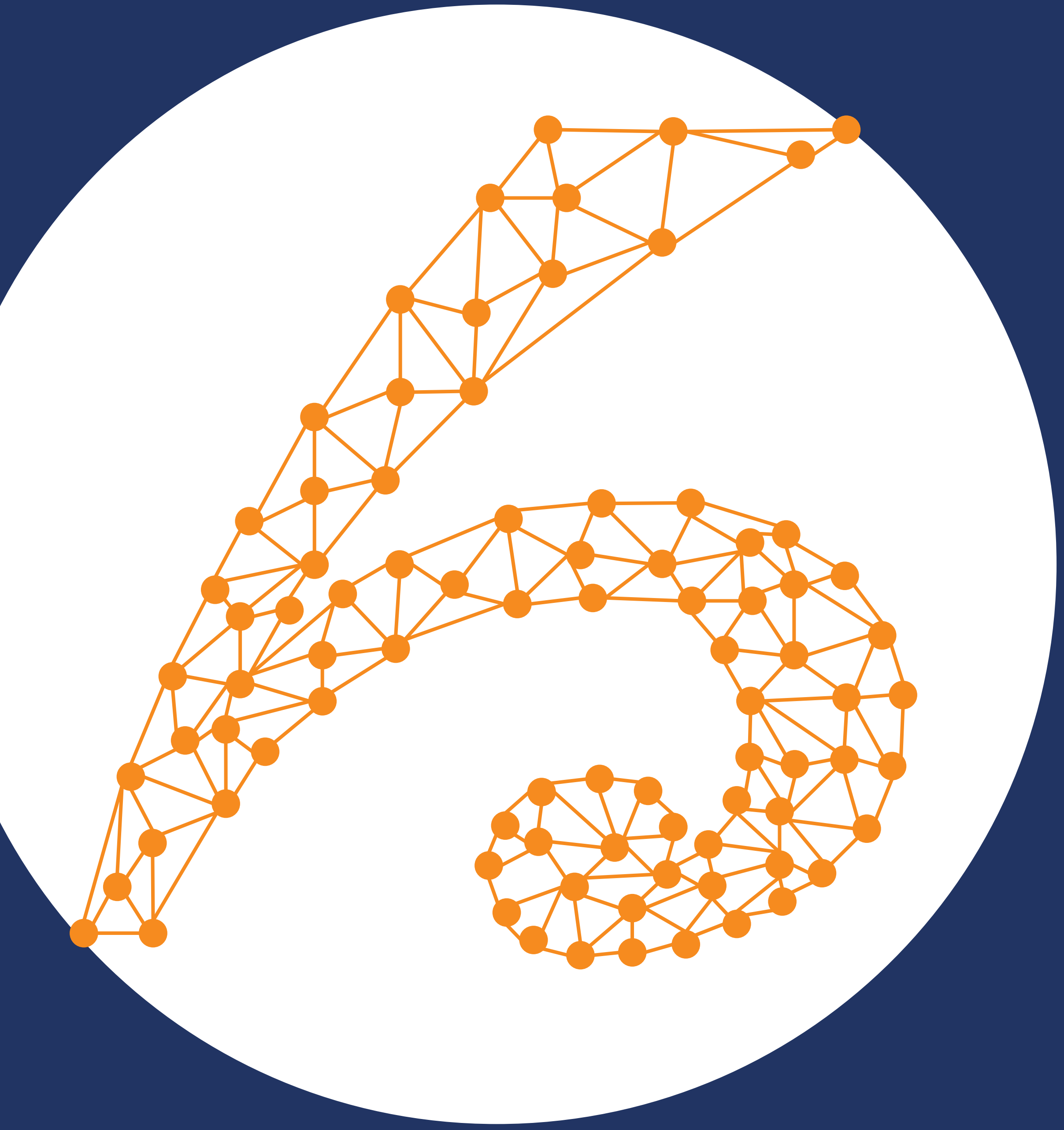
Document 1

From: Patrick Hindmarsh
Sent: Friday, 17 September 2021 4:28 pm
To: s 9(2)(a) [redacted]
Subject: Domestic use of COVID-19 vaccination certificates.pptx
Attachments: Domestic use of COVID-19 vaccination certificates.pptx

Document 1

MINISTRY OF HEALTH
MANATŪ HAUORA



Domestic use of COVID -19 vaccination certificates

Proof of concept

Document 1

Background

- MOH is progressing work to deliver an internationally recognised vaccination certificate aligned to the EUDCC, for the purposes of international travel.
- Ministers have asked for advice about the use of vaccination certificates in a domestic context, particularly for providing certainty for running large scale events for vaccinated
- Putting aside the policy questions on this, there are several technology aspects that need to be considered for domestic use
- This pack sets out key objectives and an approach to deliver a proof of concept for a domestic-issued vaccination certificate, to help inform possible policy options should they be needed.

Document 1

Key objectives

- Assess whether reuse of the EUDCC in a domestic context is suitable, factoring in privacy concerns, and cost to operate using NZ CSCA.
- Assess alternative standards that could be used to implement health certificates in a domestic context, in particular standards that offer privacy-preserving features.
- Establish a Health-PKI approach for issuing digital health certificates that does not rely on the NZ ePassports CSCA.
- Assess whether a Consumer wallet app/website is required, and how it might work
- Assess whether a Verifier app/service is required, and how it might work
- Implement a proof of concept for that could test assumptions of a production-capable solution at a “large scale public event”.

Document 1

Considerations for PKI

- International vaccination certificates are being issued using the ePassports CSCA, which has increased security and compliance requirements that may not be proportionate.
- Additionally, there is a cost per signing operation for the ePassports CSCA, which means domestic use cases could end up being expensive.
- MOH is in the process of developing a PKI strategy and supporting infrastructure. This means at present there is no established platform or approach for Health-owned PKI services.
- Trust frameworks supporting PKI are a consideration, and how we provide public key material to verifiers in a trusted way remains an open question.
- A possible option would also be to move to Health-owned PKI for international certificates, although the ramifications of this are unknown.

Document 1

Considerations for credential format

- EUDCC uses first name, last name, and DOB as the binding factors. This means a verifier needs to assert identity through another means (like a photo ID).
- Its probably unnecessary for a domestic verifier to need details about the vaccinations administered, given all they really want to know is “is this person vaccinated”.
- Other credential formats support features like selective disclosure which might be more privacy preserving, although these features require digital presentation via a wallet app
- We will need to maintain support for paper-based representations to ensure certificates are as widely accessible as possible.

Document 1

Considerations for consumers

- Paper based representation is still important
- Is the an opportunity to align to previous DIA work on decentralised identity and verifiable credentials.
- Is there a flow where a consumer does not need to present another form of ID in order for the certificate to be validated?
- How

Document 1

Considerations for verifiers

- Offer different verification paths for different assurance levels, and whether additional ID needs to be sighted or not?
- Maybe there’s three assurance levels, red for unverified, amber for verified but ID sighting is required, and green for verified and identity confirmed?
- Need to ensure that there are verification capabilities that can be embedded into other systems (e.g. a ticketing website so ticket purchase is linked to vaccination proof).
- Do we need to be able to verify an internationally issued certificate in the same place as a domestic one, or do we offer a way to convert an international cert into a domestic one, or something else?
- Are verifiers doing verification at the point of entry, or prior to an event?

Document 1

Possible solution

- Use the MATTR KMS to create a new temporary root CA for Health
- Use the current MATTR wallet app, extend with the proof of concept work done with DIA to create an OIDC bound identity in the app, then bind the digital credential to that. This could give the ‘green’ assurance level
- Implement a paper-based version, which gives the amber level assurance
- Extend the MATTR verifier app to support scanning these. Implement a set of verification rules for

MINISTRY OF HEALTH
MANATŪ HAUORA

Document 1

Visit our website to learn more

www.digital.health.nz

Document 2

Subject: Domestic vaccination certs
Location: Microsoft Teams Meeting

Start: Fri 17/09/2021 4:30 pm
End: Fri 17/09/2021 5:00 pm
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Patrick Hindmarsh
Required Attendees [redacted] Selwyn Rimmer; Jon Herries; Aaron Pratley

---

Microsoft Teams meeting

Join on your computer or mobile app
Click here to join the meeting

Or call in (audio only)
[redacted] New Zealand, Wellington
Phone Conference ID: [redacted]
Find a local number | Reset PIN

Learn More | Meeting options

Document 3

Subject: what even is a weekend anyway?
Location: Microsoft Teams Meeting

Start: Sat 18/09/2021 2:00 pm
End: Sat 18/09/2021 2:30 pm
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Patrick Hindmarsh
Required Attendees s 9(2)(a)

Microsoft Teams meeting

Join on your computer or mobile app
Click here to join the meeting

Or call in (audio only)
s 9(2)(k) New Zealand, Wellington
Phone Conference ID: s 9(2)(k)
Find a local number | Reset PIN

Learn More | Meeting options

Document 4

Subject:	Domestic certs, Mattr runthrough
Location:	Microsoft Teams Meeting
Start:	Mon 20/09/2021 4:30 pm
End:	Mon 20/09/2021 5:30 pm
Show Time As:	Tentative
Recurrence:	(none)
Meeting Status:	Not yet responded
Organizer:	Patrick Hindmarsh
Required Attendees:	s 9(2)(a) Jon Herries; Selwyn Rimmer

Microsoft Teams meeting

Join on your computer or mobile app
Click here to join the meeting

Or call in (audio only)
s 9(2)(k) New Zealand, Wellington
Phone Conference ID: s 9(2)(k)
Find a local number | Reset PIN

Learn More | Meeting options

Document 5

From: [redacted]
Sent: Wednesday, 22 September 2021 8:12 am
To: Patrick Hindmarsh
Subject: RE: EXTERNAL: RE: Verifiable Health Records - Follow up

Hi Patrick

No problem at all.

Thanks for letting me know.

