TONY BLAIR
INSTITUTE
FOR GLOBAL
CHANGE

Digital Identity: The Missing Piece of the Government's Exit Strategy

ANDREW BENNETT

Contents

Published at https://institute.global/policy/digital-identity-missing-piece-governments-exit-strategy on June 9 2020

Executive Summary

As governments face growing pressure to give people back more freedom, they must do so while suppressing the virus and without a vaccine. Yet countries risk exiting lockdowns without the comprehensive containment infrastructure needed to do so safely. While testing and contact tracing have had at least some, albeit questionable, attention from government, the crucial role of digital identity has been completely lost in the debate.

Digital identity infrastructure is a fundamental part of making sure government delivers for citizens in the 2020s. For Covid-19 specifically, it provides leaders with the optionality required to navigate an unpredictable, evolving situation. This infrastructure also presents sensitive governance challenges that leaders must address for it to succeed. This briefing therefore sets out:

- How digital identity can help to tackle Covid-19
- What an optimal system should look like
- The fault lines for public consent
- What's needed to move from debate to delivery

In summary, governments should:

1. **Implement a mobility credential linked to a secure and user-centric digital identity to allow the safe reopening of close-proximity spaces.**
   a. Adopt a secure and user-centric model of digital identity that puts individuals in control and protects their privacy. For users this would most likely mean a biometrically secured app on their phone that stores digital credentials.

   b. Create a platform to securely issue credentials based on test results. For example, someone would present their digital ID when being tested; a unique credential based on their results would then be sent to their app.

   c. Agree internationally interoperable standards for credentials so that they can be widely recognised by a range of organisations. When required, users would present a mobility credential on their app to be scanned and verified.

   d. Set out a technical, legal and liability framework for identity providers, credential-issuing parties (e.g. testing labs) and verifiers to accelerate delivery.

2. **Set the right framework for how credentials are used in practice, in order to secure broad-based public support.**
   a. For public settings, enforce access based on a mobility credential in the highest-risk settings first, e.g. care homes and airports. As rapid point-of-use tests become more available, credential-based access can become more widespread.

   b. For private settings, e.g. offices, use credential-based access as the condition for increased occupancy rates. The right to ask people to show a mobility credential should be limited to those authorised to secure such settings.

   c. Prevent anyone from being compelled to share a mobility credential outside of these settings except by the police. Similarly, the power to issue penalties for failing to show a credential should be limited to official authorities and only when strictly necessary.

   d. Ensure that a digital-identity platform and mobility credential remains independent of any digital contact-tracing efforts, unless users opt in to linking their data.

Delivering a national, interoperable digital-identity platform and getting the necessary governing framework in place will require primary legislation. It will also require political sponsorship from a senior minister to marshal the different parts of government towards a common goal.

How Digital ID Can Help Tackle Covid-19

While most of the debate about suppressing the virus has focused on mass testing and contact tracing, these measures only come into force after an infection. This leaves many high-risk or close-proximity spaces, which should only be accessible to recovered or uninfected people, exposed. This is the role for digital identity.

In the UK, identity has long been a politically fraught issue. But Covid-19 presents a use case that is fast racing ahead of policy. Care homes, airports and other settings need a way of checking that everyone who enters is safe to do so. Failing to meet this need will only lead to abuses of power and loss of privacy. It is far better, for example, for border control or other gatekeepers to scan a secure QR code issued by a verified health authority than to probe individuals' entire medical history before letting them through.

