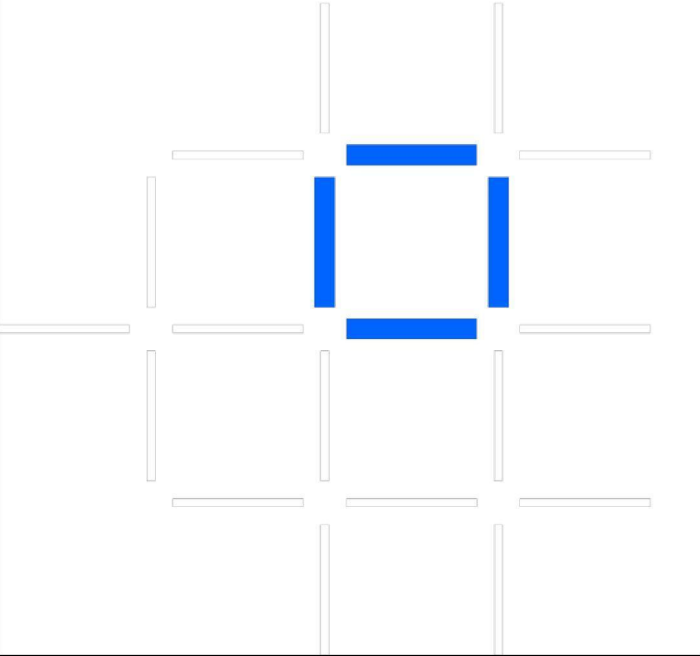


IBM Digital Health Pass

—
Enabling a proactive testing and clinical passport ecosystem



November 2020



According to a recent MIT study, for each recorded case of COVID-19, there are 12 that go unrecorded. Without a medical breakthrough, the total number of cases globally will climb to 200M-600M by Spring 2021.

You can catch it indoors, in crowds, or when people raise their voices. After the initial panic, many are becoming disenchanted and resistant. Masks help stop the disease, but some refuse to wear one because they see them as emasculating. Thorough hand-washing kills the virus, but who has not relapsed into bad old habits? Parties are dangerous but young people cooped up for months have developed a devil-may-care attitude. Most importantly, as the months drag on, people just need to earn some money. In Autumn, as life has moved indoors, infections are soaring.

You can contain the virus with three tactics:

- Changes in behavior
- Testing, tracing and isolation
- Lockdown

We no longer want to be chasing cases. We want to get ahead of the cases.

Source: [MIT Management Sloan School: COVID-19 cases are 12 times higher than reported](#)

What is IBM Digital Health Pass?

Local governments are re-opening communities and lifting stay-at-home orders, which means people are starting to return to their “new normal”. Digital health passports are emerging as a technology solution that enable individuals to present their health status so they can return to a physical location, such as a workplace, school, stadium or airline flight.

Digital Health Pass is IBM’s platform for the integration of test certification, permissioned data sharing and analytics across multiple parties, allowing governments and organisations to manage the wellbeing of individuals and take a data-driven approach for the safe return to work, travel and entertainment.

- **Privacy-first** approach, while providing secure access, traceability and auditability
- Designed to **support proactive testing** (asymptomatic)
- Supports **multiple test types** (antigen, antibody) as well as upcoming **vaccines**
- Provides **aggregated, anonymized data** on the tested population which can be analysed in real-time, while individual data remains on personal devices
- Enables individual-controlled **consent-based data sharing** with a third-party verifier
- Allows for decision-making based on aggregated test data, allowing for **targeted management** of identified outbreaks



We are engaged with:



The Challenge

Facilitating the return to normal requires knowledge of the status of individuals

- 1 Self assessment – *valid for 12 hours**
- 2 Temperature – *valid for 24 hours**
- 3 No live virus – *valid for 1-4 days**
- 4 Live virus antigen present – *valid for 1-3 weeks**
- 5 Antibodies present – *valid for 3-12 months**
- 6 Vaccinated – *valid for 1-3 years**

How do you keep track of all this?