[redacted]

From: Patrick Hindmarsh <xxxxxxx.xxxxxxxxx@xxxxxx.xxxx.xx>
Sent: Tuesday, 21 September 2021 3:12 pm
To: [redacted]
Cc: Jon Herries <Jon.Herrixx@xxxxxx.xxxx.xx>
Subject: RE: EXTERNAL: RE: Verifiable Health Records - Follow up

Hey [redacted]

Apologies I was supposed to come back to you on this, for now the meeting tomorrow will be with MOH only, while we confirm a larger Apple audience to join a call with Mattr.

So for now, no attendance required on your side.

Cheers
Patrick

Patrick Hindmarsh
Principal Architect | Data and Digital
[redacted] | patrick.hindmarsh@health.govt.nz
133 Molesworth Street, Thorndon, Wellington

Keep New Zealand safe with NZ COVID Tracer
Get your NZ COVID Tracer QR code

Document 5

From: [redacted]
Sent: Tuesday, 21 September 2021 2:39 pm
To: Patrick Hindmarsh <Patrick.Hindmarsh@health.govt.nz>; [redacted]
Cc: Jon Herries <Jon.Herrixx@xxxxxx.xxxx.xx>
Subject: RE: EXTERNAL: RE: Verifiable Health Records - Follow up

Hi all

Just following up on the meeting below.

Are we going ahead with tomorrow 2pm-3pm?

Many thanks

[redacted]

From: [redacted]
Sent: Wednesday, 15 September 2021 10:30 am
To: Patrick Hindmarsh <Patrick.Hindmarsh@health.govt.nz>; [redacted]
Cc: Jon.Herrixx@xxxxxx.xxxx.xx
Subject: FW: EXTERNAL: RE: Verifiable Health Records - Follow up

Hi there

Both [redacted] and [redacted] can make 2-3pm (NZ) work on Weds 22nd.

Many thanks

[redacted]

From: Patrick Hindmarsh <Patrick.Hindxxxxx@xxxxxx.xxxx.nz >
Sent: Tuesday, 14 September 2021 2:55 pm
To: [redacted]
Cc: Jon Herries <Jon.Herrixx@xxxxxx.xxxx.xx>; [redacted]

Document 5

s 9(2)(a)
Subject: EXTERNAL: RE: Verifiable Health Records - Follow up

Hey s 9(2)(a)

How about (in NZ times):

12-1pm Thursday 16th
1-2pm Friday 17th
12-1pm Monday 20th
1-3pm Wednesday 22nd

s 9(2)(a) can you confirm if those times are ok for you?

Cheers
Patrick

Patrick Hindmarsh
Principal Architect | Data and Digital
s 9(2)(a) | patrick.hindmarsh@health.govt.nz
133 Molesworth Street, Thorndon, Wellington

Keep New Zealand safe with NZ COVID Tracer
Get your NZ COVID Tracer QR code

From: s 9(2)(a)
Sent: Tuesday, 14 September 2021 12:44 pm
To: Patrick Hindmarsh <Patrick.Hindmarsh@health.govt.nz>
Subject: Verifiable Health Records - Follow up

Hi Patrick,

As discussed late last week, we would love to schedule a follow up discussion on Verifiable health records and the work that you are already doing in NZ. We'd be happy to jump on a call with yourselves and your partner Mattr to take you through the Verifiable health records information and ensure we have the right people on the call to answer any technical questions. We'd love also if you would be willing to take us through the work you are doing already to help us align on how we can work together.

If you'd like to proceed, please do let me know a couple of day/time options that would work for you next week with the Mattr team and I'll have this setup on our side. If we can target around midday as this will work for timezones if we need to bring in the wider team.

Thanks

?

s 9(2)(a)
Enterprise | Apple

iPhone s 9(2)(a)
Auckland | New Zealand

Document 5

s 9(2)(a)

IMPORTANT INFORMATION

This correspondence is for the named person’s use only. It may contain confidential or legally privileged information or both. No confidentiality or privilege is waived or lost by any mistransmission. If you receive this correspondence in error, please immediately delete it from your system and notify the sender. You must not disclose, copy or rely on any part of this correspondence if you are not the intended recipient.

Neither the sender nor Apple warrants that any communication via the Internet is free of errors, viruses, interception or interference. Information is distributed without warranties of any kind.

****
Statement of confidentiality: This e-mail message and any accompanying
attachments may contain information that is IN-CONFIDENCE and subject to
legal privilege.
If you are not the intended recipient, do not read, use, disseminate,
distribute or copy this message or attachments.
If you have received this message in error, please notify the sender
immediately and delete this message.
****

This e-mail message has been scanned for Viruses and Content and cleared by the Ministry of Health's Content and Virus Filtering Gateway

---

****
Statement of confidentiality: This e-mail message and any accompanying
attachments may contain information that is IN-CONFIDENCE and subject to
legal privilege.
If you are not the intended recipient, do not read, use, disseminate,
distribute or copy this message or attachments.
If you have received this message in error, please notify the sender
immediately and delete this message.
****

This e-mail message has been scanned for Viruses and Content and cleared by the Ministry of Health's Content and Virus Filtering Gateway

---

Document 6

Subject: Domestic vaccination certificates
Location: Microsoft Teams Meeting

Start: Wed 22/09/2021 4:30 pm
End: Wed 22/09/2021 5:00 pm
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Patrick Hindmarsh
Required Attendees Thomas Britton; s 9(2)(a)
Optional Attendees: Joe Beesley; Kevin O'Donnell

Hey Tom,

Matt has nominated you to help with some of this domestic vax certs stuff, hoping this time works ok to intro you into the thinking so far and get your view on the PKI side of things.

Cheers
Patrick

Microsoft Teams meeting

Join on your computer or mobile app
Click here to join the meeting

Or call in (audio only)
s 9(2)(k) New Zealand, Wellington
Phone Conference ID: s 9(2)(k)
Find a local number | Reset PIN

Learn More | Meeting options

Document 7

From: [redacted] s 9(2)(a)
Sent: Wednesday, 22 September 2021 1:13 pm
To: Patrick Hindmarsh
Subject: Decks
Attachments: MOH 20 Sep 2021 Domestic Pass Part 1.pdf; MOH 21 Sep 2021 Domestic Pass Part 2.pdf

As discussed.

[redacted] s 9(2)(a)

This communication, including any attachments, is confidential. If you are not the intended recipient, you should not read it – please contact me immediately, destroy it, and do not copy or use any part of this communication or disclose anything about it. Thank you. Please note that this communication does not designate an information system for the purposes of the Electronic Transactions Act 2002.

Document 7

MATTR

MoH Domestic Passes Decision Discussions

Prepared for Ministry of Health Manatū Hauora
20 Sep 2021

Document 7

Solution – Domestic Passes (Vaccination and Test Result)

Domestic Pass(es) to support:

- Health Certificates (Vaccination and Test Results)
- Use at large scale events
- Low cost to operate
- Privacy preserving features
- Accessibility considerations for people – specifically paper based digitally verifiable credentials and digital first credentials
- Accessibility issues for verifiers
  - Cheap and easy to use
  - Ability to be embedded into existing systems (ie ticketing systems)
- Flexibility by decoupling from ePassport PKI which was designed for a very different purpose

With these requirements the natural solution candidate at a technical level would be:

- New health Trust Model using DPKI for scalability, flexibility and low cost – recommendation DID Web for discoverability and security of government domain
- W3C Verifiable Credentials (with BBS+ Signatures for selective disclosure features in digital journey's that use the JSON-LD variant)

This solution would allow the most advanced privacy preserving features for domestic use. It would also align directionally with the DIA Digital Trust Framework that is coming in December.

In order to progress this solution we would need validation of 5 assumptions. If these assumptions are not true, an alternative solution candidate would need to be considered

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

Document 7

Key decisions that impact solutioning

Document 7

Decision 1a: Health PKI

- Choices on trust model
    - Multi-tier (CSCA + Doc Signers) application specific (e.g. e-Passports) vs General Purpose Web PKI (e.g. SHC)
- Choices on key management - MATTR KMS (see next slides)
    - Keypair generation responsibility and choice of key types (see next slide)

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

Document 7

Appendix

Document 7

MATTR

Continuation of domestic pass discussion

Prepared for Ministry of Health Manatū Hauora
21 Sep 2021

Document 7

PKI Considerations

Document 7

What is Public Key Infrastructure (PKI)?

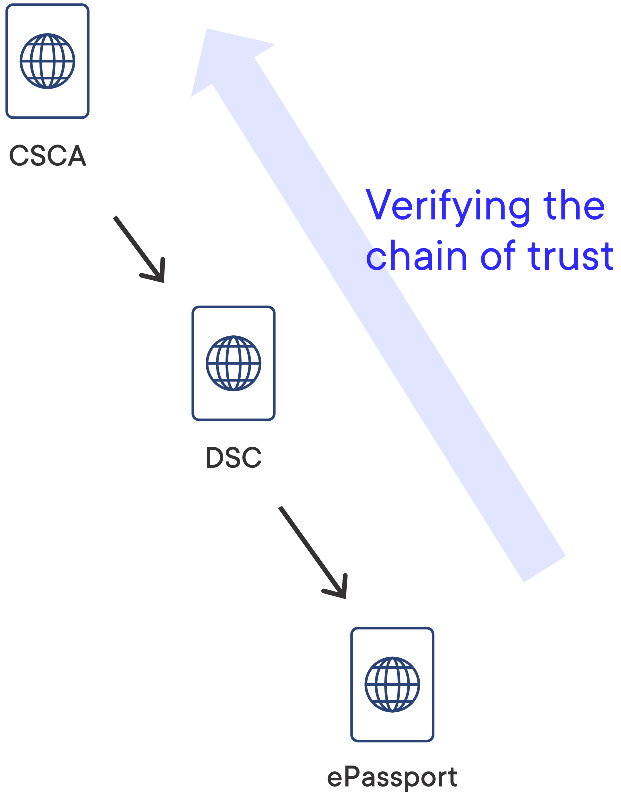
- A model for managing the usage of digital certificates and their associated cryptographic information

- A typical implementation involves
  - One or more CA (certificate authorities) who are the basis of trust
  - A set of certificates that are related via certificate chains back to one of the CA's trusted in the model
  - Certificate chains can be long 3-4 deep.

