Written evidence submitted by Nomidio

Andersen Cheng, CEO
Philip Black, Chief Product Officer
Ben Todd, Head of Worldwide Sales

The importance of preserving individual privacy in Immunity Passports

1) Executive Summary

- We believe the latest approaches to encryption can support the development of an Immunity Passport system that is both effective and protects the privacy of the individual.
- This submission is designed to explain why we urgently need privacy assurance as well as how we can apply cryptography at the system design phase to safeguard fundamental human rights.

Key sections

- About Nomidio & Post-Quantum
- The potential for Immunity Passports to support work & travel
- Key principles for protecting individual privacy during the design of Immunity Passports
- The potential for Threshold & Homomorphic Cryptography to assure privacy of a centralised Immunity Passport system
- Why an Identity Cloud offers a rapid route to privacy-preserving Immunity Passports
- How Nomidio can partner with the UK government to design privacy-preserving Immunity Passports
- Concluding observations

2) About Nomidio

At Nomidio our mission is to keep people's Personally Identifiable Information (PII) safe and under the absolute control of the individual without compromising the ability of organisations serving the individual to offer a world-class experience.

With a heritage in Post-Quantum Cryptography including 35+ Patents we have developed the Nomidio Private Identity Cloud as a single place in which Personally Identifiable Information is encrypted and stored, allowing multiple organisations to take advantage of this data in a secure and anonymised way. User ID is tokenised allowing organisations to take advantage of the user identity without the risk inherent in storing full PII.

Our initial innovations comprise Identity as a Service (IDaaS), Nomidio Identity Binding (NIB) and Identity Verification (IDV). Nomidio's technology has been conceived and developed by high-calibre cyber security, encryption and privacy experts at Post-Quantum.

3) About Post-Quantum

Post-Quantum are a team of high-calibre cyber security, encryption and privacy experts working to develop a replacement for today's open source public-key cryptography standards RSA and Elliptic Curve.

The firm's algorithm 'NTS-KEM' is the only UK entry and one of seven finalists in NIST's competition to identity a future global standard for code-based public-key cryptography that can withstand the code-breaking capabilities of quantum computers.

The company has performed work for organisations including NATO, GCHQ, NCSC, the UK Government and Avaya, and is accustomed to applying top secret grade methodologies and expertise for commercial grade applications. Post-Quantum has developed unique key splitting technology that can solve the long-standing problem of 'privileged access' to centralised databases which is of particular relevance for Immunity Passport proposals, where cryptographically provable and auditable access to citizens' data is of paramount importance.

4) The potential for Immunity Passports to support work and travel

Immunity Passports, if correctly conceived, offer the potential to support the return to work and the phased re-opening of international travel.

The ability for an individual to present 'proof-of-immunity' when arriving to the office, a hotel or when boarding a plane will help engender confidence and allow those of us that have developed immunity to Covid-19 to begin living more normally again.

However, if incorrectly conceived and without the requisite considerations to individual privacy, Immunity Passports may do permanent and irrevocable damage to individual civil liberties.

5) Key principles for protecting individual privacy during the design of Immunity Passports

User consent	Each user must be able to grant permission for the use of, or processing, of the immunity passport. Failure to deliver easy to administer control to the individual risks firms being able to access the data to form judgements without consent e.g. a life insurer may increase a premium if someone over 50 has not yet had coronavirus.
Cryptographically assured authorisations	User permissions and other 'authorisations' must be cryptographically provable and secure. It is imperative there is a mechanism for understanding 'beyond doubt', that the individual has granted this permission. Virtually all of today's identity systems run on 'software logic step' authorisations, which are vulnerable to interference.
Behavioural privacy	'Behavioural privacy' must be upheld. Any immunity passport system must not let the firm that built it, or the government, understand the purpose for which the individual presents their immunity passport. This can be achieved relatively simply by using data tokenisation, and failure to do so would turn the immunity passport into one enormous 'super cookie' that tracks our behaviour.
No data or meta-data resale	Data and metadata must not be resold. An immunity passport will provide a potential gold mine of information about every user's identity, health condition and the organisations they interact with. Today, the vast majority of digital identity firms re-sell this data for huge financial gain in a similar

	manner as social media companies. This isn't acceptable for an Identity Passport (or any other identity system) where success can only be assured with 100% trust from the end users.
Quantum-safe encryption	Full encryption is critical. Whether or not someone has survived coronavirus will quickly become a defining attribute of someone's identity and it is imperative the stored data is encrypted to 'top secret' government standards. Furthermore, this encryption should be 'quantum-safe', avoiding the need to replace it when sufficiently developed quantum computers begin to pose an existential data security risk in the very near future.