As we have set out elsewhere, governments must therefore ensure that any mass, rapid testing regime also confers a mobility credential: a biometrically secured digital code (e.g. a QR code) stored on a person's phone. Individuals would then present this code when entering specific settings. Different credentials would be issued depending on the type of test received, in turn conferring different privileges on recipients:

Table 1 – Mobility credentials generated by Covid-19 tests

Basis for credential	Permits travel + access to settings	Further testing and tracing
Lab-based, positive antibody test	Yes, at least medium term, possibly permanent	Exempt, at least medium term
Point-of-use, negative antigen test	Yes, temporary	Still participates

If the lab-based credential is like a passport, the point-of-use credential is more like a visa. This helps to avoid retesting people unnecessarily several times a day, such as when coming and going from an office, without exempting them permanently. It would be for authorities to set out when credentials expire (e.g. over time, or after visiting multiple locations), but a digital system allows for this flexibility in a way that a paper-based system could not.

Some have questioned whether governments should hold off on moving forward with mobility credentials until there is both a credible means of testing for immunity and proof that it is long-lasting and generalisable. But the different types of credentials highlight that the fundamental use case is to assess who can travel or access certain settings, not who is immune *per se*. If antibody tests don't work, or governments can't reach the necessary capacity to test at scale, rapid antigen testing can at least plug some of the gap and change the risk calculus for navigating the new normal. A digital credential could also be issued to all key workers, if authorities wished, or generated after vaccination, in time.

What Good Looks Like

States that already have a modern identity infrastructure have a head start in issuing mobility credentials, since these can be associated with specific individuals relatively easily. For others, it is helpful to set out what the basic user need and user story should look like. Crucially, the system must meet the needs of individuals, verifying parties and governments:

Table 2 – User stories for an optimal Covid-19 digital ID solution

Need	For individuals	For verifying parties	For governments
Authentication	• I download a digital wallet app and register a digital identity, generating a secure QR code • I provide my QR code to be scanned before receiving a Covid-19 test, to link results to me only • A mobility credential, verifiable via a QR code, will automatically be pushed to my digital wallet app after a positive antibody/ negative antigen test • Credentials are stored on my phone in a digital	• I can protect environments by easily checking whether an individual is permitted to access a given setting (e.g. care home, airplane)	• I create a platform that addresses the needs of private orgs and government labs to issue digitally signed credentials without taking on extra complexity • Companies and labs can easily register and create a digital signature to automate this after test results are automatically shared with the platform

	wallet		
Privacy	• I can present a mobility credential asserting my permission to access controlled settings without revealing any other personal data • I know that the identity provider will only retain the minimum data required to reissue credentials if I need a backup • I have control over my records and how they are used	• I cannot access any other information about an individual other than their mobility status	• I have set high privacy and ethical standards that identity providers must meet to provide services to users • I cannot track or identify individuals without their consent
Security	• I know my test records and credentials are accessible only by me and biometrically secured (e.g. by a photograph or fingerprint)	• I trust that QR codes are secure, fraud/ tamper-proof, and can only be issued to specific individuals	• I have set high security standards that identity providers must meet
Inclusion + ease of use	• I know if I do not	• I do not need	• I have set out

	own a smartphone/ device I can still participate, e.g. via SMS, connected smartcard or a printed code	any new hardware to verify credentials • I am not required to enter any information twice	accessibility requirements to full inclusion, accepting the cost of this is slight increased potential for fraud

In practice, this could work along the following lines:

1. **Registration:** Users would install a digital wallet (usually an app) on a device they already trust. They would register their identity through this app, secured using a biometric identifier such as a photograph or fingerprint. The wallet would start off empty, with only a self-generated public and private keypair. Users can share their public key via a QR code; any credentials subsequently encrypted with this code can only be accessed by them. Personal data is stored on the phone and not on a central server operated by government or another organisation.
2. **Authentication:** Authorities create a government platform to issue mobility credentials automatically, addressing the needs of testing parties (e.g. NHS labs and offices conducting point-of-use tests) without requiring them to take on extra complexity. These parties pre-register with the platform to generate a digital signature so that any credentials they issue can be trusted. In turn, users provide their QR code containing their public key for scanning before being tested, so that any mobility credentials arising from the test are issued uniquely to them. Testing parties encrypt mobility credentials with this public key and share to the government credentials platform, which automatically issues digitally signed credentials to the specific user's digital wallet.
    - Managing this backend via a platform helps to avoid increasing the burden on testing facilities and individuals alike, but broader applications of digital credentials should rely on organisations issuing their own credentials to prevent centralisation.
    - A digital, encrypted system also ensures that the credential is non-transferable. In comparison, physical documents are routinely stored, copied or transcribed in ways that take data outside users' control, creating opportunities for theft or fraud. A physical approach, such as a printed QR code or connected smartcard, should therefore only be reserved to promote digital inclusion while

minimising fraud risks.

