REPLIES OF THE EUROPEAN COMMISSION

TO THE EUROPEAN COURT OF AUDITORS' SPECIAL REPORT

Tools facilitating travel within the EU during the COVID-19 pandemic

Relevant initiatives with impact ranging from success to limited use

Contents

This document presents the replies of the European Commission to observations of a Special Report of the European Court of Auditors, in line with Article 259 of the Financial Regulation and to be published together with the Special Report.

I. THE COMMISSION REPLIES IN BRIEF

To facilitate free movement in the EU and protect public health during the COVID-19 pandemic, the Commission, in close coordination with Member States, developed a range of digital tools. These tools included the EU Digital COVID Certificate[1], a gateway that connected national contact-tracing applications across the EU, and efforts to promote a harmonised approach to passenger locator forms (PLFs).

The EU Digital COVID Certificate is a common framework for the issuance, verification and acceptance of interoperable certificates for COVID-19 vaccination, test or recovery. EU Digital COVID Certificates are accepted in all Member States, making it easier for EU citizens to travel during the pandemic. Developed in close cooperation with Member States experts represented in the eHealth Network and the Health Security Committee[2], the Commission paid particular attention to ensure that the EU Digital COVID Certificate reflects fundamental EU values and principles, such as non-discrimination, protection of personal data, privacy, security and openness.

The EU Digital COVID Certificate has been a crucial element in Europe's response to the COVID-19 pandemic. By September 2022, more than 2 billion certificates were issued in the EU/EEA alone. Its success also served to accelerate the digitalisation of healthcare across the Member States. The Commission and Member States are reflecting how the technical infrastructure underpinning the EU Digital COVID Certificate could potentially be used for other use cases in the future. The EU Digital COVID Certificate also attracted considerable interest from countries outside the EU. As of October 2022, 49 third countries and territories across five continents have joined the system[3], after their systems had been deemed equivalent to the EU Digital COVID Certificate framework[4].

The EU Digital COVID Certificate framework drew inspiration from the work carried out to develop the contact-tracing gateway. Work on new solutions for digital contact-tracing had begun already in April 2020, culminating in the common EU toolbox for Member States on mobile applications to support contact-tracing in the fight against COVID-19[5]. In September 2020, the Commission deployed a contact-tracing gateway, and the first countries started to connect their national contact-tracing applications to this gateway in October 2020, enabling users to travel abroad using their national contact-tracing application, hence supporting cross-border contact-tracing.

---

[1] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic. Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0953

[2] https://health.ec.europa.eu/health-security-and-infectious-diseases/preparedness-and-response/health-security-committee-hsc_en

[3] Full list available at: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en#recognition-by-the-eu-of-covid-certificates-issued-by-third-non-eu-countries

[4] As provided for by Article 8(2) of Regulation (EU) 2021/953. Switzerland is connected to the system by virtue of a decision adopted on the basis of Article 3(10) of Regulation (EU) 2021/953. Iceland, Liechtenstein and Norway are connected directly as a result of the incorporation of Regulation (EU) 2021/953 into the EEA Agreement.

[5] https://health.ec.europa.eu/system/files/2020-04/covid-19_apps_en_0.pdf

The contact-tracing gateway reached its peak in March 2022, when approximately 700 000 keys were uploaded on a single day.

In addition to the successful rollout of the EU Digital COVID Certificate, contact tracing by means of PLFs was a central element in the fight against SARS-CoV-2. The Commission promoted a harmonised approach to PLFs in two ways. It supported the work of the EU Healthy Gateways to develop a common PLF template and application – the EU dPLF[6] – to facilitate the use of a similar digital PLF across the EU[7]. In parallel, it developed a PLF exchange platform to enable the rapid and automatic exchange of passenger data among participating Member States. Since 1 June 2021, Member States were thus able to connect to this platform and to exchange passenger data from across all the transport modes for which they collected PLFs.

