

By email: Public Enquiries, Home Office
Copied: Minister Kevin Foster MP
Home Office SUG team

8 March 2022

Dear Mr Tomlinson,

Thank you for [your letter of 3 March 2022](#), in which you set out why the Home Office will not be adopting a secure QR code solution (as we explored and proposed in our document here: <https://www.the3million.org.uk/fixing-the-digital-status>) to the problems people face with accessing their status via the 'View and Prove' system.

It has become clear that since the full launch of View and Prove last year, numerous problems have arisen both with the View and Prove service and the helpline that is present to support people. We are finalising a further report of the issues with View and Prove to the IMA (which we will provide you with a copy of) and refer you to our previous correspondence relating to the service received via the helpline. A clear picture is emerging that more needs to be done to mitigate the problems arising from the online only View and Prove service (which includes both the View and Prove portal and the helpline).

A secure QR code solution, we maintain, is the most viable option and will address the concerns you have raised in your correspondence below. A large number of them are rooted in a misunderstanding of the proposal, so we are pleased to say they can be surmounted easily.

We are disappointed that the Home Office team did not meet with us to discuss the concerns raised in your letter. We are also concerned why it has taken over eight months to provide us with this feedback and particularly note the timing of the correspondence in relation to the debate in the House of Lords as part of the Nationality and Borders Bill.

We ask that you to meet with us after considering the content of this letter and to narrow the issues and strive towards a solution that will help people impacted by the current digital only process.

Given the delays and issues associated with the engagement between the3million and the Home Office team on this issue, we will be bringing it to the attention of the minister. We hope this will not distract from starting a meaningful dialogue on this issue.

Points raised by your letter

1. Basic principles

We agree with the basic principles that sharing immigration status should adhere to as set out by your letter and would add the following principles should be included at a minimum:

- The method of sharing immigration status information should be able to be used both domestically and internationally for travel and other, unanticipated, purposes
- The needs of vulnerable, low-digital skill users must be taken into consideration

We make these suggestions in line with the experience of users reported to us and elsewhere.

2. **Equivalence to vaccination status**

“Using a 2D Barcode in the context of demonstrating vaccination status is not equivalent to using a 2D Barcode to immigration status”.

- We believe that this may be a misunderstanding. Our proposal did not claim that it was equivalent, it merely mentioned that the underlying technology (**Secure** QR codes) could form the basis for an alternative implementation of a digital immigration status, which has the benefit of being able to provide for a printed backup.

3. **Expiration and change of immigration status**

“A person’s immigration status under the EU Settlement Scheme or under another immigration route can change. [...] Status can also expire.”

- We understand this and anticipated this concern, providing solutions for both these facts - see Q3.1 and Q3.2 of our proposal¹.

4. **Offline only operation**

“We have considered your central idea that a 2D Barcode could be added to a document [...] without the need for any online checks.”

- This comment unfortunately misunderstands how our proposal would work. In our meeting and email correspondence with the Home Office View & Prove team we outlined that the checks could be made in either offline or online mode.
- The View & Prove team were particularly expressing their interest in a solution that could work offline.
- It is important to compare a secure QR code solution with the current View & Prove which requires online access for **both** the citizen and the checking entity. In contrast, our proposal removes the need for online access to the citizen - thereby helping digitally excluded people - and retains highly secure fallback functionality for the checking entity even when offline.

5. **Potential of attack or inappropriate data access**

“Creating an app to scan 2D Barcodes [...] may introduce a new potential means of attempting to attack or inappropriately access the data”.

- We are not clear how this could be the case given how Public Key Infrastructure works. Please consider the explanation and related sources relating to Public Key Infrastructure in our proposal.
- Again, comparing View and Prove with a secure QR code solution, any possibility of attack or inappropriate access would be equally applicable to the web API underlying the current View & Prove infrastructure which exposes a larger attack surface than our proposal.

6. **Requirement for app and mobile device**

“Creating an app to scan 2D Barcodes [...] would require every person who is required to check a person’s status via the barcode, to have an applicable device, and have downloaded the app.” We would suggest this is an entirely proportional ask, given that:

- The vast majority of the six million citizens who needed to acquire status under the EU Settlement Scheme were required to use an applicable device. By contrast, the ‘EU Exit: ID Document Check’ app would be more complex to navigate than one required for validation of secure QR codes.

