the3million
124 City Road
London EC1V 2NX

By email:

    Public Enquiries, Home Office

CC:

    Home Office Status and Information Services
    Home Office SUG team
    Independent Monitoring Authority

Your reference: DECS Reference: TRO/0338254/22

8 November 2023

Dear Mr Tomlinson,

Online-only immigration status and discussions of alternative solutions

Thank you for your letter of 7 June 2023[1], in which you replied to our correspondence of 8 March 2022[2]. It is my turn to apologise for the delay in responding.

Firstly, I would like to thank you for your continued engagement with our concerns around the use of digital-only status, and for the intention to maintain open lines of communication with us and other stakeholders. We would very much welcome the opportunity to accept your invitation to look again at alternative solutions over the next few months, and are pleased that you will take our proposal and other evidence or suggestions into account.

You specifically asked us to provide feedback or further amendments on our QR code proposal, including feedback on the "long life share code" idea which you set out in your letter. I will do so below, as well as responding to various issues in your letter.

"Digital-by-default"

Firstly, I would like to state our continued objection to the phrase "digital-by-default" as applied to the cohort of EU citizens (and other subsequent cohorts) who have been given an immigration status that is very much "digital-<u>only</u>".

As you will be aware, the evaluation[3] by the Government's Central Digital and Data Office of the Home Office's 2018 digital right-to-work trial, which first trialled the use of share codes for those with biometric cards, stated:

---

[1] https://the3million.org.uk/publication/2023060702
[2] https://the3million.org.uk/publication/2022030801
[3] https://www.gov.uk/service-standard-reports/prove-your-right-to-work-beta

*"In particular there is a need as the service becomes mandatory to ensure that it is usable by all users, including those with a current preference for a physical object. Significant care will be required before any decision to remove the physical 'Biometric Residence Permit', due to these strongly held concerns, particularly with users with low digital skills. **There is a clearly identified user need for the physical card at present, and without strong evidence that this need can be mitigated for vulnerable, low-digital skill users, it should be retained."***

*"The services are easy for digital savvy users to get through, and the team have a good support model in place for helping low digital users through the service, although they are aware from user research how unlikely it is that low digital users are to use the online service at all. This research raises concerns around BRP cards being retired in favour of digital only services, as the team has very strong evidence that this would cause low digital users a lot of issues. This is something that needs careful consideration with the drive to convert more services to digital and potentially remove their physical counterparts - **that digital by default doesn't mean 100% digital."***

In direct contravention of the recommendations in this evaluation, the EU Settlement Scheme [EUSS] status given to EU citizens has been 100% digital.

Furthermore, the Home Office View & Prove system for proving status is not just <u>digital-only</u>, it is <u>online-only</u>. There are many fully digital status proving systems that could be envisaged, and are in use throughout society, that do not require constant online access. In choosing an online-only process, the Home Office has chosen the most challenging system for digitally-excluded individuals, as well as one that is most vulnerable to system outages.

In your letter you state *"...we acknowledge there remain some limited scenarios where people could benefit from a secure, printed document or other 'offline' token that enables them to prove their immigration status. The first of these is in the context of travel, and the second is for those who are digitally excluded and do not have additional support or help."* We welcome your acknowledgement, but would note that this is the first time that we have received such acknowledgment. We would of course welcome a further discussion about this, and an indication of any plans for such a token to be implemented.

Previous to your letter, we were consistently told that *"We acknowledge the move away from physical documents to digital status represents a change which individuals and service providers may take time to get used to. This is why it is being rolled out incrementally and with support available to help individuals use their new status."* For those granted status under the EUSS, the change was neither incremental, nor was there much support beyond being able to contact the Resolution Centre [RC]. This is not sufficient for digitally excluded or vulnerable citizens, and in any case the RC often cannot fix technical issues for months on end, and cannot give timescales in which these issues can be rectified.