*all purely illustrative

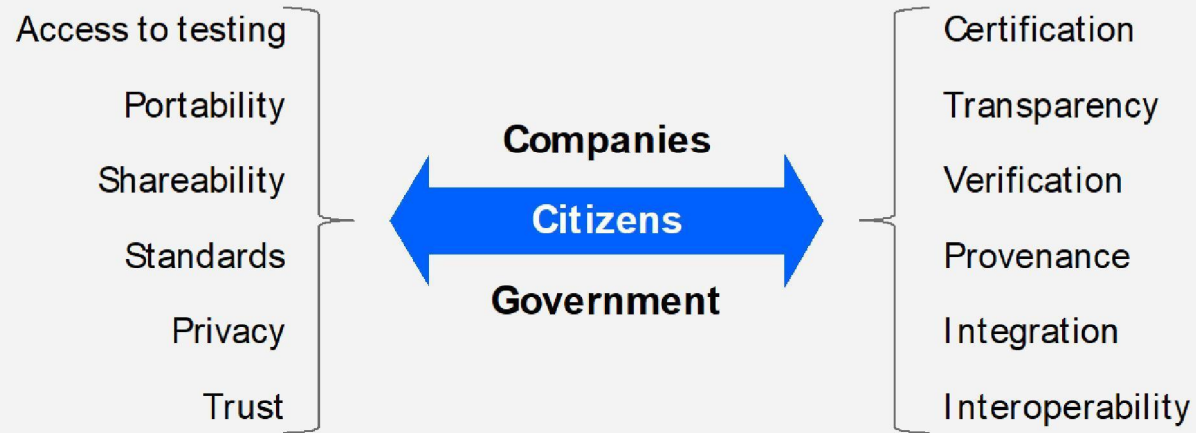


Proposed Solution

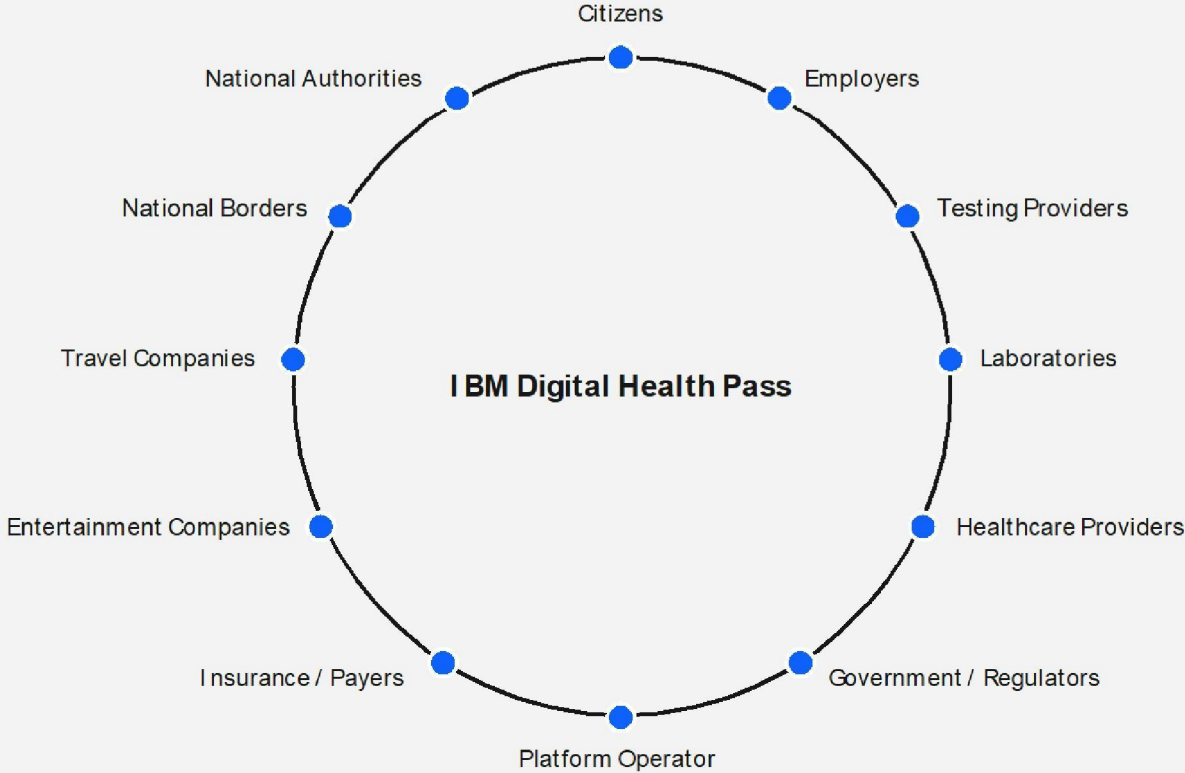
We are proposing a **digital** smartphone user interface, with a **secure** blockchain distributed ledger backend which will provide **immutable** provenance for conducting the test, an immutable set of test records, and the ability for the holder of the test to both **view** and **share** their results using the smartphone user interface with anyone that needs to **verify** their **test certificate**.