- Multiple different implemented PKI models
  - Application specific PKI
  - General purpose PKI model

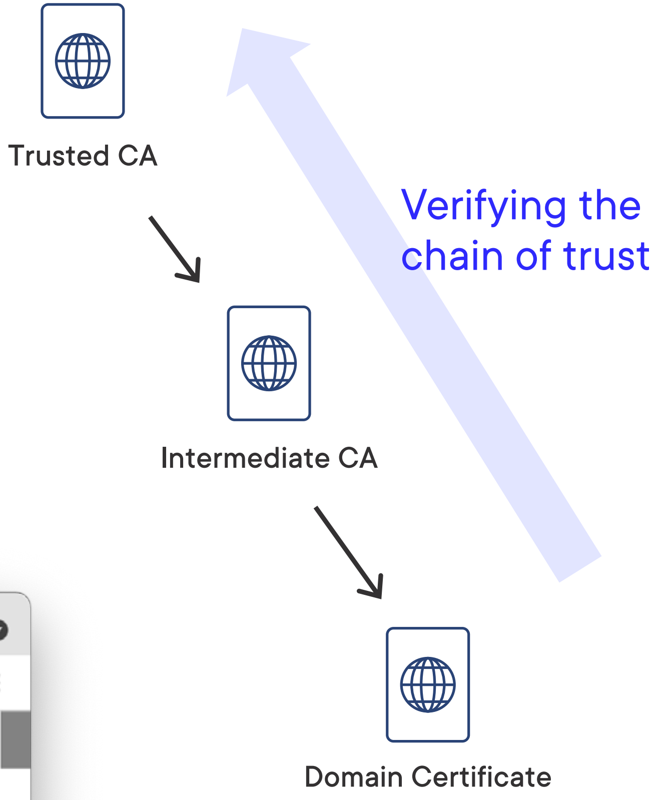
Application specific PKI model – Example ePassport

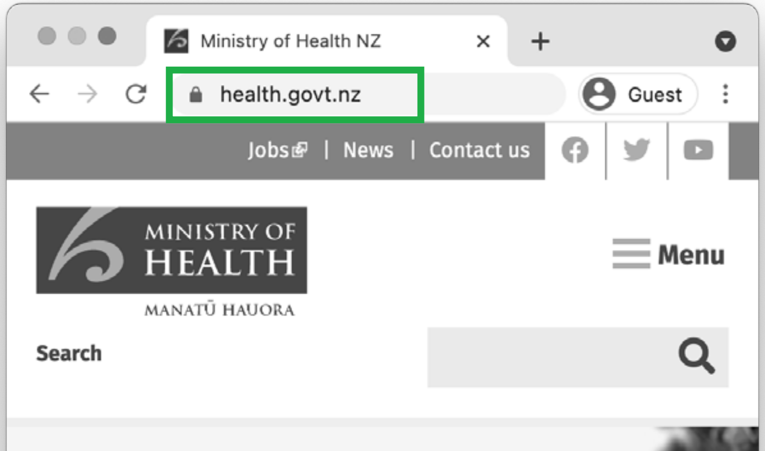
- An implementation of PKI for a specific application (e.g ePassports)
- Certificate Authorities have a narrow scope of function (basis of trust for a countries ePassports)
- Constrained two tier model
  - Country Signer CA's (CSCAs)
  - Document Signer Certificates (DSCs)



General Purpose PKI – Example Web PKI

- The PKI model which provides critical security to the web and or internet.
- Trusted CA list comes pre-loaded on every modern PC
- Essentially what the ”green/grey lock” icon in the browser
- Example – provides confidence I am talking to the domain owner of “`health.govt.nz`”





Why do we need PKI for NZ COVID Pass?

- **To establish the basis of trust for verifiable credentials issued by MoH.**
- **Safely distribute the public keys used to verify verifiable credentials issued by MoH.**

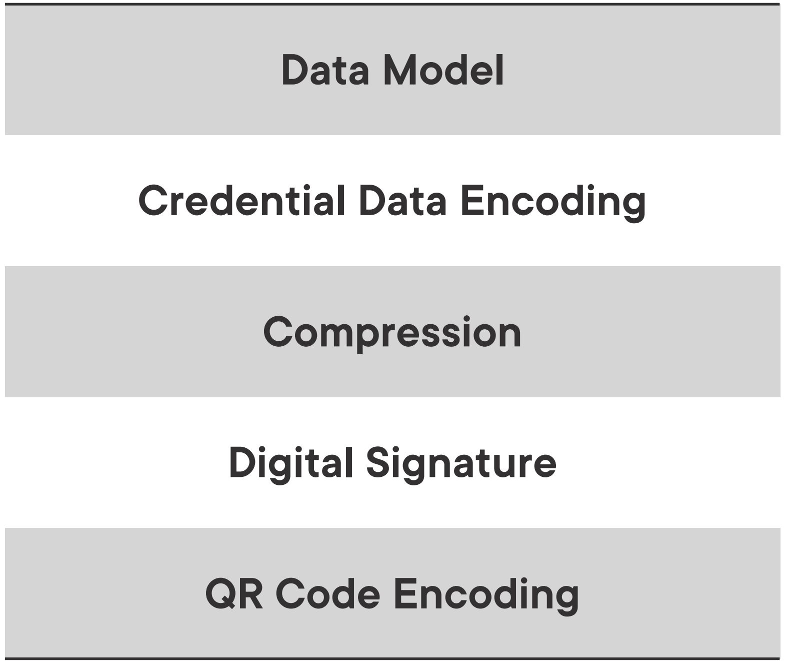
- Options for consideration
  - Application specific PKI Model, purpose specific CSCA (e.g Health CSCA for MoH Verifiable Credentials like ePassport system)
  - Rely on Web PKI model distribute public keys via web resource e.g `pki.health.govt.nz` (e.g model used by smart health cards)

Recommendation: Use Web PKI

- Prevents the need to create a health CSCA as critical path for COVID Pass
- Does not prevent adding in a CSCA later as an additional/alternative layer of security
- Host public keys used to verify COVID Passes on a MoH managed endpoint e.g "`pki.health.gov.nz`"
- Resolve via did:web
- Potential to resolve via other means in future/parallel (e.g .well-known/jwks)

Document 7

Credential Format Technology Layers – Paper Based



Data Model

Credential Data Encoding

Compression

Digital Signature

QR Code Encoding

ⓘ

Final recommendations on credential format to be provided in further deck. We are considering the following layers.

Credential Format Technology Layers – Digital First Credentials

Data Model	W3C VC Data Model (Abstract Data Model)
Credential Data Encoding	JSON-LD
Digital Signature	Linked Data Proofs

Document 7

Delivery Considerations

Document 7

	Week 1 28 Sept	Week 2 5 Oct	Week 3 12 Oct	Week 4 19 Oct	Week 5 26 Oct	Week 6 2 Nov
DROP 1 – Domestic Cert PDF Generation						
MATTR APIs Definition Published to Middleware	▨					
MATTR APIs Build	▨	▨	▨			
MATTR APIs QA & Pathway to Production			▨	▨	▨	
MATTR Early Drop of APIs			▨			
Middleware Build		▨	▨			
Middleware & MATTR Joint Testing			▨	▨	▨	
Complete Staging and Production Environments	▨	▨	▨			
Complete Risk & Compliance / A to Operate	▨	▨	▨	▨		
Penetrating Testing				▨	▨	
MOH UAT					▨	
Push to Production for Pilot						▨
DROP 2 – Apple/Google Wallet Integration (*requires more analysis to determine if can be delivered more quickly*)						
Complete Spec Work/ Solutioning	▨					
Publish API Spec to Middleware		▨				
MATTR Develop API		▨	▨	▨	▨	
Middleware Integration and inclusion in C3 journey		▨	▨	▨	▨	
Testing and Pathway to production						Plus 2 Weeks+

Delivery Considerations

Build priority

- Core APIs to Sign and produce PDF including implementation of MATTR KMS
- Wallet Integration (likely to come in a second drop as currently in a prototyping phase in MATTR)
- Full Operational Logging / Dashboards / APIs for transaction history may come later
- DCC activities would likely need to be deprioritised across MATTR, Middleware, MoH (some likely accelerated such as compliance steps) - DCC Gateway implementation would be deprioritised

Considerations

- Timeframes are best endeavours and not committed delivery dates and we would need to start tomorrow 22nd September
- ED25519 cryptography with MATTR KMS architecture as exists today
- Did: Web would be used
- MATTR will work with MOH to determine the optimal credential format/encoding approach
- Agreement on API formats (has dependency on format/encoding approach)
- MATTR Verification Capabilities require discussion

Risks

- MATTR and Middleware would need to run testing in parallel (prior to formal MATTR QA)
- Other Middleware dependencies on MoH systems and APIs would need to be resolved
- Scale of work required for compliance unknown
- Penetrating Testing would need to be done in parallel to other activities
- Tight timeframe for E2E Testing, UAT and Path to production activities
- MATTR are currently operating at risk (contracts pending)

MoH Ecosystem Support (Health Certificates Ecosystem)

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

Document 7

s 9(2)(b)(ii)

[redacted]