6) The potential for Threshold & Homomorphic Cryptography to assure privacy of a centralised Immunity Passport system

Much of the debate surrounding the UK's Contact Tracing App has centred on whether it should be centralised or de-centralised in design. The primary concern with a centralised database is that NHSX, or the organisation administering the database, would have 'privileged access' to its contents. The solution, it is argued, is a decentralised design where data resides and data processing occurs on the users own device. However there are two central problems with a decentralized design:

1. Decentralised systems cannot typically achieve the same level of performance as a centralised design.
2. It would be preferable for NHSX and its affiliates to conduct aggregated and anonymized analyses on the entire dataset to inform policy and public health decisions, but only if the privacy of the user can be guaranteed beyond doubt.

This same debate is likely to become even more pertinent in relation to Immunity Passports but it needn't be. With the correct application of Threshold, or key-splitting, and homomorphic cryptography, user privacy can be assured and cryptographically verified for a centralised identity system.

Cryptographic assurance of user-privacy for Immunity Passports

Secure multiparty computing systems can protect data and assure privacy. A technique known as threshold cryptography can split the master key to encrypted data into fragments creating a pre-defined number of these key fragments that can be shared between stakeholders.

When setting up the secure system, a number is set at which a quorum is established (say, 3). If 3 out of 7 fragment holders bring their fragments together in consensus then the archive can be decrypted (in this case someone's immunity status). 3 is the minimum number of fragment holders in this example and it can include any combination from the pool of 7 fragment holders, so long as this minimum number is reached. The system is almost infinitely flexible, a quorum of 3 of 4 fragment holders can be set as easily as a quorum level of 17 of 853 fragment holders.

Key fragments can be distributed to multiple stakeholders e.g. a government body, a privacy group, a trusted friend or relative and of course, the individual themselves.

Beyond the standard security applications of this technique, it can also be used to assure and reassure individuals that their identity and Immunity status cannot be accessed by a single privileged system administrator. By providing each UK citizen with a unique key fragment and an easy way to provide this fragment when requested, we can build an encrypted Immunity Passport system where the individual retains control and provides or withholds consent simply when requested.

Imagine an airline requests your Immunity Passport status in relation to a trip you are planning. Permission can easily be granted via an app or web interface whereby the key fragment, residing in the secure enclave on your phone, is provided. However, should another organization, including NHSX, attempt to request your immunity status then consent (and by association the key fragment) has to be separately requested from the individual.

7) Why an Identity Cloud offers a rapid route to privacy-preserving Immunity Passports

For efficient international deployment, a centralised, highly secure and tokenised Identity Cloud is needed to deliver a cloud-based digital identity system capable of allowing an individual to provide their identity information once (e.g. medical certification of immunity to Covid-19) and to use it many times with the different organisations they interact with.

An Identity-as-a-Service (IDaaS), which uses industry-leading biometrics engines, can be used to authenticate individuals via the web, call centre or physical point of presence. Individuals provide their identity information once and re-use it with the multiple organisations they interact with. The user's ID is tokenised so their behaviour e.g. where they have logged-in / authenticated, cannot be understood by any party.

Such a cloud system should be based on a unique and highly secure encryption architecture that means every data attribute about an individual e.g. first name, date or birth or immunity status has its own unique, quantum-safe, encryption key. The overall database must also encrypted again for additional security with a different key.

Importantly, with such an Identity Cloud the individual retains complete control over their identity entry and manages consent for how their data is used via a simple web interface. For example, Hotel ABC may request to query the individual's immunity status, but that request would only proceed if the individual provided consent.

Using key-splitting cryptography a number of different stakeholders are required before the individual's identity data can be decrypted. Multiple fragments also make such an Identity Cloud a secure and unattractive target.

7) A simple user experience for Privacy Preserving Immunity Passports

John wishes to travel to the US for a business meeting and is keen to formally prove his immunity status.

Step one: John registers his identity with the Identity Cloud just once and captures a face scan (aka selfie) and also a voice print using his smartphone camera and recording device. He also uploads legal documents that confirm his identity such as a driving license or traditional passport verifying that he is John Smith. He then makes an appointment with the NHS to be tested for Covid-19 antibodies.

Step two: Just before the test takes place another face scan and voice print are captured and compared to those John originally provided to the Identity Cloud ensuring someone else isn't taking the test on John's behalf. When a match is confirmed the test is administered.

Step three: When antibodies have been confirmed an immunity certificate is granted by the NHS and bound to John's Identity record residing in the Identity Cloud with maybe an expiration date when John needs to be re-tested. The immunity status, identity and flight details are all cryptographically processed with a tamper proof picture QR code generated and sent to the user's mobile device.

Step four: A month before travel John receives a notification on his phone from the Identity cloud "*US Customs & Border Protection Agency request to confirm your immunity status. Do you consent? YES/NO"*. John clicks YES.

Step five: John's fragment of the encryption key is provided securely and autonomously to the Identity Cloud, which is used to decrypt his status. An automatic confirmation of his status is then provided to the US C&BPA without a date of expiry, but with cryptographic proof that it is after his expected return from the US.

John then decides to take out some travel insurance with the same provider that insures his life and health. He is aware that his immunity status is due to expire shortly, just after he returns from the US.