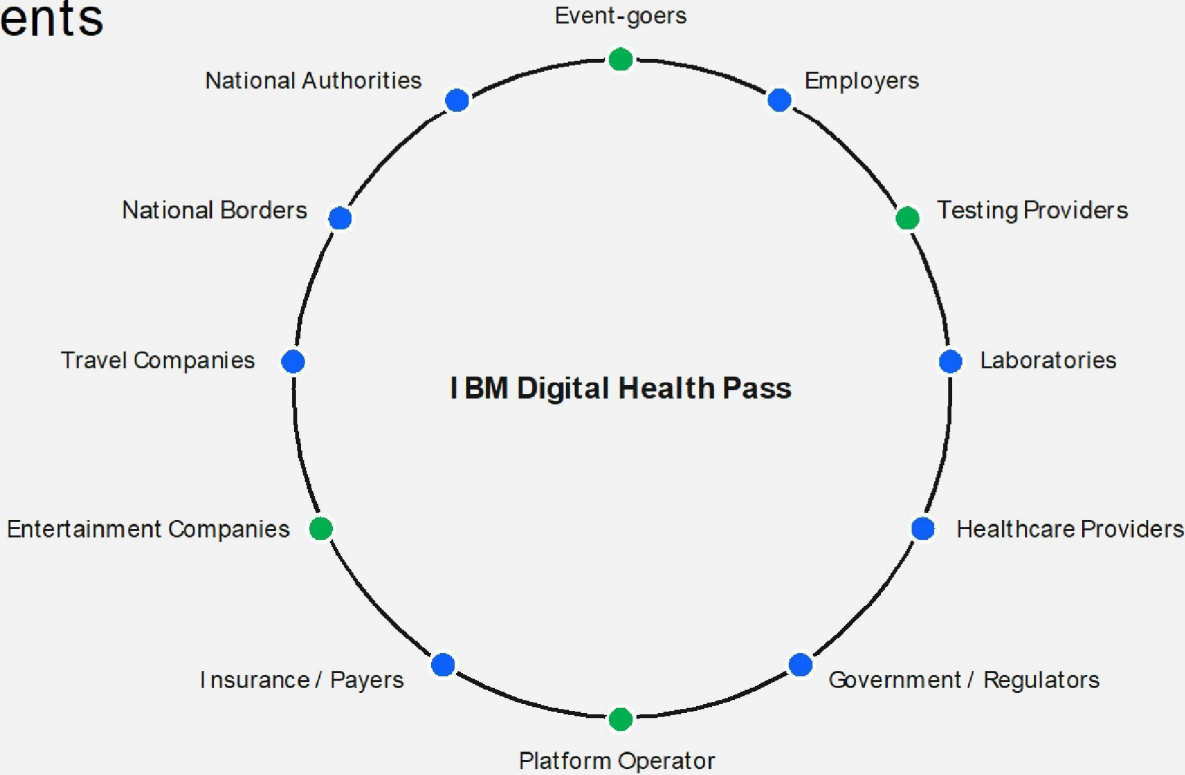
Unmet needs and the role of technology



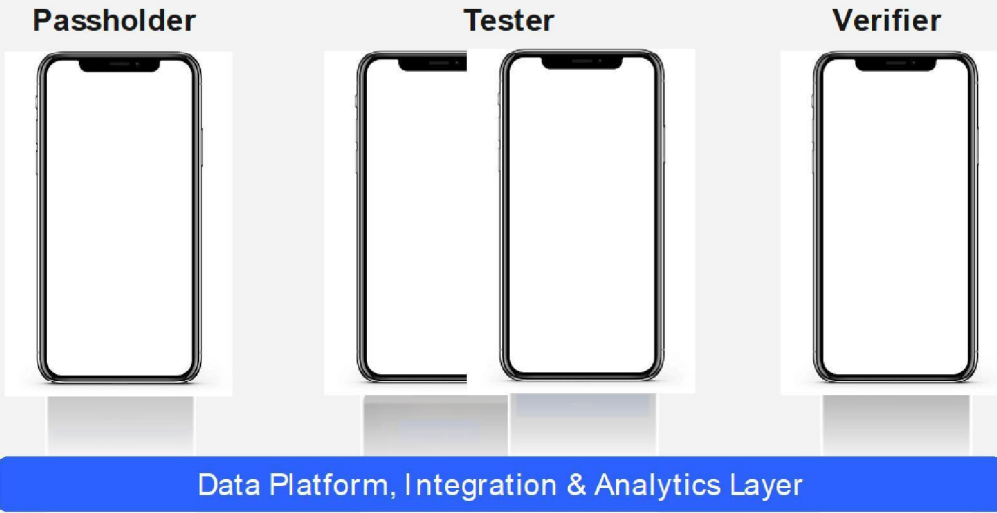
Ecosystem Parties



Indicative Ecosystem for Events



Core components of Digital Health Pass



Flexible data model

Mobile

API-centric

Scalable

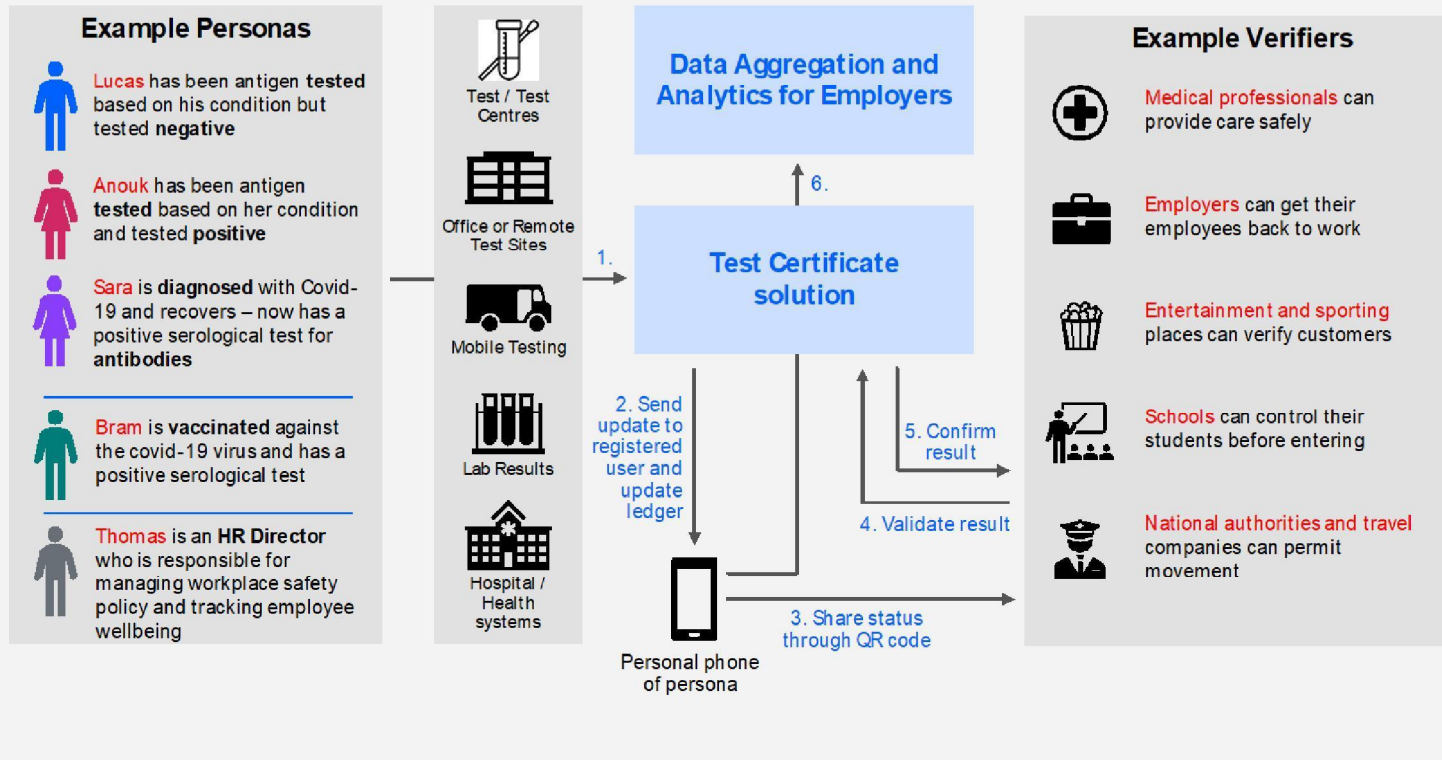
In-use today

Multiple tests / Certificates

Integrated with testers

Data Aggregation

How the Test Certificate service works



Example Journey



Our Personas



Passholder



Test centre clinician



Lab technician



Verifier

High Level User Journey



Invitation

A passholder receives an invitation to be tested and downloads the testing passport app to their phone. The app generates a secure digital testing passport.



Test

At the testing centre, a physical test is linked to a user's testing passport in the ledger. A test sample is taken and the passholder leaves the centre.



Results

When the test is complete, it is scanned and the results are written to the ledger. The passholder receives a notification that their new results are ready.

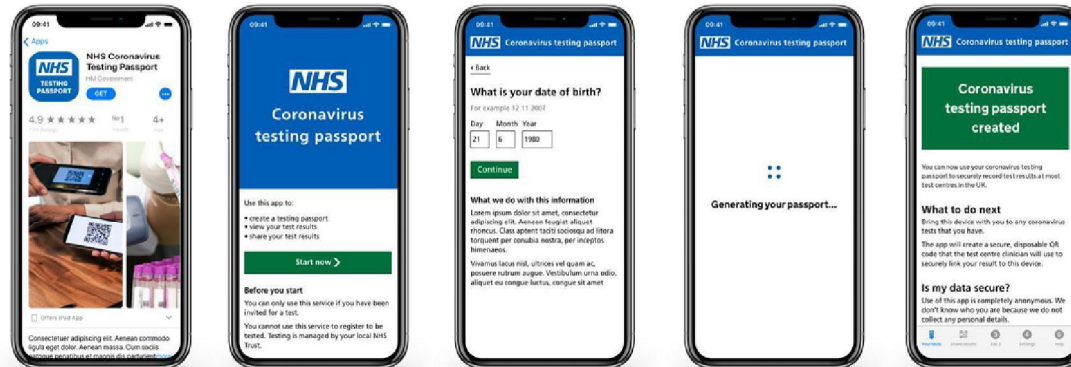


Verification

Passholders can create secure, one-time QR codes within the app. A verifier scans one of these codes to see verified test results, enabling the passholder to return to work.

Invitation

John receives an invitation to get tested. The invitation includes instructions for visiting the testing centre and an app to download.



The invitation

The invitation explains that the app will be used as a passport to hold and view his test results, and to notify him when new results are ready.

Getting the app

John downloads the app. He provides his date of birth but no other identifying information. Only his date of birth and a unique private key are sent to the ledger.