Offline use of printed tokens

You state in your letter that you do not accept that any printed token should be able to work offline, and that you cannot envisage any circumstances where that would be needed, other than in the situation of travel.

We would like to make three comments on this.

Firstly, the reason the3million put so much emphasis on the ability of our proposed Secure QR code token to work offline, is because the Home Office team we met with in June 2021 specifically requested us to explain more about this feature. They said this was the aspect of our proposal that they were most interested in, as they suggested that the ability to also work offline could fill some requirement gaps that the View & Prove system cannot fill. This was why we went out of our way to demonstrate, with technical detail to back it up, how our proposal can work securely and robustly while offline, as a fall-back to the full online functionality.

Secondly, while we may understand that the Home Office has a preference for online functionality, we do not understand why you would positively reject the additional option of offline fallback functionality. You state in your letter that this would compromise the principle of making real time checks on the master record of people's immigration status. As we stated in point 13 of our detailed technical reply of [8 March 2022](4), we anticipated and addressed this in our proposal. Our proposal means that you do not need to compromise this principle.

Thirdly and most importantly, we do not accept your assertion that, beyond the travel scenario, you "*cannot envisage any circumstances where an individual or organisation required to check an eVisa could to wait until our online services were available, or until they had internet connectivity, to carry out a check*". We have direct evidence of negative impact on individuals during the widespread View & Prove outages in August. People reported losing out on job offers, rental opportunities and other time critical situations such as education pre-enrolment (which is required to go on to secure limited course and accommodation allocations). In particular, the gig economy and the extremely tight rental market mean that the proof of immigration status is extremely time-sensitive for a very large cohort of people, often including the most vulnerable.

Data-sharing interfaces within the Home Office

We would be grateful if you could provide us with more information about precisely how the data-sharing interfaces with the Home Office, that you reference in your letter, would work.

If only name and date of birth is used then such data-sharing is vulnerable to identity mismatches, including false positives and false negatives. There will be cases of multiple individuals sharing the same name and date of birth, which can lead to serious errors. We have seen examples of people stopped and interrogated at the border as a result of mistaken identity. On the other hand, there will be cases where a difference in name spelling or transposition of accents or from foreign alphabets mean that individuals will not be found.

If a passport number forms part of the match (as your letter appears to imply where you say "*A person applying for access to services need only provide proof of identity to the organisation e.g. provide Department for Work and Pensions with their passport number, and immigration status checks can be run automatically*"), then this solution pre-supposes that the individual is able to keep a UKVI account updated when a passport is renewed. The system would fail entirely if someone had a new passport that was unknown to the Home Office database.

One piece of feedback we receive so often from individuals reporting to us is their frustration that they do not have a standalone proof of their immigration status, one that is not tethered to their current travel document. This is a Home Office design issue that we discuss extensively in our March

---

[4] https://the3million.org.uk/sites/default/files/documents/t3m-reply-HO-SecureQRProposal-08Mar2022.pdf

2022 report[5] to the Independent Monitoring Authority on the challenges of maintaining a digital status (see section "*Access to immigration account through a changing identity document number*", paragraphs 35-41).

Feedback on the Home Office "long life" share code proposal

Your letter explains that one idea under consideration is a "long life" share code provided in the decision letter. The status holder would therefore not need to engage with View & Prove. The status checker would use this share code in the same way as current share codes, by entering it into the View & Prove system.

You explain that one disadvantage is that once a checker had been given such a code, they could use it at any time to continue checking a person's status, regardless of any need to do so, which poses privacy concerns.

You go on to state that the Secure QR code proposal would not offer any benefits over and above a long-life share code, because it "*would be harder to share remotely and would always require internet-connected scanning technology to access and read it*".

We disagree that the Secure QR code proposal would not offer any benefits over and above a long-life share code, and we set out our reasons below.

Firstly, the long-life share code does not address the situations where status checkers are unwilling or even unable to engage with the View & Prove process.