Document 7

Appendix

Document 8

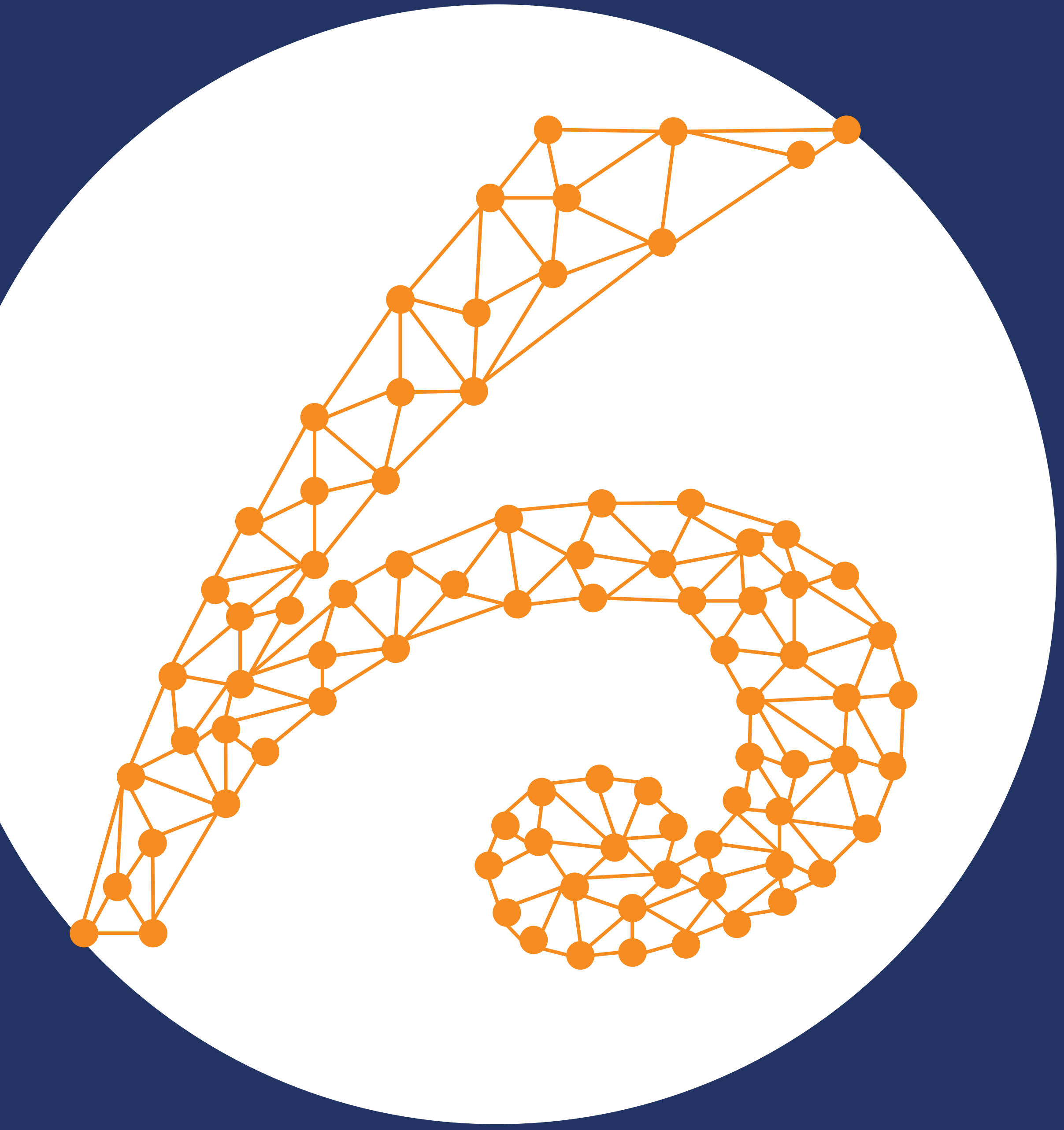
From: Patrick Hindmarsh
Sent: Friday, 24 September 2021 1:11 pm
To: s 9(2)(a) [redacted]
Cc: Jon Herries; Selwyn Rimmer
Subject: Domestic COVID-19 vaccination and test certificates.pptx
Attachments: Domestic COVID-19 vaccination and test certificates.pdf

Attached is the pack we've prepared for the PM.

Please keep distribution for this to people who need to know.

Document 8

MINISTRY OF HEALTH
MANATŪ HAUORA



Domestic COVID-19 vaccination and test certificates

Solution approach for a “Summer Pass”

Document 8

Background

- Work began in April to establish My Health Account and My COVID Record. This work is foundational for the wider health reforms and the investment announced in Budget 21 for the Hira Programme
- Similar work in other jurisdictions has been a multi-year effort, with Australia taking five years to establish similar services (ie. My Health Record)
- Now these foundations are in place, they allow us to build more features on top of them such as vaccination and test certificates, but also provide alignment to the Digital Identity Trust Framework that is currently in Select Committee in preparation for a first reading in the house.

Problem Statement

- Vaccination rates for the young and healthy are currently lagging the rest of the population
- Auckland and the rest of New Zealand continue to be at elevated alert levels, with internal boundaries in place
- Use of a domestic vaccine pass should deliver dual outcome of motivating the public to be vaccinated and supporting public health controls by reducing the risk of spread in public settings such as a summer festival or other large scale event
- The solution needs to be support privacy and equitable access for the public at scale and itself be easy to access and use. This is important for social license
- Solution needs to be available as soon as possible, then rapidly iterated to improve consumer experience and remove requirement to present photo ID with certificate to link it to the consumer

Design and technical goals compared to EUDCC

How does this fit with Reconnecting New Zealand

- NZ is adopting the EUDCC (European standard) for international travel certificates.
- The EUDCC data specification has much more than needed if these were used domestically. The Office of Privacy Commissioner has expressed concerns about this being used domestically.
- EUDCC requires photo ID (e.g. a normal Passport) to be presented when verifying, to prove the holder is the owner.
- In addition, using the EUDCC domestically is likely to be confused by New Zealanders with international certificates and incorrectly presented to foreign border agencies.
- Not using EUDCC domestically might mean we need to offer visitors and those vaccinated overseas an ability to convert their international certificate.
- MoH recommend using a different approach for a domestic pass.

Design and Technical Goals

- Highly privacy preserving, only the minimum data set is disclosed to allow verification
- Non-digital options available first, people should not require a modern smartphone to participate
- Tamper and forgery resistant using electronic verification, it should be very hard for someone to fake one of these
- Quick to deliver, we may need the solution in place before summer
- Standards-based, use existing technology standards to support future intents rather than inventing something new
- Open and transparent, we should publish documentation so others can build on it with creative ways to enable the public - as recently seen with examples Locations of Interest, TimeInline or Vaxx.

Document 8

Approach for domestic certificate

Develop an “NZ COVID Pass”

- A QR code containing consumer’s name and date of birth, minimum data for proving health status, and a digital signature to prove authenticity and tamper resistance.
- Leverage same technology platform used for international travel certificates, but use different data standards and signature (trust framework)
- Provides freedom to modify domestic certificate for domestic needs, including additional privacy protections and verifier capabilities.
- Can be printed on paper, and also leverages native support for ‘passes’ in Apple and Android phones, reducing reliance on another MOH-owned app to store it. Also will support other standards-based wallets.
- Based on W3C Verifiable Credentials standards, aligned to future digital identity trust framework legislation under consideration by parliament. Also forwards compatible with emerging SMART Health Cards standards from US/UK.

Verifier (to check the passes) ecosystem:

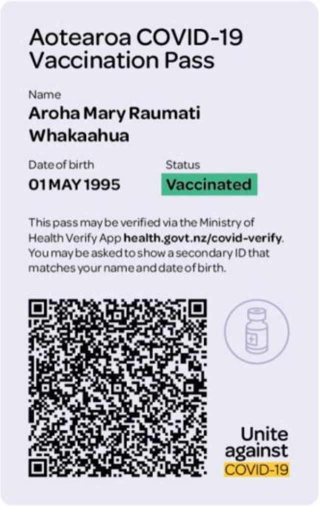
- We should support verifiers to implement verification capabilities into existing workflows (e.g. Ticketek), rather than requiring them to use a new app & hardware.
- Develop documentation and test suites for implementing third party verifier apps. Publish this publicly and engage larger partners (e.g. WhosOnLocation) to adapt existing scanning technology for events or entry control to business or buildings.
- Publish standards & guidelines for verifiers to evaluate certificate claims (e.g. time since vaccination)
- Implement an MOH-branded verifier app, using above documentation & standards, and publish open source on GitHub as a reference implementation. This would be available for those who don’t have existing verification hardware.

Two stage delivery

To accommodate timelines, we propose a two stage process.

Stage 1: Paper & Lo-fidelity Digital

- Paper based certificate that can be stored within iOS/Android operating system wallets.
- No native app required.
- 5-7 weeks



Aotearoa COVID-19 Vaccination Pass

Name
Aroha Mary Raumati Whakaahua

Date of birth
01 MAY 1995

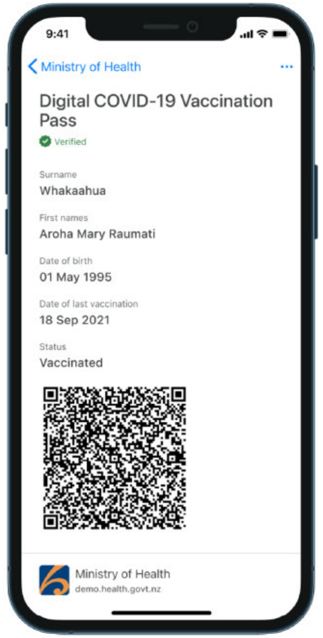
Status
Vaccinated

This pass may be verified via the Ministry of Health Verify App **health.govt.nz/covid-verify**. You may be asked to show a secondary ID that matches your name and date of birth.