Creating the testing passport

The app talks to the ledger and generates a testing passport for him to store his test results. He now has a secure place to store his results.

Test

John arrives at the testing location. Staff check his photo ID and use an existing process to check his eligibility to be tested.



Identification

John uses his testing passport app to generate a one-time QR code. This code allows his testing passport to be linked to the test that's about to be performed.

Security

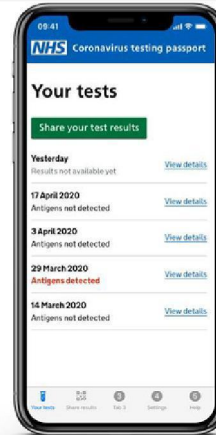
A clinician who's signed into the system scans John's one-time code and enters his date of birth. These are checked against the ledger to ensure authenticity. The clinician prints and attaches a unique ID to a new testing kit.

The test

A sample is taken from John. He leaves the test centre and goes home. The test sample follows its normal process through the lab.

Results

John is eager to receive his result as soon as it's ready so he can get back to work.



Logging the result

Lab staff conduct the tests following their normal process. Once a result is available, a technician signs into the system, scans the test and enters the result, securely and permanently writing it to the ledger.

Notification

John instantly receives a notification telling him that a new test result is ready. He uses Face ID to unlock the app and view his latest test result.

Test details

John can see a history of all the tests that have been attached to his anonymous ID. He can view more details about any of the tests.

Verification

To ensure workplace safety, John's employer needs to verify test results for every employee.