3. **Verification:** Users share this digitally signed credential with third parties via a scannable QR code when entering a restricted setting. To prevent people from screenshotting and sharing codes with others, QR codes would have to be unlocked via a biometric check (e.g. fingerprint or selfie) and would refresh regularly to prevent fraud. For verifying parties, they would scan this QR code simply using a smartphone or other device (e.g. the tablets already used in many offices to register visitors), with each scan calling the government platform API to ensure the issuer's signature is authentic and up to date.
4. **Updates:** Credentials must be tamper-proof by individuals but amendable by health authorities, e.g. if immunity is proven to last longer or shorter than originally understood. A digital, platform approach allows government to control updates and make them automatically in one swift move, rather than every testing lab or office having to issue new credentials separately. This ensures that trust settings are appropriately protected and continuous rather than time-limited.

The Fault Lines for Public Consent

Digital identity infrastructure provides leaders with the optionality required to be responsive to an ever-evolving situation. But building a technical system is only half the challenge. Initially people accepted that comprehensive lockdowns were necessary to suppress a virus over which we otherwise had no control. In contrast, digital identity systems facilitate granular, personalised restrictions that governments *do* control and which represent a break from mostly universal measures that have been implemented so far. If new digital-identity systems are perceived by the public to be unfair, they risk undermining the collectivism required to beat the virus more broadly.

Leaders must therefore ensure that digital-identity infrastructure is trusted by the public. While digital systems generally improve on the status quo of insecure and unwieldy paper documents, they bring new risks, too, in particular for privacy and security, equity and inclusion, and enforcement:

Table 3 – Primer on digital ID risks and mitigations

	Risks	Solutions
Privacy & security	• Centralised databases can be abused for surveillance, either by design or mission creep, and risk creating a single point of failure (e.g. 'honeypot' cyberattacks) • Individuals can be identified and sensitive information revealed if data isn't anonymised or encrypted • Risk of inability to restore integrity of biometrically secured systems in case of cyberattack, since biometric data (fingerprints, facial scans) cannot just be changed like a password • Opaque digital systems can	• Commit to a user-centric approach to managing IDs; i.e. no central database • Use modern public-key cryptography to secure data • Use on-device biometric scans only so that data stays on device, minimising attack surface • Allow only users to share data via discrete, use-specific credentials • Have identity providers keep a log of which APIs issued individuals'

	undermine users' trust • Storing data on device only complicates data recovery if device is lost or stolen	credentials (with users' permission); credentials reissued after a biometric check
Fairness, discrimination & inclusion	• Digital-only authentication can exclude those without access or ability to use technology, most often communities that are already marginalised • Minority groups may distrust state digital infrastructure if associated with restricting liberties and surveillance	• Work with ID providers to create accessible alternatives, e.g. SMS, connected smartcards, printed QR codes, nominating proxies • Avoid mission creep, communicate openly and add safeguards that build trust with all users
Enforcement*	• Mandatory ID checks risk curtailing liberties, exacerbating exclusion risks • No existing channel to report harms or seek redress	• Restrict checks to highest-risk settings first, until rapid point-of-use tests become more available • Provide feedback loops to improve services and a redress service to ensure accountability

**Risks equally applicable to physical and digital systems*

Digital ID Applied to Covid-19

The solutions above hold for any digital-identity infrastructure, including any applied to tackle Covid-19. But this crisis presents some unique decisions for governments, too. Code alone cannot set the rules for the whole system.