- Airlines and airline ground operators have made it very clear on numerous occasions that they are not prepared for their check-in and boarding staff to go through the steps of logging into a UK Government website in order to access someone's proof of immigration status. The process is not suitable for a time-sensitive situation, where a large queue of passengers may need to be checked, and checkers object to having to enter details about themselves and their job function.

  We are aware of course that the Government's intention is for the interactive Advance Passenger Information (iAPI) to negate the need for such checks. However the development of the iAPI system has already suffered long delays and may not be fully operational in time for when the Electronic Travel Authorisation (ETA) system is fully operational. In any case, a fallback is urgently required for when iAPI suffers an outage, and an airline will want to reassure themselves of passengers' right to enter the UK in order to prevent being responsible for the cost of returning any passengers who are refused entry at the UK border.

- Many private sector status checkers would prefer the convenience of scanning a barcode with an app, over having to go through a multi-step interaction with a website. Scanning apps are common-place these days and universally used - compare boarding passes, COVID smartpasses, event/transport ticketing and many more. On the other hand, a "long life" share code would require manual input and hence it would make the process vulnerable to human error.

Secondly, we disagree (as explained earlier) with the premise that the Secure QR code proposal "*would always require internet-connected scanning technology to access and read it*". Rather, it is the

---

[5] https://the3million.org.uk/publication/2022032801

proposed long-life share code that would definitely require both internet-connectivity and the Home Office systems to be available at the time of checking. We have explained how the Secure QR code system *could* have (albeit fallback) offline functionality. This means in situations where there is temporarily no internet-connectivity, or there is any system outage meaning that View & Prove is unable to function, status checkers will still be offered a high degree of reassurance about someone's up-to-date immigration status.

Thirdly, for those specific situations where checks are being done remotely, we concede that sharing a QR code would require sending an image rather than reading out a string of characters. However, a QR code is not subject to the human error that a character string is vulnerable to. We have heard of many instances where someone's share code did not work when the status checker tried to enter it, and believe many of these cases are down to human error confusions such as between zero and the letter O, or one and the letter I.

Fourthly, regarding the privacy concerns, there are ways of mitigating this within the Secure QR code proposal which are not possible with a long-life share code.

- For those who are happy to use the QR code within an app, it is trivial to seamlessly integrate a scanning validity cut-off into a secure QR code. This would mean that someone who saves a screenshot of the QR code could only scan this (again) during a certain period of time. If set at 3 months this would then replicate the same situation as with the current share code validity time. The status holder would not even be aware that the QR code in the app changed over time. This same validity technology was used in the NHS COVID Pass.

- For those who are digitally excluded and require a physical card to be sent to them, the QR code on their card could also have a validity end-date integrated into it. The length of this time would require discussion, whether between e.g. a year (akin to membership cards such as the National Trust), or a period between five and ten years - to align with the EU's validity limits on biometric cards issued to British citizens in the EU with Withdrawal Agreement status. This would also align with the Home Office / EU requirement for people to change their photographs on their status (whether on their digital profile or their physical card). As you know, a card with a Secure QR code would be extremely cheap to produce yet highly secure, in contrast to existing biometric cards.

  While we acknowledge that for vulnerable and digitally excluded people, there may be practical problems around issuing new cards over time, this would still be a major improvement to the current situation where the fact of their digital exclusion creates life-damaging barriers every time they need to assert their rights such as their right to work or rent. Charities, friends, family members and/or government grant-funded organisations would only need to help them once in a number of years to ensure a new card is obtained, rather than trying and often failing to help in the time-critical situations of asserting rights.

- The long-life share code would not have any such time-limiting ability, unless it is not limited to the stated idea of a simple one-off code provided in the decision letter.

Potential amendments to our Secure QR code proposal

We could envisage a range of amendments to our Secure QR code proposal, as Home Office requirements are discussed and become clear. The following are merely a number of possible suggestions and discussion points rather than actual recommendations. We urge you to carry out a proper consultation on this issue, with input from other relevant sector actors and individual status holders.