Returning to work

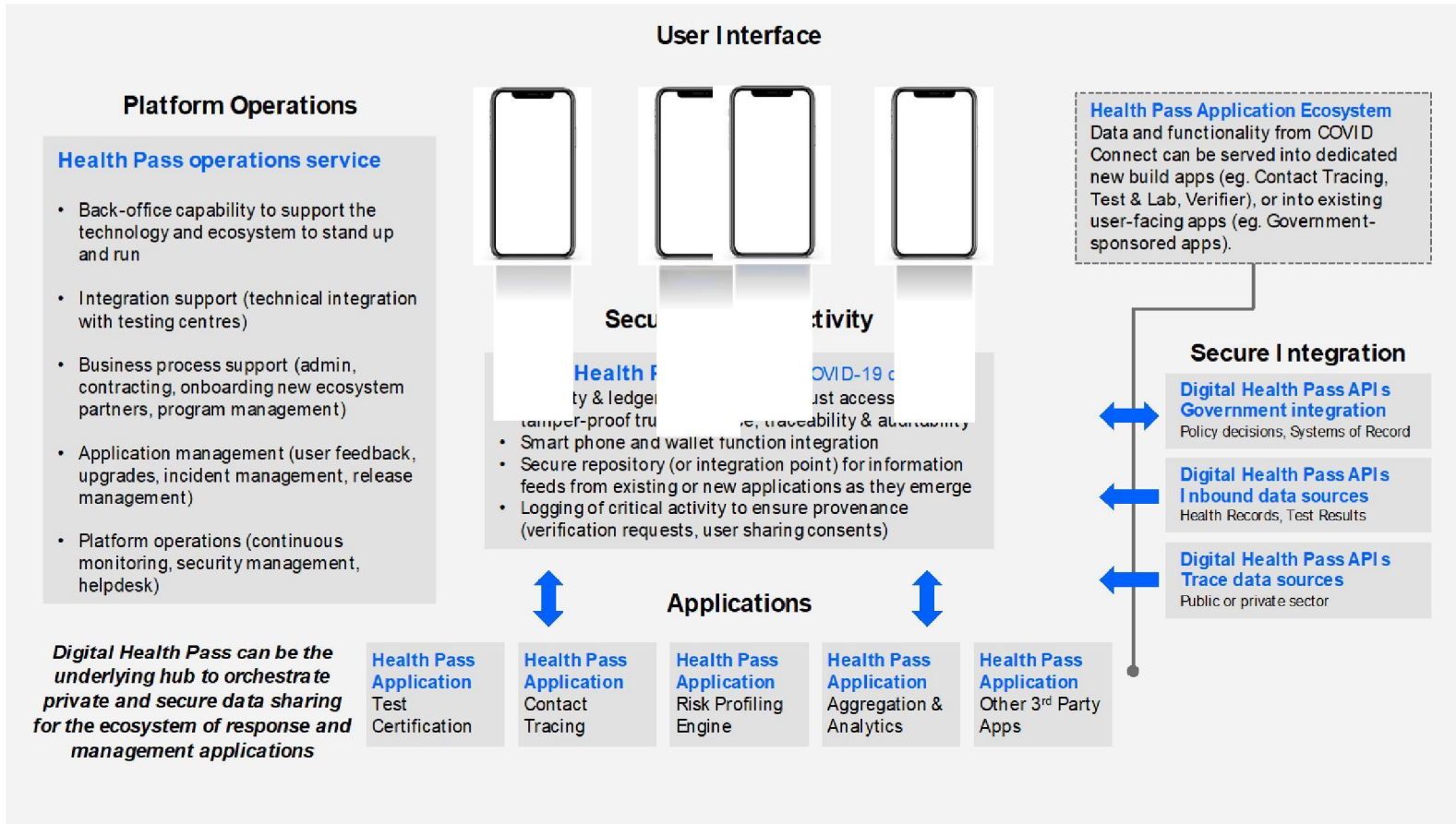
When John arrives at work, he's asked to share his test results. He uses the app to generate a secure, one-time QR code that's written to the ledger. He shows this to the verifier along with his photo ID.

Viewing the results

The verifier at John's workplace scans the one-time code and enters John's date of birth. These credentials are checked against the ledger and if they match, the verifier is shown John's test results. The one-time code is invalidated so it cannot be used again.

Making a decision

The verifier is shown a version of John's results that has come directly from the ledger, so they can be confident that the data is verified and complete. They make a decision based on the latest government guidance.



Multi-application source of input

The aggregated data model enables combined COVID risk information and pan application warnings with appropriate anonymity

Testing Application

Field	Value
Id	38656088564
Test type	PCR
Test code	NR-9973
Sample type	nasopharyngeal
Sample time	2020-05-17T10:06:45.000Z
Result time	2020-05-18T10:06:45.000Z
Test center	5967847
Result	Positive

COVID Connect
aggregated data model
(superset of all source application data input)