Unite against COVID-19

Stage 2: Digital native

- Native app with a digital wallet. Supports additional privacy enhancements
- Supports more of the future Digital Identity Trust Framework and may allow a person to prove their identity as well.
- 3-6 months



9:41

Ministry of Health

Digital COVID-19 Vaccination Pass
✓ Verified

Surname
Whakaahua

First names
Aroha Mary Raumati

Date of birth
01 May 1995

Date of last vaccination
18 Sep 2021

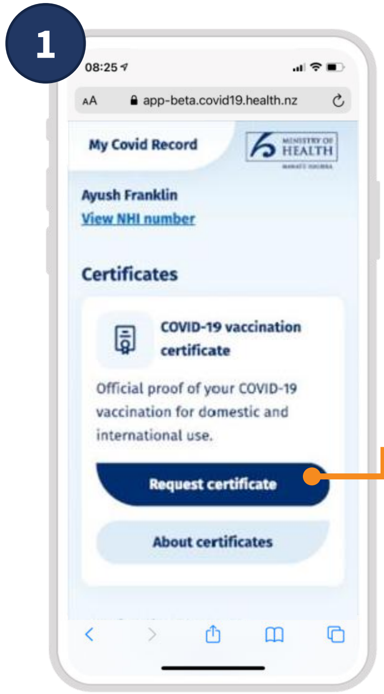
Status
Vaccinated

Ministry of Health
demo.health.govt.nz

Document 8

Consumer experience – Stage 1

- Log into My Covid Record to request a domestic certificate (needs My Health Account)
- Domestic branded PDF emailed to consumer
- Buttons in the email allow to add the pass to Apple Wallet on iOS or G Pay on Android.



1

08:25

app-beta.covid19.health.nz

My Covid Record

MINISTRY OF HEALTH

Ayush Franklin

View NHI number

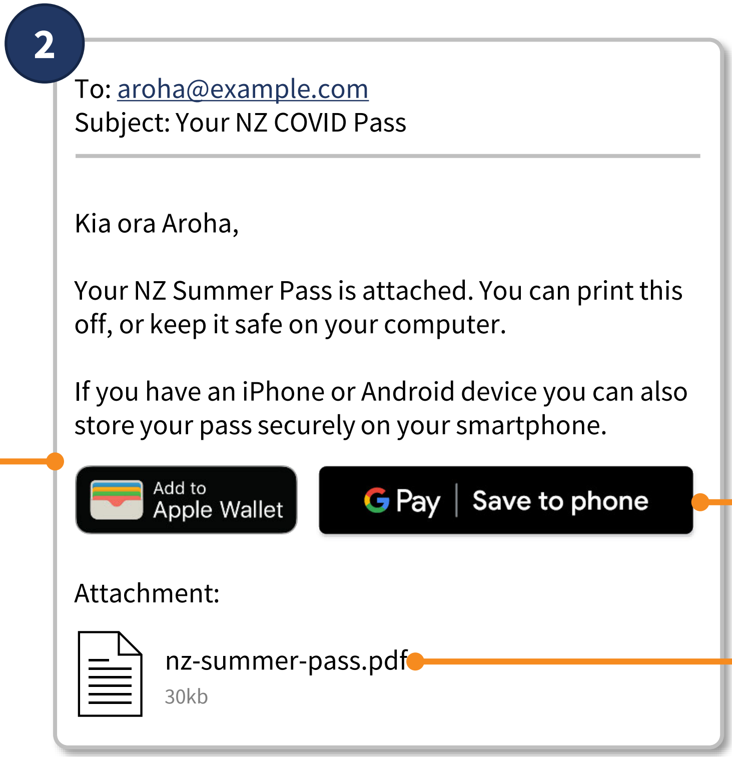
Certificates

COVID-19 vaccination certificate

Official proof of your COVID-19 vaccination for domestic and international use.

Request certificate

About certificates



2

To: aroha@example.com
Subject: Your NZ COVID Pass

Kia ora Aroha,

Your NZ Summer Pass is attached. You can print this off, or keep it safe on your computer.

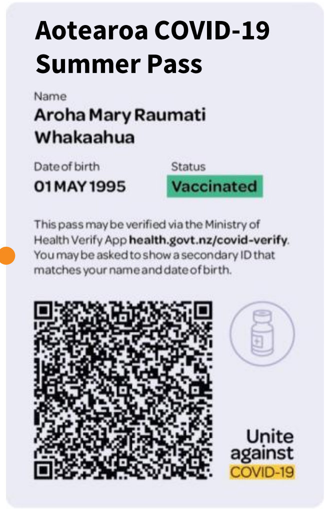
If you have an iPhone or Android device you can also store your pass securely on your smartphone.

Add to Apple Wallet | G Pay | Save to phone

Attachment:

nz-summer-pass.pdf
30kb

Printed copy



Aotearoa COVID-19 Summer Pass

Name
Aroha Mary Raumati Whakaahua

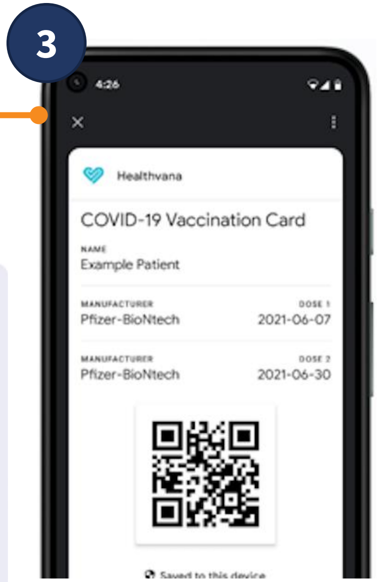
Date of birth
01 MAY 1995

Status
Vaccinated

This pass may be verified via the Ministry of Health Verify App **health.govt.nz/covid-verify**. You may be asked to show a secondary ID that matches your name and date of birth.

Unite against COVID-19

3



4:26

Healthvana

COVID-19 Vaccination Card

NAME
Example Patient

MANUFACTURER
Pfizer-BioNtech

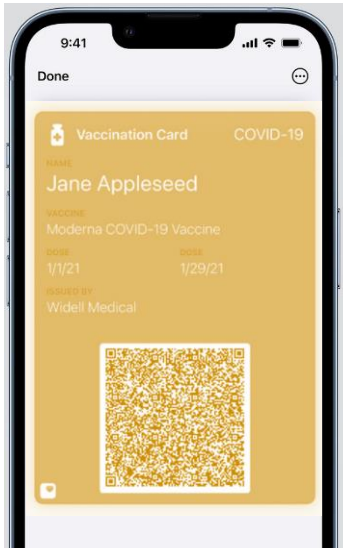
DOSE 1
2021-06-07

MANUFACTURER
Pfizer-BioNtech

DOSE 2
2021-06-30

Saved to this device

Google COVID Card



9:41

Done

Vaccination Card COVID-19

NAME
Jane Appleseed

VACCINE
Moderna COVID-19 Vaccine

DOSE
1/1/21

DOSE
1/29/21

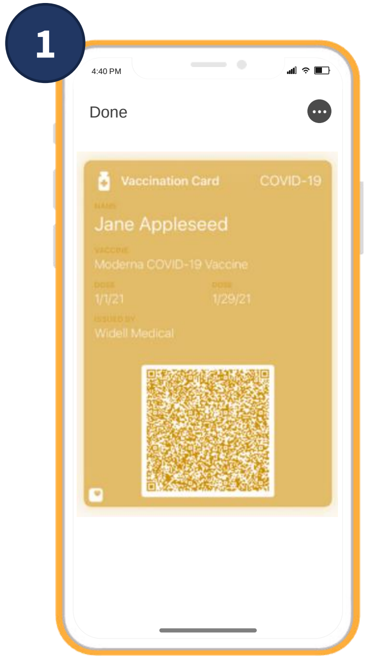
ISSUED BY
Widell Medical

In Apple Wallet

Verifier experience

Here is my NZ COVID Pass
Welcome to "The Summer Festival". Can I scan your NZ COVID Pass please

1


4:40 PM

Done

Vaccination Card COVID-19

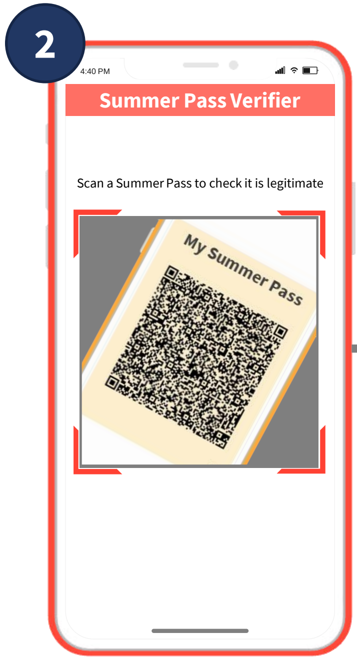
Jane Appleseed

Moderna COVID-19 Vaccine

1/1/21 1/29/21

Widell Medical

2


4:40 PM

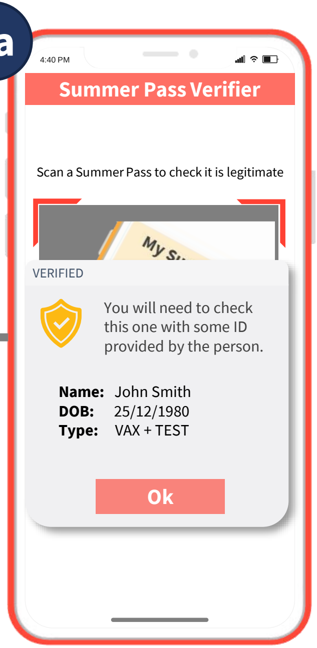
Summer Pass Verifier

Scan a Summer Pass to check it is legitimate

Person provides a valid summer pass

Person doesn't provide a valid summer pass

3a


4:40 PM

Summer Pass Verifier

Scan a Summer Pass to check it is legitimate

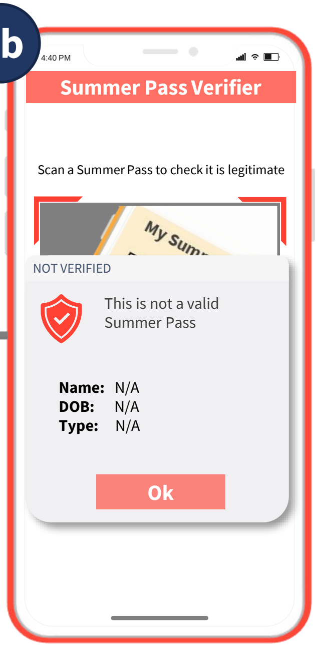
VERIFIED

You will need to check this one with some ID provided by the person.