II. COMMISSION REPLIES TO MAIN OBSERVATIONS OF THE ECA

1. The development of the contact-tracing gateway

For the contact-tracing gateway, the Commission conducted detailed consultations with Member States[8]. This resulted in the eHealth Network adopting a common EU toolbox for Member States on mobile applications to support contact-tracing in the EU's fight against COVID-19[9], interoperability guidelines[10], specifications for contact tracing applications[11] and the contact tracing gateway[12].

However, national strategies to fight against the COVID-19 pandemic varied across Member States and not all decided to implement contact-tracing applications. Most Member States supported the roll out of contact-tracing applications that were interoperable across borders, with 19 countries out of 22 being connected eventually to the contact-tracing gateway. Those that opted for technologies that were not compatible with the contact-tracing gateway relied on the common EU toolbox and were closely involved in the EU cooperation in this area.

2. The use of the EU passenger locator form tools and the contact-tracing gateway

The success of contact-tracing applications and, as a consequence, of the contact-tracing gateway, largely depended on their adoption by the wider public. While the volume of downloads was not

---

[6]   European Union digital Passenger Locator Form.

[7]   Accessible here: https://app.euplf.eu/

[8]   Paragraphs 28-29, Figure 3, ECA Special Report XX/2022.

[9]   https://health.ec.europa.eu/system/files/2020-04/covid-19_apps_en_0.pdf

[10]   https://health.ec.europa.eu/system/files/2020-05/contacttracing_mobileapps_guidelines_en_2.pdf

[11]   https://health.ec.europa.eu/publications/ehealth-network-guidelines-eu-member-states-and-european-commission-interoperability-specifications_en

[12]   https://health.ec.europa.eu/publications/technical-specifications-interoperability-contact-tracing-apps-ehealth-network-guidelines-eu-member_en

uniform across Member States, contact-tracing applications were downloaded voluntarily over 74 million times (as of October 2021), surpassing in, at least, 14 countries the equivalent of 15% of their population. Due to the high standards for data protection and security of the contact-tracing applications, monitoring the actual use by users is very limited. However, preliminary findings of an independent study on lessons learned, best practices and epidemiological impact of the common European approach on digital contact tracing suggest that the total number of downloads by July 2022 in EU/EEA countries was almost 170 million. The uptake of the applications also depended strongly on the promotional campaigns managed by Member States in addition to other non-pharmaceutical measures (e.g. keeping distance, mask-wearing, hand hygiene, etc.) citizens were asked to take to slow down the spread of COVID-19).

Once the pandemic is over, should the need arise to reuse the contact-tracing gateway, the same legal instrument that was used for its original deployment could be used again[13]. In the context of the European Health Union package[14], the Commission extended the mandate of the European Centre for Disease Prevention and Control (ECDC) to include automated contact-tracing tools[15] which will give the ECDC the possibility to develop and deploy, as needed, new tools for cross-border digital contact-tracing.

It is important to underline that Member States were under no legal obligation to collect PLFs. The use of such tools remains voluntary. In addition, all the Member States that expressed interest in joining the PLF exchange platform were able to do so.

3. The development of a revocation mechanism for the EU Digital COVID Certificate

To help safeguard public health, there may be a need to revoke EU Digital COVID Certificates[16] if they have been issued erroneously, as a result of fraud or following the suspension of a defective COVID-19 vaccine batch. The EU Digital COVID Certificate Regulation already provides that its trust framework may support the bilateral exchange of certificate revocation lists, which are lists that contain the unique certificate identifiers of revoked certificates[17]. Member States were therefore able to quickly invalidate fraudulently issued certificates by using the system's Business Rules functionality, that is, a set of rules that is embedded into the verification software.

The EU Digital COVID Certificate Regulation clearly designated the unique identifier as part of the certificate dataset to be used for revocation purposes. The Commission and the Member States decided to study the possibility to further facilitate the cross-border automatic exchange of certificate revocation lists via the central EU Digital COVID Certificate Gateway. This provided a flexible solution, giving Member States the possibility to choose the technological approach which suits their needs better.

---

[13] Implementing Act of Article 14 (eHealth Network) of the Cross-border Healthcare Directive (2011/24/EU).

[14] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-health-union_en

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0726

[16] See paragraphs 44 to 46, ECA Special Report XX/22.