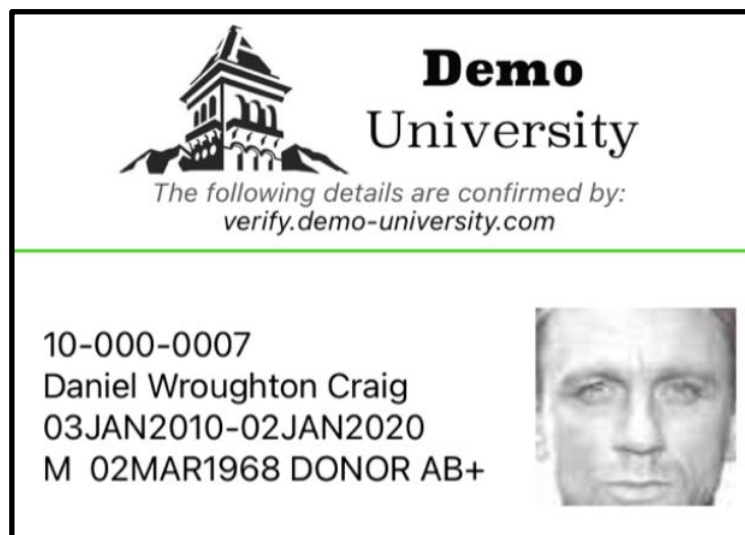
¹ <https://www.the3million.org.uk/fixing-the-digital-status>

- On balance, there are far fewer entities who need to check status than citizens who need to have their status checked.
- Entities who check status are vastly less likely to be digitally excluded than citizens who need to have their status checked.
- Entities who check status are already forced to engage with a digital check via the Home Office portal. We cannot see how it could be the case that giving entities reviewing status the alternative of scanning a code via an app forms a technological barrier for this group.

7. Facial image within barcode

“Our research has indicated the largest 2D Barcodes can contain 3KB of data and this is insufficient to encode a high-resolution image of the person with status. Given it would not be possible for a 2D Barcode to store a viable face image, a printed document with a 2D Barcode attached could not be used to verify the person presenting it was the rightful bearer.”

- We pointed out to the Home Office team in June 2021 that secure QR codes can “work seamlessly in a **combined** way, to show critical information when offline, and more detailed information when online - including showing high-res images from blob storage.”
- We also provided samples of the low-res images that could be displayed when *offline* - and reproduce such sample images below, which clearly contains a viable face image:



- We also pointed out that any documents would show a high-res photograph on the document itself, and therefore the photo embedded within the QR code (displayed when scanning) is an extra security measure that the document has not been tampered with.
- By contrast, the existing View & Prove **only** works in an online mode. The secure QR code proposal addresses this problem and can work both online (showing high-res photo when scanning) while additionally providing useful and secure offline functionality.
- In online mode therefore, our proposal can produce as high-resolution an image as any existing online service you describe in your letter, thereby matching the same risk reduction of fraud as the View and Prove service.
- In offline mode on the other hand, the existing online View & Prove services are rendered inactive, whereas our proposal retains the ability to inspect the document itself with its details and high-res photograph, and then scan the code contained on the document to gain a high degree of confidence that the document has not been tampered with in any way.

- To place into context the problem with View and Prove in this area, we have already seen cases where for example, UK Border Force was unable to access its systems to view status linked to identity documents. In those circumstances, Border Force officers were reduced to asking people to find and produce - on the spot - decision emails sent to them possibly 3 years earlier (with no photo document to check authentication we might add). People who could not do so either had to persuade officers of their status or face being detained. Having a physical card or an app as described in our proposal would have given UK Border Force reassurance even in offline mode that people had status.

8. **Data minimisation principle**

“Nor would the 2D Barcode easily allow a person to choose which elements of their status to share. [...] The 2D Barcode would not support the data minimisation principle.”

- Firstly, there is a careful balance to be struck when considering data minimisation. In particular when the risks of exclusion are concerned. We would be very interested to see any evidence/assessments that the Home Office has which support that data minimisation should override a physical backup of their immigration status. Especially when considering the findings of the Central Digital and Data Office.²
- Secondly, the data minimisation principle appears to be overstated. Whether an employer, a landlord or another entity checks someone’s status via View & Prove, they all see the following information:
 - Date of birth
 - Full name
 - Photograph
 - Date until which they have the right to work/rent/have leave to remain
 - Legal basis of status
- British citizens use their passports to prove their right to work, rent and access to other services subject to the Compliant Environment, and the data minimisation principle is not applied to them.

