meets the needs of the MoH.

Logging within Cogito products is anonymised where it relates to data and the requesting of certificates to ensure the protection of privacy information. This logging information can be reconstituted later but protects from information aggregation.

Support Services

Cogito Group provides operational support for the software and infrastructure it provides to enable the creation and publication of Digital Health certificates under the TaaS construct. Operational support includes:

- Performance monitoring
- Reactive support for issues as they occur
- Proactive maintenance and software support to ensure that the MoH has the most available and secure service possible
- Change control and incident management, including integration with MoH processes where required to deliver changes, fixes and maintenance
- A service desk capability for tech support query escalation and the provision of responses and answers to frontline support teams

Support services are available 24/7 via Cogito's on call support operator.