Self Reporting Questionnaire
Risk exposure

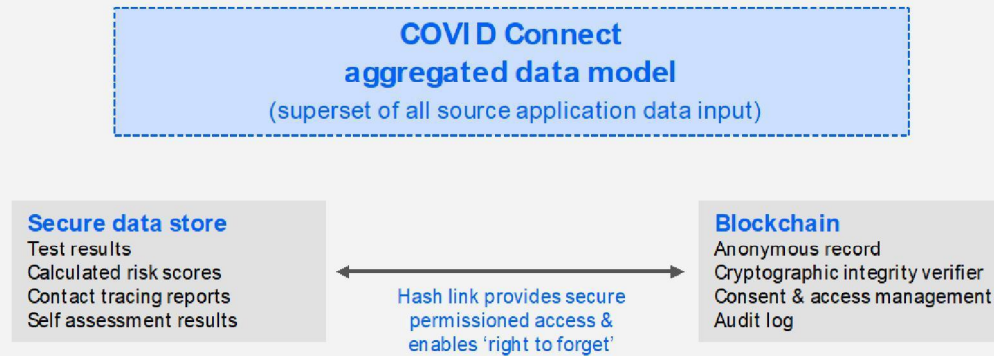
Contract Tracing App
Exposure score

Risk Analysis Engine
Reports

Personal and private information



Secure Aggregated Data Model

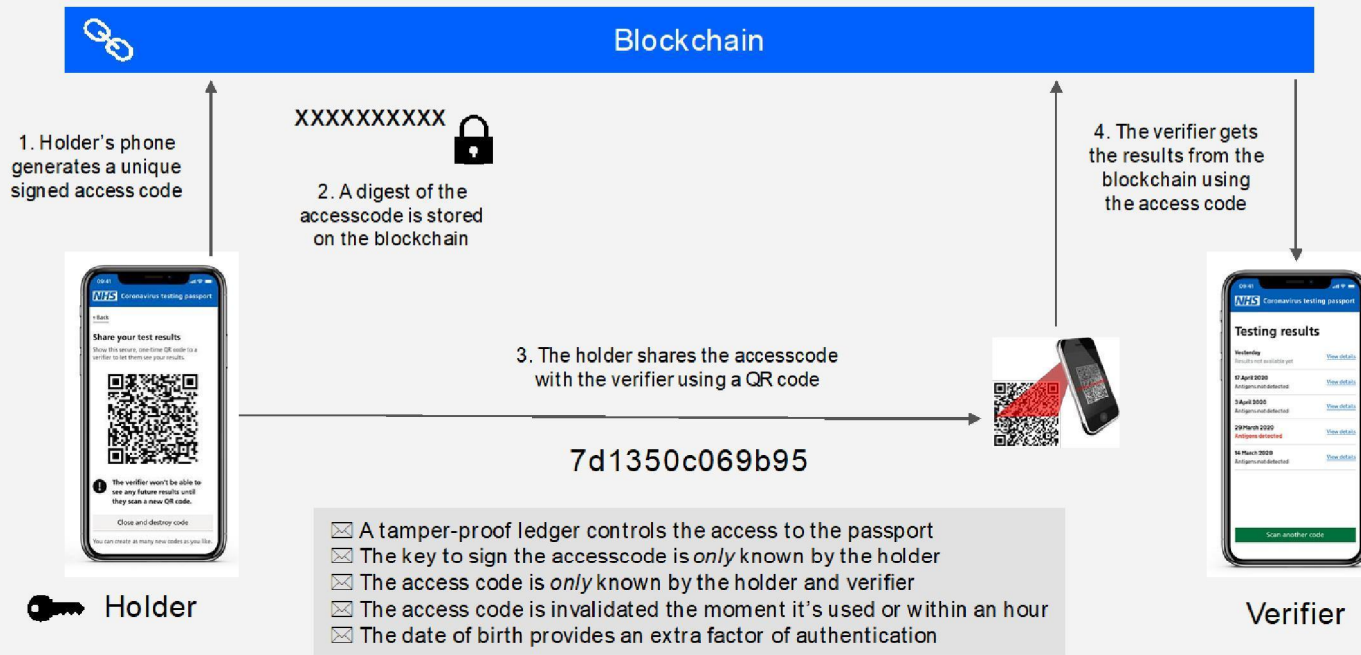


- All content is stored in secure stores of trusted data
- Enables use of both anonymised data, & ability to support GDPR needs
- Steward organizations, only accessible when permissioned through the blockchain

- The user controls access to their anonymous record, using the blockchain as a tamper-resistant consent management system

Meeting the information needs of citizens with blockchain provenance for auditability and security

Secure Data Encryption



Functional Scope

- Develop a **decentralised** technology platform, with **centrally managed governance**, to scale TTT quickly whilst ensuring security and privacy.
- Establish an **assured process for employee testing** to minimise risk of fraud and allow for commercially viable scaling to a national level.
- **Enable permission-based data sharing** including test and trace between employees and employers, and other external 'verifiers'.
- **Aggregate anonymised data** on the workforce population to allow for employer health tracking, while individuals' data remains on phones.
- **Enable analytics and 'next best action'** aligned with Government policy and advice to generate personal risk scores
- Develop a **front-end which drives engagement** – considering gamification of risk scoring and enabling individuals to self-serve relevant care information.
- Enable a **service that supports the digital infrastructure** to manage user and organisational engagement, integration and technical support.
- Establish **clear governance principles** for the platform and all participants (IBM, diagnostics companies, technology companies, Governments, etc.)

Emerging requirements from Employers

- **Daily risk scoring** mechanism ("Am I safe to come to work today?")
- **Workforce analytics** to monitor and track wellness of employees over time
- **Proximity tracing** within the workplace (both between employees and customers / clients)
- Ability for employees to share **test data** to inform risk scoring
- Government '**code of conduct**' to employers for how to apply risk scoring fairly
- **Consent management** for data sharing between employee-employer
- **Data privacy and GDPR compliance** (personal data or health data not to be held on employer systems)

Secure Data Encryption

Core MVP Delivery Team

An experienced team that has been working on delivery of Digital Health Pass for the past 6 months.

Leveraging IBM's Knowledge of T&T

Interlocking with our T&T colleagues will help us to accelerate design, architectural, people or policy issues as we progress.

Program Governance

We will govern MVP and post-MVP scaling through existing programme governance we have put in place for T&T.

MVP – Speed, agility & alignment

- Mobile Development
- Integration
- DevOps
- Security
- Test

IBM can scale from a pool of technology delivery expertise to support specific feature, platform or infrastructure requirements.