9. **Multiple 2D Barcodes for data minimisation**

“While it may be possible to have multiple 2D Barcodes for different purposes, this may be confusing to users”.

- Again, it is important to consider the QR code proposal against the View and Prove status quo. There are currently three varieties of View & Prove which is creating confusion to users. We have received reports from people struggling to prove their rights to access services, some of which will be down to the wrong type of View & Prove code having been produced, or the wrong checking URL having been used.
- Even if multiple 2D Barcodes were to be used, selecting the correct one would be fundamentally the same as the current requirement to select the correct code and the correct URL. The current NHS app already allows people to choose whether to show a QR code for domestic or international use, for example.
- As such, the risk of confusion appears equal between the solutions but given the wider use of QR codes in society and familiarity with them the preference arguably tips in favour of them.

² <https://www.gov.uk/service-standard-reports/prove-your-right-to-work-beta>

10. **Delivering functionality improvements**

“Any improvements to user experience or functionality of the online service can be released on an ongoing basis, and all users will benefit. With a more static 2D Barcode solution, such iterative improvements will be harder to deliver.”

- It is important to consider that apps are upgraded all the time, industry wide, so the scanning app used in this proposal would be no different. In fact, the user experience of frequent ongoing changes to View & Prove without notification or audit can be problematic in and of itself. Organisations creating helpful videos to guide people through the process often find their videos have become out of date as the process changes.

11. **Requirement to use an app and mobile device (repeat from point 6 above)**

“...the third party wishing to check the holder’s status would need to use a mobile phone with a bespoke app to scan the 2D Barcode [...] this offers little advantage over the current process, and has the disadvantage of requiring the third party to obtain the app and a suitable mobile device to run it on.”

- The proposal offers a fundamental advantage over the current process when considering the citizen who is obligated to repeatedly prove their lawful status in the UK in order to access employment, housing and other services. The proposal takes the burden of technology away from citizens, many of whom are digitally excluded, and leaves only a burden on the third party wishing to check the holder’s status. This would be a huge advantage and improve people’s quality of life and the service provided by the Home Office.
- We say it is self-evident that the rate of digital exclusion amongst the population needing to prove their status is vastly higher than amongst the (in any case far smaller) population of third parties such as employers, landlords or other corporate or state entities required to check someone’s status.
- Furthermore, obtaining an app on a smartphone is something which is performed with extreme ease on a near-daily basis by most smartphone users. In any case it is only required to do so once - the first the time someone performs their first right-to-work check for example - rather than at every check.
- Research shows that ownership of PCs, laptops and tablets continues to decline across the world³, with smartphones frequently being the primary and sometimes only digital device owned by many internet users - as such the requirement to have a smartphone for this proposal cannot be seen as a barrier.
- Given the above, we believe you will agree that performing a scan with an app on a smartphone is indeed far easier than navigating to a gov.uk URL and typing in or pasting a code along with a date of birth.

12. **Cost to the taxpayer**

“Developing and maintaining the app would carry a cost to the taxpayer, while delivering no real benefit over the current process.”

- See above for an explanation of why we disagree that this will not deliver any benefit over the current process.
- Ultimately, anything the government does carries a cost to the taxpayer. The cost of our proposal would be minimal compared with the cost of issuing millions of citizens with a biometric residence card, which was costed by the Government during the debates around

³ <https://www.emarketer.com/content/global-media-intelligence-report-2021>

the Immigration and Social Security Coordination Bill. The secure QR code proposal establishes solutions to the problems View and Prove and its associated telephone line have given. The real benefit is to the user and the gaps in the service provided so far.

- We would invite you to consider that the cost argument can only be used within a thorough impact assessment, where different solutions are compared to address the problem. Your letter does not provide alternatives to addressing the current problems arising from View and Prove and its associated telephone line.
- Your letter does not consider the costs still to be incurred to solve the problem of all foreign carriers and airports being able to check the immigration status of travellers to the UK once biometric residence cards/permits are retired. In contrast, our proposal provides a solution which seamlessly integrates with the increased need for checking healthcare records via the same internationally recognised, secure QR code technology.