1. **Validity time limit - for QR codes generated by an app**

As discussed above, a validity time limit can be seamlessly and transparently built into a Secure QR code - such that attempting to scan it beyond that time limit could result in certain outcomes.

If an app were developed, it could automatically regenerate a timestamped QR code with each use, with the chosen built-in validity period. Attempting to scan it beyond that time limit could result in a simple refusal to scan the code, with an explanatory message displayed. This message should make clear that this secure QR code is guaranteed to have originated from the Home Office: and that although it is no longer valid for scanning, this says nothing about the validity, expiry or otherwise of the underlying immigration status.

2. **Validity time limit - for QR codes on physical cards issued by the Home Office**

For QR codes specifically generated for use on a physical card, issued by the Home Office to vulnerable or digitally excluded people, a different functionality can be built in. These cards could still have a validity limit - for example between five and ten years in line with EU validity lengths on their cards for British citizens under the Withdrawal Agreement, and in line with the Home Office requirement to update photographs. Attempts to scan it could result in the following:

1. If approaching the validity end date, display the immigration information and include a message that the card and code should be renewed soon.
2. If beyond the validity end date, but within an agreed grace period interval, display the immigration information, but include a statement that the card and code must be renewed as soon as possible.
3. If beyond the agreed grace period interval, don't display the immigration information but state clearly that this is not a reflection of the person's immigration status and direct the person to obtain a new card from the Home Office.

Such a scheme would strike a balance between the privacy concerns of all users on the one hand, and the protection of immigration rights of vulnerable citizens on the other hand.

3. **Amount of information displayed - for QR codes generated by an app**

It would be easy to build options into an app to allow the status holder to choose how much information should be displayed to the person scanning. Since the secure QR codes would be generated dynamically, it would be trivial to generate codes containing or excluding immigration route information, status expiry dates and more.

4. **Amount of information displayed - for QR codes on physical cards issued by the Home Office**

A static secure QR code on a physical card issued by the Home Office would need to include all information required by any status checker. This however is no worse than the current

biometric card scheme, and individuals would prefer a reliable way of asserting their rights over struggling to do so due to digital exclusion.

5. Offline scanning mode and statutory excuse for employers and landlords

As discussed several times in this letter, we believe that the ability to have an offline fall-back mode is very helpful. This is to cater for situations such as system outages or lack of internet access. Those checking status would still see a low-resolution photograph to match with the photograph displayed in the app or on a card, and the person in front of them. As we have set out in our original proposal, the scanning app could contain a revoke-list so that even in offline mode, it would know whether a particular secure QR code represented a revoked immigration status. (And this is done in such a way that the app would *not* contain any identifying information about the statuses referenced by the revoke list.)

However, to address the Home Office concern that status checks should be done online at all times, it could be envisioned for example that the use of an offline scan provides only a time-limited statutory excuse for employers and landlords and that they need to re-do the scan in an online mode within a period of e.g. six months.

The Secure QR code proposal is based on internationally accepted best practice, and as such it should be possible to address any functionality requirements of the Home Office. We would of course argue (as we did in our proposal) that some aspects require parliamentary oversight, most notably around the gathering and retention of data. We also emphasise the need for wider consultation on the issue, which was lacking prior to the roll out of the current digital-only and online-only system.

Finally, of course, implementation of the Secure QR code proposal does not necessitate removal of the View & Prove system. If the Home Office wanted to, it would be possible to have both schemes available to individuals to view, maintain and prove their status.

We look forward to discussing these proposals with you in more detail. Such discussions should also involve individuals who currently have online-only status, and any organisations, charities and other voluntary bodies that help people view or prove their status.

Kind regards,

Monique Hawkins

Interim Co-CEO and Policy and Research Officer, the3million