After talking with the insurer he receives a request from the Identity Cloud "*Insurance Company ABC would like to confirm your immunity status. Do you consent? YES/NO"*. On this occasion John clicks NO and it isn't possible for his Immunity status to be decrypted.

Step six: At the airport John is checking-in and needs to prove both his identity and his immunity status. The tamper proof picture QR code is produced, scanned to retrieve the flight details and face checked as an extra security measure, all without the check in or security staff needing to touch the user's device. The check-in process optionally triggers a request from the Identity Cloud *"British Airways would like to confirm your immunity status. Do you consent? YES/NO"*. John clicks YES and biometrically authenticates to confirm that he is providing consent via his phone. John also then specifies that he is happy to share his immunity status with British Airways on all future occasions.

Step seven: At the US airport, John presents the tamper proof picture QR code which is then scanned to retrieve details and also face checked as an extra security measure, all without the security staff needing to touch the user's device.

After his trip to the US John receives another request from the Identity Cloud ***"The UK Government would like to analyze the nation's immunity status, do you consent? YES/NO."*** John clicks YES. An aggregated and anonymous dataset is compiled using AI in reverse, and is only released when "zero knowledge proof" is assured that reverse engineering is not possible.

8) Ease of roll-out across key immunity touchpoints

If Immunity Passports are to support the effective re-opening of the economy to their fullest potential then it must be possible for someone's immunity status to be checked easily at a wide range of touchpoints e.g. the office of a small employer or through the website of a small travel and tours provider.

With a cloud-based platform approach to identity management, it is possible to have a system such as the one described in this document up and running within 24 hours. Indeed, following disruption to replace its previous in-person verification process, Hitachi Capital recently deployed the Nomidio Identity Cloud in a 24 hour period as part of its requirement to remotely validate applicant identities as one of the 40 accredited lenders to the Coronavirus Business Interruption Loan Scheme(CBILS).

9) How Nomidio can partner with the UK government to design privacy-preserving Immunity Passports

A) Easily deployable: The Nomidio Identity Cloud is already built and can be deployed in less than 24 hours.
B) Intellectual Property for privacy preservation: Nomidio stands ready to commit its Intellectual Property and high-calibre cryptography skills to the government's Immunity Passport programme. In particular, our unique Threshold Cryptography system is an ideal means of deploying a centralized system with cryptographic privacy guarantees for users.
C) Ease of use: The Nomidio Identity Cloud can be delivered to users within an app, or via a secure mobile web page without needing a dedicated app. This nuance is important because it means each organization administering an immunity check does not need to build its own app. For users, the biometric authentication process is straightforward and can be completed within seconds.
D) Privacy & security at our core: The Nomidio team is accustomed to working with the UK government to Top Secret grade and we have applied this unique heritage and experience to the security and privacy design of the Nomidio system.
E) Neutrality: Nomidio's independence is assured as all the key processes are cryptographically provable rather than software logic steps which can be tampered with. Its core IP is already in the public domain and all the key cryptographic innovations are externally reviewed by Royal Holloway University of London, which is the most reputable crypto institution in the UK.
F) Quantum-safe encryption expertise & IP: Our engineers are part of an extremely limited number of experts globally that are pioneering encryption capable of withstanding attack by quantum computers. Our algorithm is a finalist in NIST's competition to identify a new global Open Source standard for public-key cryptography to replace the RSA/Elliptic Curve standard currently used to protect virtually all internet and mobile traffic. This is a key consideration as citizen identity data is permanent and needs to be quantum proof. Nomidio Identity Cloud is already quantum-ready and

will not need to be “thrown away” in the next few years when the government starts to future proof the Immunity Passport system.

G) Homegrown innovation: Nomidio is not a new startup with retail grade incubator quality solutions. Whilst retaining a startup’s agility, the team’s achievements are well recognised in the government security circles. We can either work individually or team up with our preferred list of systems integrators. If Nomidio is selected to build the system, it will be a truly disruptive move from the government to honour its promise to back the UK’s homegrown startups and talents.

10) Concluding observations

1. Someone’s immunity status is likely to become a defining characteristic of their identity and it may both open and restrict access to certain services. It is therefore essential that this information is protected with the highest standards of ‘privacy by design’ and encryption.
2. Immunity status must be ‘portable’ so it can be provided by the individual to the various organizations they interact with but only when the individual consents to do so.
3. With the correct cryptographic measures the problem of centralized privileged access can be overcome so the government, and indeed Nomidio as a trusted third party, can prove beyond doubt that the privacy of system users is protected without the need for decentralization.
4. We have an opportunity to ensure the effectiveness of Immunity Passports by designing them first and foremost with users in mind. It is only by assuring people of privacy preservation that a critical mass will actively use Immunity Passports with confidence.
5. Once this “permission by user” trust is built, there is every potential to reuse the platform and for it to become a true “register once, use many” Bring Your Own Identity solution.