As we have set out previously, extraordinary measures that throw up sensitive policy challenges must be matched with appropriate transparency and scrutiny. The following protections should all be set out in primary legislation and accompanied by sunset clauses that prevent crisis measures unwittingly becoming the new normal:

Do not combine with other digital tools such as contact tracing.

States may be tempted to lump digital identity systems and mobility credentials together with contact tracing and other Covid-19-related health apps. But contact tracing is explicitly about tracking and monitoring individuals' relationships with others, whereas identity is about authenticating specific individuals and should be under their control. Both can and should function separately from one another. Mobility credentials are also only one particular use case for digital identity, so governments should build this as a standalone piece of infrastructure to be applied and reused in different cases. This approach could also be transformational in building a truly 21st century state.

Widespread credential checks require a functional mass-testing regime.

Covid-19 mobility credentials are primarily generated by either a positive antibody test or a negative antigen test. Given that these credentials confer privileges on the holder, this means testing becomes an equity issue: Unfair access to testing can lead to discriminatory outcomes such as delayed access to travel, services or the labour market. There will always be some residual risk given that not everyone will carry a credential and point-of-use tests are not 100% accurate, but comprehensive testing is still a necessary condition for the public to trust the role of mobility credentials.

Additionally, this case underlines that a positive antibody test cannot be the only qualification criteria for a mobility credential, since this would incentivise people to catch the virus in order to access services earlier. A negative antigen test should therefore also suffice so that people retain the incentive to avoid infection.

Governments must regulate where credentials can be enforced, and by whom, to prevent abuses.

1. Where to enforce

In general, digital identity should be considered as an enabling platform, where an ecosystem of actors interact to provide the infrastructure or issue and verify credentials, such as proving your qualifications when applying for a job. In this sense, governments might provide the infrastructure directly or set privacy and data standards for a market-led approach, but would rarely regulate the use of credentials *per se*.

But Covid-19 is a different case and warrants greater government involvement. The impact of restricting someone's ability to travel or access some spaces is an order of magnitude greater than, for example, that of someone declining to share a degree credential as part of job application checks. States must therefore set the rules to ensure that any restrictions are necessary and proportional to limit the spread of Covid-19, and do not reproduce pre-existing systemic biases.

In practice, the central trade-off governments face is between protecting certain spaces and minimising restrictions on people. If the benefit of restrictions is negligible but the social cost is high, policymakers should therefore think twice. For most settings, this means leaders will need to trust that official guidance and self-isolation requirements will provide adequate protection. For example, parks and other outdoor settings appear to be relatively low-risk transmission environments, so enforcing mobility credentials would primarily result in unnecessary friction and increased public frustration.

However, some settings clearly warrant restrictions, such as care homes with vulnerable residents and high-transmission-risk large gatherings. The public may accept these measures easily, but leaders may be unsure where to draw the line. Even if rapid antigen testing and piggybacking on existing restrictions, such as ID checks at an airport, may minimise widespread friction, checks will still be very visible and potential targets of public frustration. The solution is that governments should not try to play whack-a-mole with every building or sector, but instead devolve the decision to organisations. For example, private office buildings should have the right to require all staff to present a credential on entry, otherwise the occupancy limitations on offices may make them economically unviable. Similarly, airplanes and trains could operate at maximum capacity if these checks were in place.

2. Who can enforce and/or sanction

Alongside deciding where credentials can be enforced, authorities should also consider *who* can enforce these checks. Given that digital credentials protect individuals against leaking unnecessary data or being subject to probing questions, leaders must not allow gaps in governance to still leave people exposed to other abuses of power.