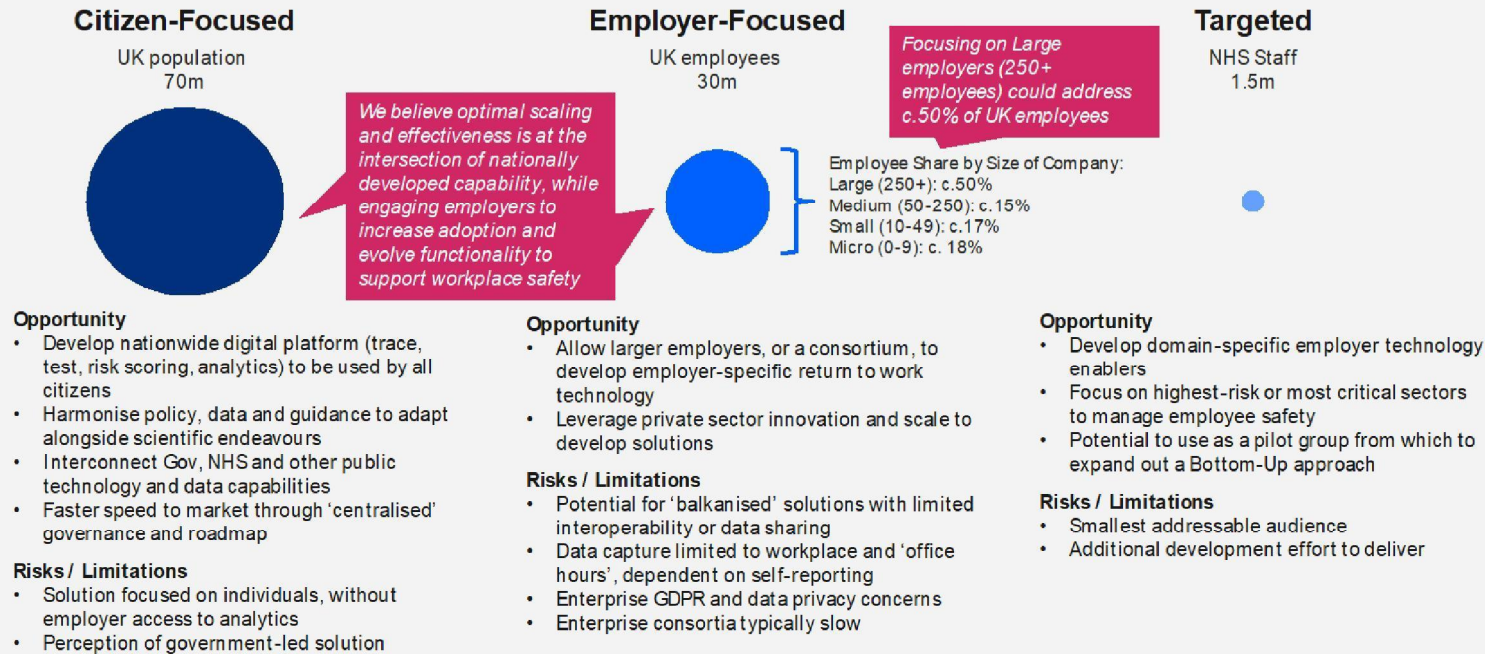
Platform Operations and 24/7 Support

Support for Digital Health Pass at scale can be integrated into IBM's wider support model.

Post-MVP – Scale, expertise and support

Reference: Scaling National Return to Work solution in the UK

Enabling return to work with technology could be addressed 'Top Down' (Gov-led) or 'Bottom Up' (Industry-led). We see that engaging industry can be an accelerator in terms of data collection and adoption but Bottom Up has scaling challenges.



Reference: Scaling National Return to Work solution in the UK

In all scenarios, it is foreseen that Government provide the majority of Return to Work applications (and supporting guidance) although employers could choose reduced-functionality tracing capability if employees don't opt-in to a national solution

Top Down

Government Led

Government provides a suite of applications and tools to support return to work, that is appropriate for both citizens and employers

Bottom-Up

Employer Led with Gov't Endorsement

Employers develop workplace-specific trace (and in a few cases testing) solutions to help manage their own workplace safety.

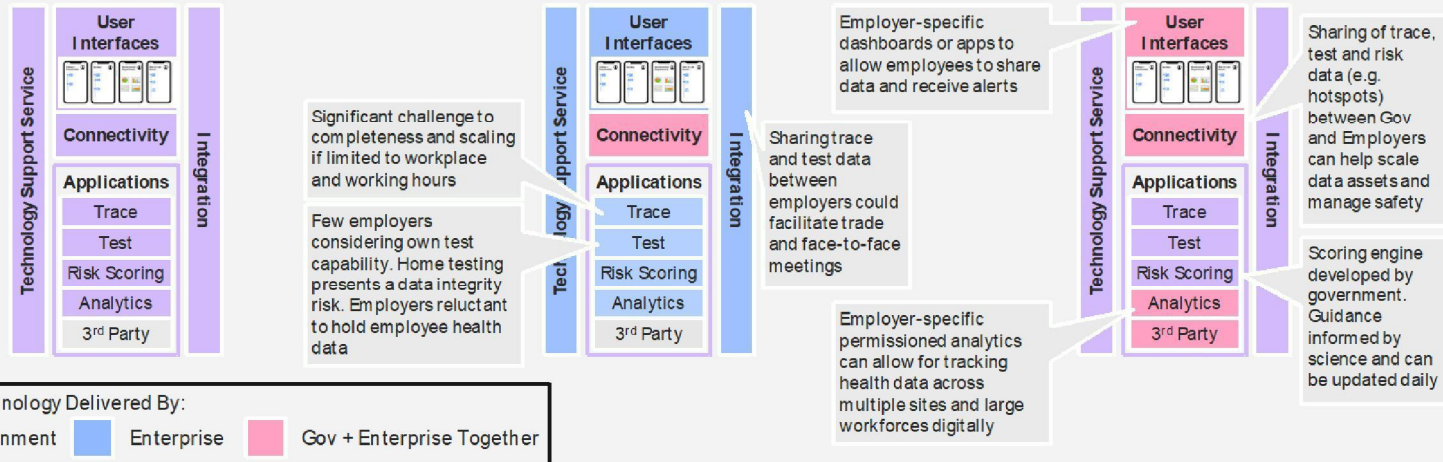
Connectivity between employers and NHS (e.g. test certificates) could increase test integrity.