[17] Article 4(2) of the EU Digital COVID Certificate Regulation.

The modalities of this revocation process are set out in Commission Implementing Decision 2022/483 of 22 March 2022[18]. There are two parts to the technical specifications of the revocation mechanism: one part pertains to the EU Digital COVID Certificate Gateway, and is binding in its application. The other part relates to how Member States distribute the revocation lists from their national infrastructure to the verifier applications, and is non-binding. For the latter, Member States are free to choose among a range of options, all of which take privacy concerns into account.

4. Security controls and fraudulent certificates

With regard to the security of the EU Digital COVID Certificate system[19], the Commission, as the operator of the EU Digital COVID Certificate Gateway, is responsible for ensuring state-of-the-art security to protect the system from risks, vulnerabilities and malicious actors. An 'onboarding' process is applied to all participating countries. The Commission rigorously verifies participating countries' compliance with the security requirements for onboarding to the EU Digital COVID Certificate Gateway before connecting the country concerned. Such testing is carried out to verify that all security measures needed to connect safely are in place.

The responsibility for the security controls at the level of the issuance of EU Digital COVID Certificate and related connection to the national backend infrastructure (the national system connected to the central EU Digital COVID certificate gateway) lies with the Member State or third country. Participating countries have to comply with relevant cybersecurity and data protection legislation – whose enforcement is in the hands of specific national authorities – when establishing and operating their national systems and services. The Commission systematically requires all Member States and third countries to submit a self-assessment to provide additional assurance that the country has taken specific account of particular risks. Any failure to adhere to any of these requirements prevents onboarding to the EU Digital COVID Certificate framework.

Any fraudulent activities related to the EU Digital COVID Certificate – such as the issuance of technically valid certificates by persons with legitimate access to the system without the underlying medical event having taken place – are the result of criminal behaviour punishable under national law, and do not constitute cyberattacks. It is necessary to distinguish between security controls at the level of the national backend infrastructure and the malicious intent of those operating the certificate's issuance systems at national level. National backend systems were not compromised and unauthorised parties did not access the national backends.

From a cybersecurity point of view, the EU Digital COVID Certificate is safe. The risk of authorised personnel having lawful access to the issuance systems in order to issue technically valid but fraudulent certificates is managed by participating countries authorities in accordance with their national legislation and access control procedures.

---

[18]   Commission Implementing Decision (EU) 2022/483 of 21 March 2022 amending Implementing Decision (EU) 2021/1073 laying down technical specifications and rules for the implementation of the trust framework for the EU Digital COVID Certificate established by Regulation (EU) 2021/953 of the European Parliament and of the Council. Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022D0483

[19]   See paragraphs 51 to 56, ECA Special Report XX/22.

5. The EU Digital COVID Certificate as an international standard and travel facilitator

Member States used the EU Digital COVID Certificate extensively[20] and it was effective in facilitating travel[21]. The EU Digital COVID certificate was also adopted in a timely manner[22]. The EU Digital COVID Certificate has been a crucial element in Europe's response to the COVID-19 pandemic and has rapidly become a standard in Europe and beyond. It has had a positive impact on free movement at a time where Member States were limiting its exercise on grounds of public health.

The positive impact of the EU Digital COVID Certificate system extends beyond the EU, as it has developed into a global standard firmly based on the EU's values of openness, security and data protection. This is evidenced by the strong interest of third countries in being connected to the EU Digital COVID Certificate system, the only functioning COVID-19 certificate system operational at international level on a large scale. This success has contributed to the resumption of safe international travel and global recovery.

The Commission remains fully committed to a return to unrestricted free movement as soon as possible. As of October 2022, all Member States had lifted intra-EU travel restrictions, including the need to be in the possession of an EU Digital COVID Certificate. While the EU Digital COVID Certificate has demonstrated the capacity of EU institutions and Member States to deliver tangible results to the benefit of EU citizens, its end will be an indication that the pandemic, and the restrictions linked to it, have been overcome.