13. **Checking current immigration status**

“If the app did not connect to the person’s live immigration status record, the key principle that the person’s current immigration status would be checked is lost. An app designed to work without checking a person’s immigration status record would need to store an up to date record of all valid 2D Barcodes. The amount of data which would have to be stored, the necessity of constantly updating the stored data, and the security risk of storing the data of millions of individuals on a personal device, make your suggestion of adopting this approach unfeasible.”

- This paragraph demonstrates a misunderstanding of our proposal. We had anticipated it and addressed it multiple times within our proposal in Q1.10, Q1.15, Q3.1 and Q3.2.
- In particular, we stated that **“Note, the app will not contain the revoked QR codes themselves, only their identifiers.”** It is not the case that the data of millions of individuals is held on a personal device.
- Revoke-list functionality is widely used - see the example we quoted in our proposal of the London Underground with regard to contactless payment cards, where each gate holds a cache of up to three million encrypted card numbers that should be refused.

14. **Sharing of 2D barcodes without face-to-face contact**

“...the 2D Barcode and app reader approach implies face-to-face contact between the individual and the third party wishing to carry out a check. Share codes can be easily generated and passed on by email, written down, or read out over the phone, minimising the face to face contact required - an important advantage given the current COVID19 pandemic. Passing on a 2D Barcode by and or over the phone would be impossible, and 2D Barcodes are more difficult to add to an email than simply typing a code or using the share facility in the relevant checking service.”

- You will of course be aware that the Covid-19 adjusted temporary advice⁴ for employers carrying out right to work checks require the use of video calls, and similarly for right to rent checks⁵.
- Our proposal made clear (our emphasis to show relevance to this point): *“The citizen could show the service provider their QR code in any number of ways – if they were meeting face-to-face the citizen could hand over the paper document, or show the code from their phone. **They could display the code in an online meeting.** Or they could send the document to the provider electronically or by post. In other words, this would work exactly as if the user*

⁴ <https://www.gov.uk/guidance/coronavirus-covid-19-right-to-work-checks>

⁵ <https://www.gov.uk/guidance/coronavirus-covid-19-landlord-right-to-rent-checks>

needed to show proof of a British passport or physical residence card but safer, since the employer or landlord could be sure that the code is authentic.”

- Indeed we have tested ourselves that a barcode can be easily held up in a video meeting and scanned by another meeting participant, and would argue that this is easier than reading out a code which can be (and frequently is) misread or mistyped.
- It is as easy to scan a card with a barcode and email it to someone as it is to scan a passport and email it to someone.

15. Expiry dates of barcodes

“If 2D Barcodes did not have an expiry date, as proposed, once a person had a copy of a 2D Barcode, they could use it any time to check a person’s status, even when they had no reason to do so. If 2D Barcodes expired after a set period, the 2D Barcode reader would need constant refreshing with the list of expired codes.”

- It is not correct to say that we proposed the codes would have no expiry date. We of course recognise that codes need an expiration date, and indeed clarified in an email to the Home Office View & Prove team that we would ideally like to see a ten year expiry for settled status, and the full expiry time for pre-settled status - in line with other identity documents and biometric residence cards.
- It is not correct that a Barcode reader would need to be supplied with a list of expired codes. We believe you may have confused the concepts of expiration and revocation? An expired code would be automatically recognised as expired by the scanner because the expiration date is programmed into the barcode itself.
- We would be grateful if you would clarify the point raised that someone could use a barcode at any time to check a person’s status even when they had no reason to do so. Someone could also look at the retained photocopy of a British person’s passport, or the retained PDF of someone’s View & Prove check, at any time even when they had no reason to do so.

16. Regular logging into UKVI account

“We also believe there are clear advantages to a person regularly logging into their UKVI customer account and checking the contact and status information held about them before sharing. If the person spots any issues, they can resolve these by contacting the UKVI Resolution Centre before sharing their status. A person sharing a persistent 2D Barcode would not necessarily check their online records first. Therefore they may share a status they did not believe to be correct before having the opportunity to realise there was a potential problem and address it.”

- A person would only need to visually inspect their document to see if there was anything incorrect about their status information, therefore we do not understand the point that is being raised here.
- Contact details are not shared with the third party in any case.
- The evidence base supports that it is precisely the need to log into an account (and therefore engage with technology) that is so problematic for digitally excluded people. Hence the proposal for a secure QR code.

17. UKVI Resolution Centre as mitigation for online-only status

“We acknowledge some users may find it harder to access their information online. In such circumstances they can call the UKVI Resolution Centre, to have their status information explained to them, and if required, a share code generated for them, which they can then pass on to a

checking organisation. We believe this meets the need to provide a non-digital alternative for individuals who cannot access the online service.”