Name: John Smith
DOB: 25/12/1980
Type: VAX + TEST

Ok

3b


4:40 PM

Summer Pass Verifier

Scan a Summer Pass to check it is legitimate

NOT VERIFIED

This is not a valid Summer Pass

Name: N/A
DOB: N/A
Type: N/A

Ok

1. Consumer presents their NZ COVID Pass via smartphone or printed copy
2. Verifier scans with Verifier App
3. Verifier app checks the signature is authentic, and the certificate claims pass requirements
   a. If the details are valid the verifier is shown enough detail to verify the holder's identity
   b. If the signature is invalid, or the data doesn't meet requirements (e.g. it has expired) the verifier sees an error message

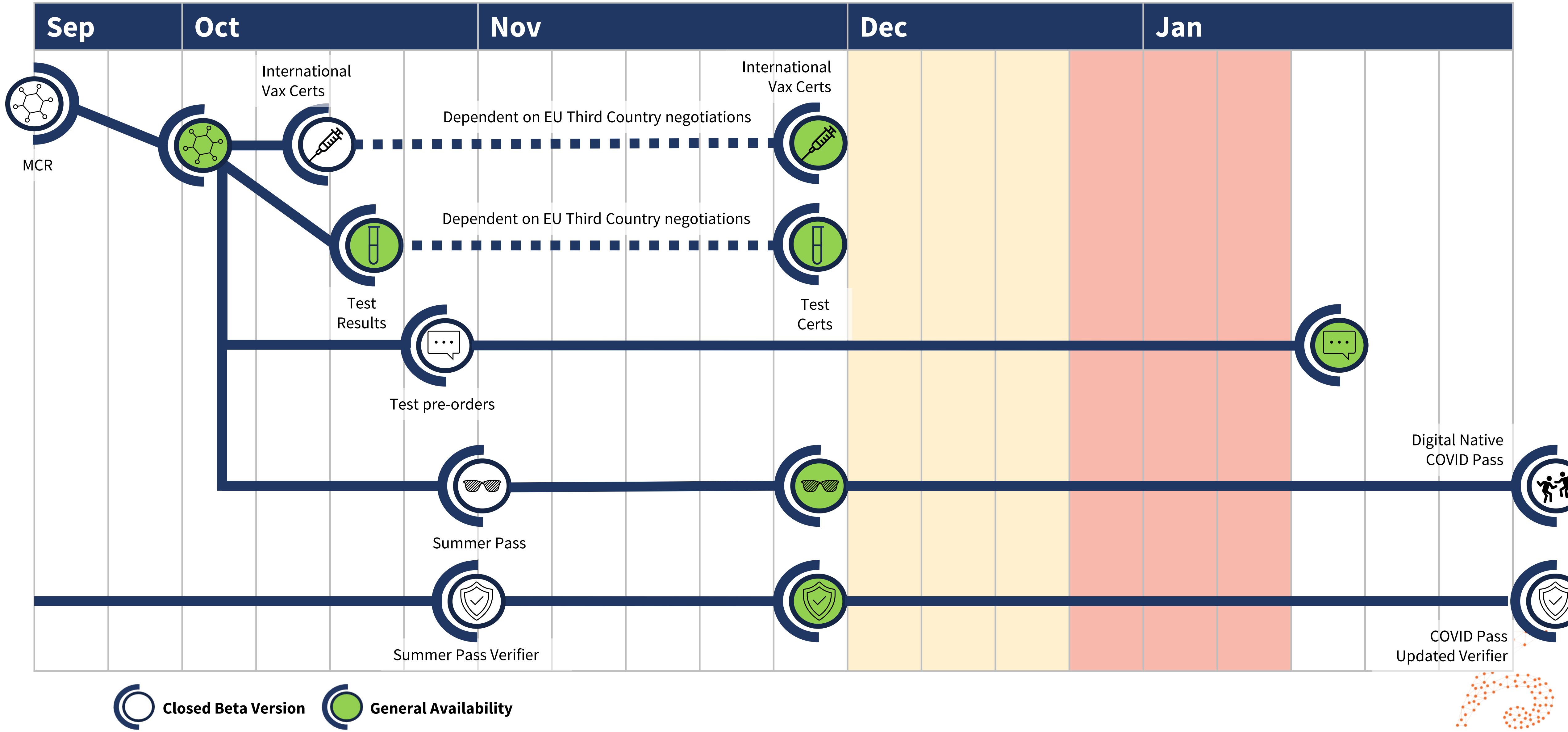
We could offer different requirements for different venue or event types or internal boundaries (e.g. fully vaccinated more than 14 days ago, vaccinated in the last 6 months, test completed in last 2 weeks, etc) but simple is better.

For Stage 1 it is incumbent on the verifier to confirm the identity of the consumer matches the details on the Pass. Stage 2 adds additional assurance and this step could be removed.

DRAFT – NOT GOVERNMENT POLICY

Document 8

Roadmap



Sep | Oct | Nov | Dec | Jan

MCR

International Vax Certs

Dependent on EU Third Country negotiations

International Vax Certs

Test Results

Dependent on EU Third Country negotiations

Test Certs

Test pre-orders

Summer Pass

Digital Native COVID Pass

Summer Pass Verifier

COVID Pass Updated Verifier

○ Closed Beta Version

🟩 General Availability

Document 8

Consumer experience – Stage 2

- The Stage 1 approach serves our immediate needs, but could be improved:
  - We can take advantage of our My Health Account and biometrics in the phone to remove the need for a consumer to have to provide a photo ID at the same time.
  - Further enhance privacy by allowing just-in-time disclosure of specific data to a verifier, while still having the certificate being digitally verifiable (known as Selective Disclosure).
- Both these features currently require that we develop a native smartphone app, and do not work for paper-based representations. This means they will only be available for digitally included cohorts.
- The supporting technology for this is complex, and while it works technically there's additional discovery work required to understand the UX implications and how we make it accessible to the general population.
- As we seek to reconnect New Zealand and eventually to run a containment approach and "flatten the curve" we will require greater automation and self-serve for management of people with Covid and at risk of Covid.
- Demand exists for self-serve capability for Covid services such as self isolation, contact tracing, daily health checks, test ordering and results, exemptions, adverse reactions and self-update of personal information.
- In this context Health would likely use My Health Account and My COVID Record to become the first and anchor implementation of the governments intended Digital Identity Trust Framework.
- There are strategic advantages in a generic Health App which has high uptake across the population. Longer term opportunities exist around population health services such as immunisations and screening.

MINISTRY OF HEALTH
MANATŪ HAUORA

Document 8

Visit our website to learn more

www.digital.health.nz

Document 8

Appendix 1: What about NZ COVID Tracer?

- NZ COVID Tracer is positioned as an **anonymous** digital diary for contact tracing. Accounts were removed in late 2020, and there are no strong ties to the identity of the user within the app.
- By their nature, health certificates require strong binding to a digital identity. This somewhat contradicts the privacy and anonymity stance of NZ COVID Tracer.
- We could implement a simple wallet, where you request the certificate outside app and simply use it as storage mechanism (fulfilling a similar function to the native iOS/Android wallets in Stage 1). This is the approach taken by the Republic of Ireland in COVID Tracker.
- However, when we get to Stage 2 we require an integration into My Health Account to be able to properly bind the certificate to a device. Doing this in COVID Tracer poses an interesting social licence question, would the public accept introducing a digital identity that requires an ID document to set up into COVID Tracer?
- There are additional developer rules that are levied by Apple/Google for apps that use Exposure Notifications, including restrictions on including personal details and strong identity binding. Some other countries have opted to implement vaccination certificates in a separate app due to this (e.g. NHS).

Document 8

Appendix 2: PKI and Trust - Technical

- Certificates are digitally signed to prevent tampering and forgery. Verifiers need to obtain an official public key from the issuer (Ministry of Health) to verify the signature is authentic.
- Providing a secure way for verifiers to get this public key is essential to establishing trust in the system
- health.govt.nz is a recognised and trusted domain name within New Zealand, and verifiers can be confident that information published on health.govt.nz domains is authorised by the Ministry.
- Each certificate contains a reference to a health.govt.nz web address that contains the public key corresponding to the private key used to sign the certificate.
- Verifier apps only download this public key if its comes from health.govt.nz, using a valid SSL certificate.
- This model leverages existing web security standards, and is a known and established technology pattern, reducing security and compliance efforts.

Document 9

From: Patrick Hindmarsh
Sent: Monday, 27 September 2021 9:55 am
To: s 9(2)(a)
Subject: Fwd: OPC Comments on Draft Domestic CVC paper

—
Patrick Hindmarsh
Principal Architect, Data & Digital
s 9(2)(a)

From: Jon Herries <Jon.Herries@health.govt.nz>
Sent: Thursday, September 23, 2021 7:21:10 PM
To: Jack Haddow <Jack.Haxxxx@xxxxxx.xxxx.nz>; Michael Dreyer <Michael.Dreyer@health.govt.nz>; Caroline Greaney <Caroline.Greaney@health.govt.nz>; Jane Hubbard <Jane.Hubbard@health.govt.nz>
Cc: Simon Ross <Simon.Rxxx@xxxxxx.xxvt.nz>; Selwyn Rimmer <Selwyn.Rimmer@health.govt.nz>; Patrick Hindmarsh <xxxxxxx.xxxxxxxxx@xxxxxx.xxxx.xx>
Subject: Re: OPC Comments on Draft Domestic CVC paper
Yep - we intend to pick this up with OPC - had planned to do it Tuesday but didn't pan out.