Collaborative Top Down

Gov't Led, with Employer Engagement

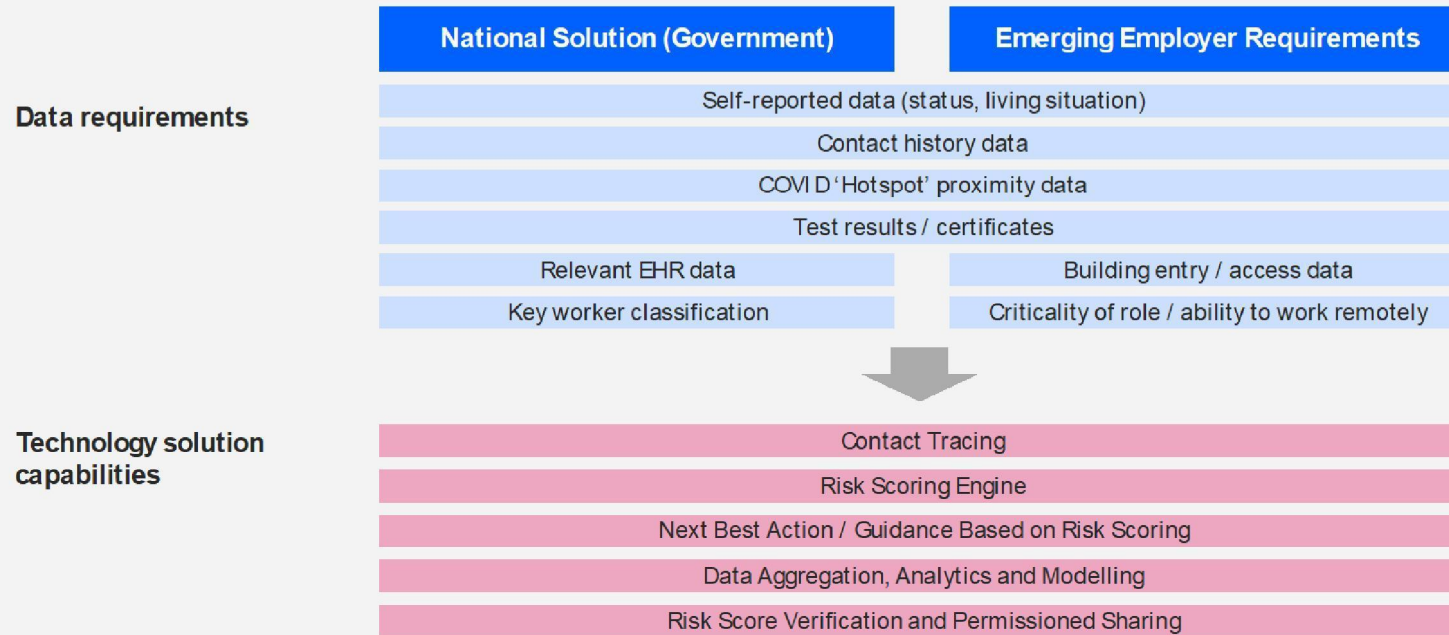
National trace, test and analytics applications form the basis of the solution set, but with specific applications developed for employers (e.g. trace only during working hours)

Multi-national companies could support interoperability with other countries.



Government and Employer Requirements

There is significant **overlap of the data and technology enablers** that can support both Government and employer management of the Return to Work – an ‘employer solution’ could be a sub-set of the functionality deployed for citizens.



More Materials

IBM Digital Health Pass

IBM Digital Health Pass is currently under limited availability. Schedule a demo to learn more and get started today.

Schedule a demo Read the blog

Looking for a workplace specific solution?

Work safer, work smarter and help guard the health, safety and productivity of your people in a changing workplace.

Explore Watson Works

Supporting the exchange of an individual's health status

As individuals may need to present their health status to return to public places, organizations are looking for solutions that can help substitute the risk of COVID-19 while protecting privacy.

Powered by IBM Watson, IBM® Digital Health Pass is designed to help organizations verify an individual's health status while protecting personal privacy. Individuals can manage their information through an encrypted digital wallet on their smartphones and control what they share – and for what purpose – while

Let's talk

IBM Digital Health Pass puts privacy first

As people may need to present their health status to return to public places, organizations are looking for solutions that can help substitute the risk of COVID-19 while protecting privacy.

IBM Digital Health Pass is designed to help organizations verify an individual's health status while protecting personal privacy. Individuals can manage their information through an encrypted digital wallet on their smartphones and control what they share – and for what purpose – while

Micro-site

High level overview of the IBM Digital Health Pass proposition, value statement, and legal-approved go-to-market narrative.








<https://www.ibm.com/products/digital-health-pass>

Blog

Social-ready overview and description of why Health Pass and IBM are the right partner to work with in this space.

<https://www.ibm.com/blogs/watson-health/health-pass-puts-privacy-first/>

We are using this technology to deliver similar capabilities

Who	What	Ecosystem	Scale
			<ul style="list-style-type: none"> • 60% of global container volume • 1.5B transactions in 12 months
			<ul style="list-style-type: none"> • 270 members worldwide • 17,000 individual products tracked
			<ul style="list-style-type: none"> • 14 Global banks • High value, cross-border transactions

Thank you