III. COMMISSION REPLIES TO THE RECOMMENDATIONS OF THE ECA

1. Recommendation 1 – Address the reasons for the low uptake of EU digital passenger locator forms
(Target implementation date: December 2023)

The Commission accepts this recommendation and will consult the Member States through the Health Security Committee and collaborate with the ECDC on its implementation.

2. Recommendation 2 – Streamline communication on incidents linked to the EU digital Certificate
(Target implementation date: June 2023)

The Commission accepts the recommendation.

A Security Committee was established in November 2021 under the auspices of the eHealth Network. Its purpose is to analyse any incidents after an issue has been adequately contained to discuss and

---

[20]   See paragraphs 69-70 and Figure 4, ECA Special Report XX/22.

[21]   See paragraphs 72 and 74, Figure 5, ECA Special Report XX/22.

[22]   See paragraphs 28 and 35, ECA Special Report XX/22.

disseminate lessons learned, and to recommend security improvements. The Committee is not a first line of defence but an information sharing mechanism between competent authorities solely dedicated to the EU Digital COVID Certificate. For security reasons, the Committee cannot intervene and disseminate information before the incident is appropriately handled and sufficiently contained at the national level.

The Commission will analyse what further steps can be taken to strengthen participation in the Committee as well as to enhance information sharing between competent authorities.

The Commission considers this Security Committee as an integral and effective part of the overall design architecture of the EU Digital COVID Certificate, and will therefore incorporate this into any reactivation plan that will form part of the instrument outlined in the reply to Recommendation 3 regarding the re-use of the tools covered by this report.

In this context, as part of its actions under Recommendation 3, the Commission will also analyse how the Security Committee and its communication mechanisms might have to be adapted and extended to properly serve in a harmonised way any additional needs of security incidents associated with future pandemic crises, beyond the one of COVID-19.

3. Recommendation 3 – Prepare relevant EU tools for future crisis

a) **Identify those EU tools created during the COVID-19 pandemic that have been most useful to citizens and the Member States and prepare procedures for reactivating them quickly in the event of future emergencies (Target implementation date: September 2023)**

The Commission accepts recommendation 3(a), but notes that this analysis will necessarily depend on the tool and crisis concerned.

In its Communication on a contingency plan for transport[23], the Commission noted that if a similar crisis to COVID-19 occurs, the Commission and Member States should build on the experience in developing a common template for EU digital passenger locator forms and a platform to share passenger data for cross-border contact tracing. The tools developed at EU level for that purpose should be reactivated rapidly and easily if necessary.

In addition, the Commission adopted, on 19 September 2022, a proposal for a Regulation establishing a Single Market Emergency Instrument[24]. This instrument aims to put in place a flexible and transparent mechanism to respond quickly to emergencies and crises that threaten the functioning of the single market. The objective is to ensure coordination, solidarity and coherence of the EU crisis response and protect the single market's functioning, ensuring, in particular, the continued free movement of persons, goods, and services. The Regulation would also entitle the Commission and the Member States to set up interoperable digital tools or IT infrastructures supporting these objectives.

At the same time, it is important to emphasise that some of the EU tools analysed, in particular the EU Digital COVID Certificate, were specifically conceived as a response to the COVID-19 pandemic.

---

[23]   COM(2022) 211 final.

[24]   COM(2022) 459 final.

They were partially expressly limited by the co-legislators to the estimated duration of the pandemic as a way to facilitate the right of free movement of EU citizens and their family members during this extraordinary period. This will necessarily have an impact on whether it is appropriate to prepare procedures allowing for their re-activation.

b) Through synergies or simplifications, make the EU tools used to facilitate cross-border contact tracing during crises easier for EU citizens to access (Target implementation date: September 2024)

The Commission accepts recommendation 3 (b). The work will be carried out following the consultation referred to under Recommendation 1, will require the existence of an appropriate legal basis and will depend on the epidemiological situation.

c) Together with Member States, analyse the need for any additional tools to address potential future crises (target implementation date: September 2023)

The Commission accepts recommendation 3(c). In this context, the proposal for a Regulation establishing a Single Market Emergency Instrument is also relevant.