Simon - can you reach out please, and we will see if we can have a convo after tomorrow (when Michael gets a go/no go on the plan).

Jon

Jon Herries
Emerging Health Technology & Innovation | Data & Digital
s 9(2)(a) | jon.herries@health.govt.nz
Note: this came from a mobile phone so will probably have some spelling and grammatical error$

From: Jack Haddow <Jack.Haddow@health.govt.nz>
Sent: Thursday, September 23, 2021 5:29:26 PM
To: Jon Herries <Jon.Herrixx@xxxxxx.xxxx.xx>; Michael Dreyer <Michael.Dreyer@health.govt.nz>; Caroline Greaney <Caroline.Grxxxxx@xxxxxx.xxxx.nz>; Jane Hubbard <Jane.Hubbard@health.govt.nz>
Subject: FW: OPC Comments on Draft Domestic CVC paper
FYI

From: Liz MacPherson <Liz.xxxxxxxxxx@xxxxxxx.xxx.xx>
Sent: Thursday, 23 September 2021 5:06 pm
To: 'Kayleigh Wiltshire [DPMC]' <Kayleigh.Wiltshire@dpmc.govt.nz>; Shane Kinley <Shane.Kinley@mbie.govt.nz>; Gayathiri Ganeshan <Gayathiri.Ganeshan@mbie.govt.nz>; 'xxxx.xxxxxx@xxxx.xxvt.nz' <sara.mcfall@mbie.govt.nz>; '^MBIE: Karl Woodhead' <Karl.Woodhead@mbie.govt.nz>; 'Rachel.McLean@mfat.govt.nz' <xxxxxx.xxxxxx@xxxx.xxvt.nz>; 'Alastair Cameron [TSY' <xxxxxxxx.xxxxxxx@xxxxxxxx.xxxx.xx>; Shelley Tucker <s.tucker@transport.govt.nz>; 'Paul Fenton' <xxxx.xxxxxx@xxxxxxxxx.xxxx.xx>; 'henry.broughton@tearawhiti.govt.nz' <henry.brouxxxxx@xxxxxxxxxx.xxxx.xx>; Jack Haddow <Jack.Haddow@health.govt.nz>; Maria Cotter <Maria.Cotter@health.govt.nz>; 'jeet.sheth@ethniccomunities.govt.nz' <jeet.sheth@ethniccomunities.govt.nz>; 'Emma Spooner' <Emma.Spooxxx@xxx.xxvt.nz>; 'Sally.Wheeler@justice.govt.nz' <Sally.Wheeler@justice.govt.nz>; 'PTdutymanager@mpi.govt.nz' <PTdutymanager@mpi.govt.nz>; 'Maria-Laura Crespo' <Maria-xxxxx.xxxxxxxxx@xxx.xxxx.xx>; 'bronwyn.donaldsxx@xxxxxx.xxxx.xx' <bronwyn.donaldson@police.govt.nz>; '^Customs: Richard Bargh' <Richard.bargh@customs.govt.nz>; 'keene@tpk.govt.nz' <keene@tpk.govt.nz>;

Document 9

'matthew.gileone@mpp.govt.nz' <matthew.gileone@mpp.govt.nz>; 'xxxxx.xxxxxx@xxx.xxxx.xx' <laura.sommex@xxx.xxxx.nz>; 'Katie Anderson' <Katie.Anderson@crownlaw.govt.nz>; 'Jessica Gorman [DPMC' <Jessica.Gorman@dpmc.govt.nz>; 'Doogan, Hannah' <Hannah.xxxxxx@xxxxxxx.xxxx.nz>; Nick Wilson <x.xxxxxx@xxxxxxxxx.xxxx.xx>; 'James Gallagher [DPMC' <James.Gallagher@dpmc.govt.nz>; 'CHRISP, Sophie (CPCD' <Sophie.Chrisp@mfat.govt.nz>; Ephraim Wilson <Ephxxxx.xxxxxx@xxxxxxx.xxx.xx>; Peter Mee <Peter.Mee@privacy.org.nz>; Amy de Joux <Amy.deJoux@privacy.org.nz>; 'Jago, Rose' <Rose.Jago@tearawhiti.govt.nz>; 'Michael Sherwood [TSY' <Michael.Sherwood@treasury.govt.nz>; 'Ian Auld' <Ian.Auld@crownlaw.govt.nz>; 'teene@tpk.govt.nz' <teene@tpk.govt.nz>; 'olset@tpk.govt.nz' <olset@tpk.govt.nz>
Cc: 'Megan Stratford [DPMC]' <Megan.Stratford@dpmc.govt.nz>; 'Ruth Fairhall [DPMC]' <Ruth.Fairhall@dpmc.govt.nz>; 'Elizabeth Oxenham [DPMC]' <Elizabeth.Oxenham@dpmc.govt.nz>
Subject: FW: OPC Comments on Draft Domestic CVC paper

Kia ora Kayleigh me e hoa ma koutou

Thank you for providing the paper for comment, and for hosting the meeting on Wednesday this week. We appreciate the timeframes you are working to on what is significant and complex policy advice.

We understand that the proposal is for mandating the use of Covid-19 vaccination certificates (CVCs) at high-risk (as per public health advice) venues/settings as a condition of entry, while prohibiting requiring CVCs at 'basic human need providers' (such as supermarkets). All other settings will have discretion in the using CVCs. This considerable discretion poses an implementation challenge for businesses, which will have to undertake risk assessments of their own. There is a considerable risk of inconsistent application of these risk assessments, as well as an expected tendency of businesses to err on the side of caution (and potential commercial benefit) by requiring CVCs even if the public health/workplace health and safety argument does not stack up. This raises privacy concerns, which we consider below. We recommend that the Government considers drawing a **clear line on which businesses/settings will require vaccination status as a condition of entry, and which won't**. This would be the same clarity that Government has provided for mandatory record-keeping and the wearing of facemasks. Leaving it to most businesses to make this decision themselves, on the basis of guidance alone, risks widespread inconsistent application of the requirement, with attendant privacy risks.

If the government proceeds with the specific high-risk settings proposal, we recommend the model for domestic use of CVCs incorporates privacy at the heart of its establishment – that the system be designed from a privacy-protective point of view, rather than as an adjunct to implementation. This will be essential to ensuring that individuals can have confidence that their sensitive health information is not being misused, which is central to the social licence behind our Covid-19 response and recovery.

We have provided comments below to assist in the incorporation of privacy considerations into the policy and regulatory settings. These comments primarily relate to the proposal for high risk settings to require vaccination certificates as a condition of entry. The privacy implications change for the wider use of vaccination certificates, and we recommend that these are revisited with us if the requirement progresses beyond high risk settings. Having said that, we have considered this wider use in a couple of points below.

CVCs should employ a system that verifies an individual as 'Authorised' but does not share any other personal information

The paper notes at paragraph 45 that the Ministry of Health "encourages a largely anonymised CVC to manage privacy, for example a CVC that includes name, date of birth, date of second dose of vaccination and date and result of last COVID-19 test."

We support limiting the personal information on the CVC, in accordance with the principles of data minimisation. However, we believe the personal information listed is in excess of what is required to give effect to this policy. The CVC should limit the personal information being shared with event operators and reduce the risk that people who have a legitimate reason not be vaccinated are excluded from events, or required to explain why they are not vaccinated, which would involve sharing sensitive health information (e.g. disability, religious, or other reasons). **We therefore recommend the high-risk venue only needs to know that a person is Authorised to enter**. Venues do not need to know specific vaccination or testing information to discharge their responsibilities, even if this information will sit behind the Authorised status.

The paper and general terminology refers to Certificates, and sometimes domestic passports. Thought should be given to an alternate name that illustrates the CVC is about supporting Authorised entry.

CVC information should not be used for any other purpose and this commitment should be made explicit

We recommend that legislation and/or the regulatory framework is explicit that the CVC information will only be used for determining entry to a venue/setting and not be used for other purposes, including law enforcement. Overseas examples where information collected as part of the COVID-19 public health response has been accessed and used by law enforcement illustrate the importance of restricting use of the collected information in the

Document 9

legislative design; while a person may, for example, attend an event in breach of bail conditions, the collection is aimed at public health risk which could be undermined if the individual used someone else's credentials. There is also a real risk for scope creep in the use of CVCs, beyond the current policy rationale to reduce transmission risk at large, potential super spreader events (and potentially at other settings, where a public health and/or workplace health and safety justification can be made).

As the paper outlines, public trust and the social license is paramount. This would be supported by **prohibition on re-use** of information collected, so that individuals can have confidence their personal information will not be re-used for purposes other than entry to a particular venue/setting. This should include re-use for law enforcement purposes.

Large high-risk events should not collect or hold personal information

The paper does not specify whether a venue will be required to collect the Authorisation Record from the patrons, or keep a record as proof of compliance. The collection of personal information should be limited to what is absolutely necessary for the purpose of the CVC. Venues collecting and holding this information increases the risk of a privacy breach and the potential for misuse of personal information.

We recommend a solution is designed that does **not** require venues collect and hold the personal vaccination status of potentially thousands, (or tens of thousands), of patrons. If the system absolutely requires that venues collect info, the information should be limited and retained for the bare minimum period (as guided by public health advice).

Venues/settings may require individuals to provide identification to verify that the Authorised status is their own; as noted in our previous advice, clarity is required as to what businesses will be required to do to assure identity.

Requiring employees to be vaccinated

We note from paragraph 21 that MBIE is preparing advice for Minister Wood on a framework to use when considering reviewing vaccination requirements in the workplace. MBIE also mentioned on the call with agencies 22 Sept, that legislation changes would likely be required.