- EU citizens have encountered numerous problems accessing the UKVI Resolution Centre, which we have written⁶ to the Home Office about:
 - In July 2021 we wrote about the confusion between the UKVI Resolution Centre (UKVI RC) and the EU Settlement Resolution Centre (EUSRC). The UKVI RC was charging people 69p a minute, requiring a £5 pre-authorisation on a debit or credit card.
 - We wrote a follow-on letter, again in July 2021, that the opening hours of the UKVI RC were not as advertised in the View & Prove guidance, and instead of Mon-Fri 8am-8pm, Weekends 9:30am-4:30pm, the UKVI RC was only open from 9am-4:45pm on weekdays, and closed at weekends. Furthermore, staff at the UKVI RC said they were unable to help anyone with EUSS status problems, and informed people to hang up and call the EUSRC instead.
 - Both letters raised the long wait times and reports of people being unable to get through. In response we were told that more than 1.5 million callers have been helped by the EUSRC - which does not address the issue of those callers who cannot get connected with the EUSRC.

- An FOIA request revealed that over the 12 months of November 2020 to October 2021, **56% of calls** to the EUSRC were not able to be successfully connected. We wrote to the Home Office about this in December 2021. The reply in January 2022 stated that the SRC has handled over 2 million calls and emails since going live. Again, this does not address the vast number of calls that were unanswered - the FOIA request showed that in 12 months, over 800,000 calls could not be connected.

- Furthermore, for digitally excluded people, those we are most concerned about, these helplines are not easy to find. Fewer than a third of people who report problems to us answer our form question “Are you aware of the helplines available through the EU Settlement Resolution Centre or the UK Visas & Immigration Contact Centre?” with ‘Yes’. It is important also to state that people who report to us via an online form are by definition less likely to be digitally excluded in the first place.

- There are numerous situations in which a telephone helpline could not possibly replace the existence of a physical card held on a person. One only needs to think of someone being admitted to hospital, where those accompanying the person do not know about that person’s status or the existence of the UKVI RC or the EUSRC.

- We cannot see that either the UKVI RC or the EUSRC meets the need for a non-digital alternative for individuals who cannot access the online service. The evidence we have acquired to date supports this. This makes the case stronger for a secure QR code alternative.

⁶ <https://www.the3million.org.uk/library>

18. Proposal does not satisfy security and data protection requirements

“The online service is secure, protects personal data, gives checkers confidence in the status information, and protects against fraud. Overall, the proposal does not satisfy the requirements set out above.”

- The proposal makes clear in detail how it is secure, protects personal data, gives checkers confidence in the status information and protects against fraud. We would be grateful for details as to why this is not the case.

19. Simpler implementation

“We also considered whether the 2D Barcode could be used in a simpler implementation as a security feature to validate a document containing status information. However, unless the code also contains information about the rightful holder, there would be a risk of a genuine code being cloned onto a false document, or a genuine document could be obtained and used by a person who was not its rightful owner.”

- This paragraph unfortunately misunderstands the proposal. Our proposal uses the barcode BOTH as a security feature to validate a document containing status information, AND contains information about the rightful owner. To conclude otherwise produces a false dichotomy.
- There is no risk of a genuine code being cloned onto a false document, as the third party scanning the code would see that the details within the code would not match the details on the document. We anticipated and addressed this in Q2.2 and Q2.4 of our proposal.
- Likewise, the risk of the genuine document being obtained and used by a person who was not its rightful owner is exactly the same risk as someone obtaining a passport belonging to someone else. We anticipate and address this in Q1.10 of our proposal.

20. Improving services based on feedback from users

“Please be assured we take such suggestions seriously and are committed to continuously improving our services based on feedback from users. As an example... the validity duration of ... share codes has been increased from 30 to 90 days.”

- We raised this 30-day issue as a problem in our second report to the Independent Monitoring Authority, which was shared with the Home Office on 19 August 2021. Our recommendations included *“Provide a solution to the problem where a government department is not processing applications within 30 days yet is requiring share codes which expire after 30 days.”*
- We were very pleased to see this change but note that the software change from 30 to 90 days was announced on 17 February 2022 - a full six months after we raised it.

Kind regards,

Monique Hawkins

Policy and research officer, the3million