As legal scholars Lilian Edwards et al have argued convincingly, policy should set out the different powers that are prohibited or available to verifying parties, rather than letting mobility credentials become unregulated, *de facto* internal passports that exacerbate exclusion. In particular, individual choice and consent cannot be undermined by others assuming powers that they do not have. For example, companies should be allowed to refuse entry to an office building if someone declines to show a mobility credential, but the same person could not compel another to show this credential in the street. Only a police officer would have that power, or could issue any penalties for failing to do so, but even this should be restricted only to where absolutely necessary and proportionate, with authorities held to account through the standard appeals process.

Moving From Debate to Delivery

Securing public consent is a necessary condition for a digital identity to be effective, but it is also insufficient to move fully to implementation. Delivery means that the state either builds itself or creates a market for identity infrastructure, and several obstacles remain before this can happen.

Governments need to decide what role the market should play, and how to regulate.

States may wish to create a market for identity, where any number of companies can provide identity services to individuals and organisations. But this introduces many issues where a clear government steer is required to allow providers to proceed, including but not limited to:

- Deciding which technical standards providers must build to, likely in agreement with other countries to secure international travel through interoperable credentials
- Establishing a way of regulating or enforcing standards, e.g. creating a statutory regulator, certifiers or a chartered body; requiring providers to open source apps
- Publishing and documenting APIs for test results, so that credentials can be scanned for authenticity and validity
- Setting out data protection requirements, e.g. requiring providers to complete a data protection impact assessment (DPIA)
- Clarifying what liability risks companies take on by providing identity services, e.g. in case of fraud
- Explaining how credential checks should work to verifying parties and setting clear limits of powers
- Working with providers and verifying parties to explore sustainable business models
- Creating feedback mechanisms, possibly including systems for user redress, to keep systems and verifying parties accountable
- Monitoring implementation to capture broader, strategic transformation opportunities

This guidance should be published in the open: This not only improves transparency and secures all parties' trust but minimises information asymmetries that would otherwise undermine the effectiveness of the policy.

Identity should be in the portfolio of a senior minister with authority across government.

The combined complexity of responsibilities in securing public consent and accelerating delivery highlights that leaders must treat digital identity with the significance that critical national infrastructure merits. The policy should therefore be owned and led by an authoritative part of government and executed as part of a firm, holistic grip on Covid-19, rather than relegated to a small team on the fringes of a department or health system. This would also help identity providers that frequently struggle to wade through the various government bodies with a stake in this issue. Indeed, even in normal times, the wide and often conflicting interests of policymakers, providers and campaigners make it especially hard to make progress on this issue. But Covid-19 presents an opportunity where all parties recognise the significance of the challenge ahead. Leaders must grasp it.

Conclusion

This briefing has set out how digital identity can help to manage Covid-19, what an optimal solution should look like, the fault lines of public consent and the obstacles that need clearing to accelerate delivery.

The need for digital identity is clear. To deal with the invisible threat of a contagious virus, states need a way to embed a visible and verifiable layer of trust into society. International travel – and by extension the world economy – cannot properly restart without some way of ensuring that they are safe. The same applies to care homes, offices, and other high-footfall settings and large gatherings. Instead of crude border closures or keeping vulnerable residents isolated, we need a way to grant granular permissions for people to credibly assert that they can safely enter these spaces. A properly implemented digital credential could provide this assurance, while precluding the risk of other apps or intimate medical records being required as a substitute – perhaps in an unlawful overreach.

But building an effective containment architecture, including digital identity, requires as careful an approach to governance as anything technical. Strict guardrails, accompanied by robust mechanisms for accountability and redress, must be in place to secure public consent.

Crucially, while the success of digital identity for tackling Covid-19 is dependent on a range of other factors, in particular mass testing, it would be a mistake to point to those challenges and write off the entire project. The need to safely reopen economies and societies won't go away, and mobility credentials underpinned by a digital identity can play a vital role in achieving this.

FOLLOW US

facebook.com/instituteglobal
twitter.com/instituteGC
instagram.com/institutegc

GENERAL ENQUIRIES

info@institute.global

FIND OUT MORE

INSTITUTE.GLOBAL