Requiring employees to be vaccinated is closely tied to privacy. An individual's vaccination status is personal health information and is subject to the protections laid out in the Privacy Act 2020. Under the current law, an employer cannot require their employee be vaccinated – or ask a person's vaccination status – unless for health and safety reasons, justified by a COVID-19 exposure risk assessment (or, if covered by COVID-19 Public Health Response (Vaccinations) Order 2021).

There seems to be a clear public health rationale at high-risk venues for requiring an employee to be vaccinated. It is less clear what the public health basis will be in other settings. We can envision a situation under the proposed model, where some employers will consider they can require employees to be vaccinated, or that businesses collect vaccination information, for purposes beyond public health (e.g. to promote their workplace as "fully vaccinated"). This would be a breach of the privacy of these individuals. We expect that a great many businesses will be tempted to take this approach, which could lead to the widespread requiring of vaccination status far beyond the policy rationale. If Government agrees to the proposal as drafted, then clear guidance and expectations will need to be communicated to businesses to ensure they operate in accordance with the policy intent and public health evidence. However, as noted above, we recommend that the Government provide absolute clarity on which businesses/settings will require vaccination status as a condition of entry, and which won't, rather than leaving it to businesses to determine through guidance.

Equity

To be justified on the basis of public health, any requirement to be vaccinated for employment or for access to a venue or service must be proportionate to, and effective in mitigating, the public health risk. However by mandating, or prohibiting, proof of vaccination as an entry (or employment requirement), government will, in some cases, cut across risk assessments carried out by businesses as to the risk posed by COVID-19. This raises a number of questions including:

- How will the safety of workers at, and visitors to, the limited set of "basic-human needs providers" be managed and assured? (noting that under the present proposal that PCBUs will be prohibited from imposing entry requirements based on vaccination status).
- Can PCBUs require vaccination for other purposes? (for example, when this is seen as being a competitive advantage, or is required by contractors);

We trust these comments are of use in your development of the paper and overall policy proposal – we are more than happy to provide clarification, or expand, on the points above. We look forward to seeing the final version of the paper and being updated on decisions by Ministers.

Ngā mihi

Liz

Document 9

Liz MacPherson (she/her)
COO and Assistant Commissioner – Policy and Operations
Office of the Privacy Commissioner Te Mana Mātāpono Matatapu
PO Box 10094, The Terrace, Wellington 6143
Level 8, 109 Featherston Street, Wellington, New Zealand
T +64 4 474 7590
M s 9(2)(a)
E liz.macpherson@privacy.org.nz
privacy.org.nz

Document 10

From: Patrick Hindmarsh
Sent: Tuesday, 28 September 2021 11:29 am
To: s 9(2)(a)
Subject: FW: Smart Health Cards and iOS 15.1

Thoughts?

Patrick Hindmarsh
Principal Architect l Data and Digital
s 9(2)(a) l patrick.hindmarsh@health.govt.nz
133 Molesworth Street, Thorndon, Wellington

Keep New Zealand safe with NZ COVID Tracer
Get your NZ COVID Tracer QR code

-----Original Message-----
From: s 9(2)(a)
Sent: Thursday, 23 September 2021 4:01 pm
To: Patrick Hindmarsh <xxxxxxx.xxxxxxxxx@xxxxxx.xxxx.xx>
Cc: s 9(2)(a)
Subject: Smart Health Cards and iOS 15.1

Hi s 9(2)(a)

Following up from our meeting this week:

1. Apple is currently strongly focussed on support for the Smart Health Card standard (smart http://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOJnhT3Btlg&u=http%3a%2f%2fhealth%2ecards%29 in the platform to delivery the best overall balance of user-experience, security and privacy.

2. Smart Health Cards are not priopretary to Apple - they are an open standard that has come out of the medical informatics industry in the US, and are supported in Apple Wallet, Google Wallet and Samsung Wallet.

3. The standard also can fall back from platform vendor Wallet support to supporting it in your own App , if there is an equity need for the broadest possble digital support across legacy mobile devices.

4. In addition, it supports both PDF and hard copy mechanisms for citizens who are either do not have a smartphone OR choose not to use one for this purpose. The standard is flexible enough that citizens can be emailed for MMS'd the smart health card, and we can ingest to Apple Health.

5. MOH can issue a smart Health card, with as little or as much information as it sees http://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOJu1TSlpkw&u=http%3a%2f%2ffit%2eYou can also take advantage of cards issued for international travellers once they are past border control.

6. The onus would still be on the entity reading the card, to ensure that the verified health record was issued to the identity of the human presenting it.

Document 10

7. No app needs to be installed on the citizen's device for this to work (if it can run 15.1) - they can ingest from PDF or hard copy via the built in camera into Apple Health, and as of 15.1, this will give them the option of generating a non-syncable, non-transferable wallet pass (of a new pass type - created specifically for this use-case).

8. Wallet support, vs app support is important for user privacy , as a digital wallet pass can be presented by a locked device, and their is no implied consent to search, as their would be handing an unlocked phone open to an App to say a Police Officer.

9. Note also, Apps on the device can read the health record (if the user gives them consent) and if they find the signing identify and data acceptable - generate derived credentials in a wallet pass that contain less sensitive info that the originating record.

10. Data Stored in Health is only accessible while the device is currently unlocked - in broad terms it is held to a similar level of assurance as what is required for RESTRICTED or PROTECTED data. Whilst ic can sync across devices logged in with the same AppelID, that is done using a set of asymmetric key pairs anchored in the devices so that Apple can not access the data.

They are digitally verifiable health records, tied in with standards asymmetric encryption keys to a digital signing identity, so the source of a particular card is attested to by a strong cryptographic hash. The two control points for sovereign control of information are the sining identity and the reader apps.

Any business logic that MOH NZ wants to apply as to which identities it wishes to accept for validity, can be accomplished by a reader App published by MOH on the whatever OS platforms it chooses.

Such a reader App can check the validity of any wallet pass, App screen, PDF image or hard copy smart health card. A reader App doesn't need to disclose the health data to its operator, if could simply display a green tick if the record presented passed the business rule requirements.

This means that something presented to say an police officer might present more information to the officer, than the App used to get entry to a concert.

We strongly feel that Smart Health Cards is the lowest effort, most equitable, and most broadly accessible mechanism for citizens to have proof of vaccination status and test results in their devices.

We note the work ICAO has done with VDS for national point of entry, and are watching adoption and developments of this carefully.

With respect to wallet passes:

A Generic PKPass can be generated by an App or a Web site. Passes can update dynamically from a web service - so things like rolling QR codes that change over time are feasible if the device has a network connection. PKPass generated from a web site will always be portable off the device, and can be shared with other people, and passes without any kind of verification mechanism such as a QR code or NFC interface are trivially forged. In addition, standard PkPass objects sync as files to all devices logged in tot h4 same iCloud account. Files that sync through iCloud are encrypted at rest and in transit, however they key material is under Apple's control, and thus we can access them under warrant. Putting PHI in a normal PKPass would normally constitute a disclosure event under most privacy legislation (and this is different for the non-syncing pass types built specifically for health information mentioned above)I note we have no part of our business model that involves accessing, reading or aggregating information in passes, beyond the sync functionality.

If a pass is generated on device by an App, then it is possible to generate asymmetric key pairs to anchor the pass to the device so it cannot sync or be copies. Happy to put you in contact with the Apple Pay and Wallet team here in Sydney to discuss the details on doing this further.

With respect to identity, noting we have public pilots for building access Student ID card and Driver's licences underway - we do not expect the Driver's Licence functionality to come out of pilot and be available in this region

Document 10

for at least 12 months, and potentially longer. Please also note that what we support is the ISO-18013-5 standard - this is a NFC read only mechanism, that does not include a visual representation of the physical card, and does not require unlocking the device.

References:

http://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOM6zFCw5xA&u=http%3a%2f%2fsmarthealth%2ecards
https://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOMHnSn1vlg&u=https%3a%2f%2fdeveloper%2eapple%2ecom%2fvideos%2fplay%2fwwdc2021%2f10089%2f
https://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOJy1Typtxw&u=https%3a%2f%2fdeveloper%2eapple%2ecom%2fnews%2f%3fid%3d7h3vwlh5
https://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOMjnTSlvlQ&u=https%3a%2f%2fdeveloper%2eapple%2ecom%2fdocumentation%2fhealthkit%2fsamples%2faccessing%5fdata%5ffrom%5fa%5fsmart%5fhealth%5fcard
https://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOJmzFXtsyA&u=https%3a%2f%2fdeveloper%2eapple%2ecom%2fdocumentation%2fpasskit
https://scanmail.trustwave.com/?c=15517&d=l4bN4ZISOXFIjj9hQOunmzjgXPeIVIvAOJuzTy1vwQ&u=https%3a%2f%2fdeveloper%2eapple%2ecom%2fdocumentation%2fwalletpasses

What I think I still owe you is:

- documentation on the iOS 15.1 wallet functionality, including to what extend this new pass type is available to your Apps
- Intro to Apple Pay / Wallet team if required
- any indication of 15.1 release timeframe

I’d suggest the most workable domestic strategy is as follows:

- adopt Smarthealth Cards as the record proving status of vaccination and test results
- Leverage the vendor provided capabilities for wallet integration on modern devices - Apple, Google and Samsung All support this
- Potentially: build a cross platform app for legacy devices > 7 years old that displays a smart health card on device if required
- Allow citizens the option of retaining a PDF or hard copy if they don’t want to use the wallet features or an App
- you MAY want to build apps that generate Wallet passes with less sensitive information in them that a DVHR
- NZ Govt would need to build one of more verifier Apps that implement the desired business logic as to what is accepted or not in terms of vaccination status. The more invasive ones might be only used by Government officers on Government issued , government managed devices, and not be available on the App Store.

cheers

s 9(2)(a)