Annex II

Technical procedure to onboard third countries

Contents

1 Introduction

Welcome to the community of EU Digital COVID Certificate (EU DCC) Framework.

The goal of the EU DCC architecture is to establish a trust framework that ensures a secure data exchange between participating countries and by that to achieve the goal of safe free movement.

Your country is planning to become part of the EU DCC framework. This document provides a technical guideline to connect to the EU DCC Gateway. It contains an overview about

- Functional and technical overview of the DCC framework and the related technical documentation (see chapter 2)
- The technical procedure to onboard on the different environments and the support you will receive during this process (see chapter 3)
- The Quality checks which must be passed to have a smooth Go-Live (see chapter 4).

2 Functional and technical overview and technical information

2.1 Functional Overview

The aim for the EU Digital COVID Certificate (EU DCC) framework is to enable the safe free movement of citizens in pandemic situations as COVID-19. Therefore, people need to receive proofs of their health status which could be verified by other countries.

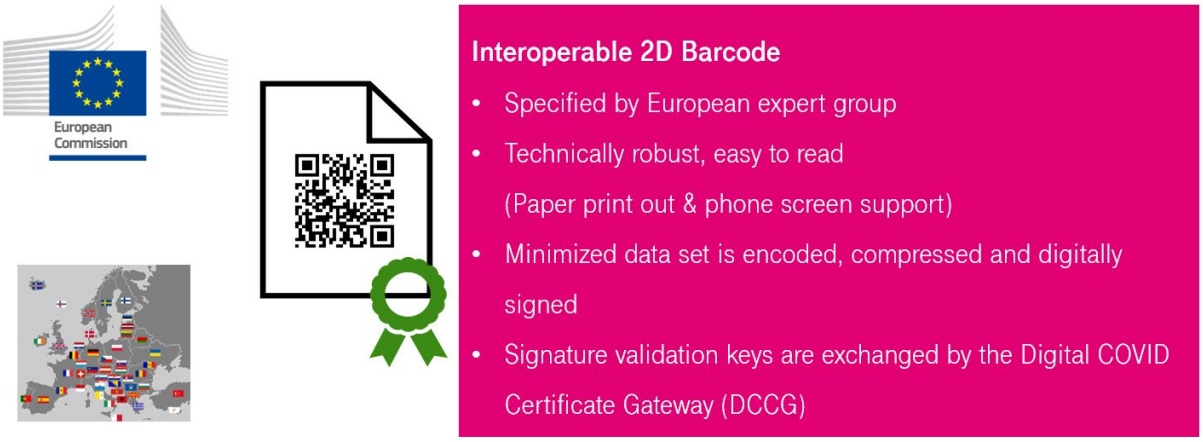

Figure 1: What is the Digital COVID Certificate (DCC)?

In the DCC framework the proof is represented by an interoperable 2D barcode (see Figure 1). It provides an encoded minimized dataset and is digitally signed. Currently there are three types of certificates representing the health status with respect to COVID-19 pandemic:

- **Vaccination certificate:** certificate proving the vaccination status of the citizen
- **Test certificate:** certificate proving the test result of COVID-19 test
- **Recovery certificate:** certificate proving that a citizen has recovered from COVID-19.

To serve the mission of a free movement three key use cases are supported within the DCC framework (see Figure 2):

- **Issuance:** The DCC is only issued by organizations that are entitled by the national health authority. The entitlement is represented by a Document Signer Certificate (DSC) which is used to digitally sign the barcode of the DCC.
- **Portability:** The citizens receive the DCC from the issuing organization either on paper or digitally and stored in a secure wallet app.
- **Verification:** The DCC could be verified by other entitled organizations (e.g. border control) by checking the authenticity of the signature of the DCC using the public key of the DCC issuer.

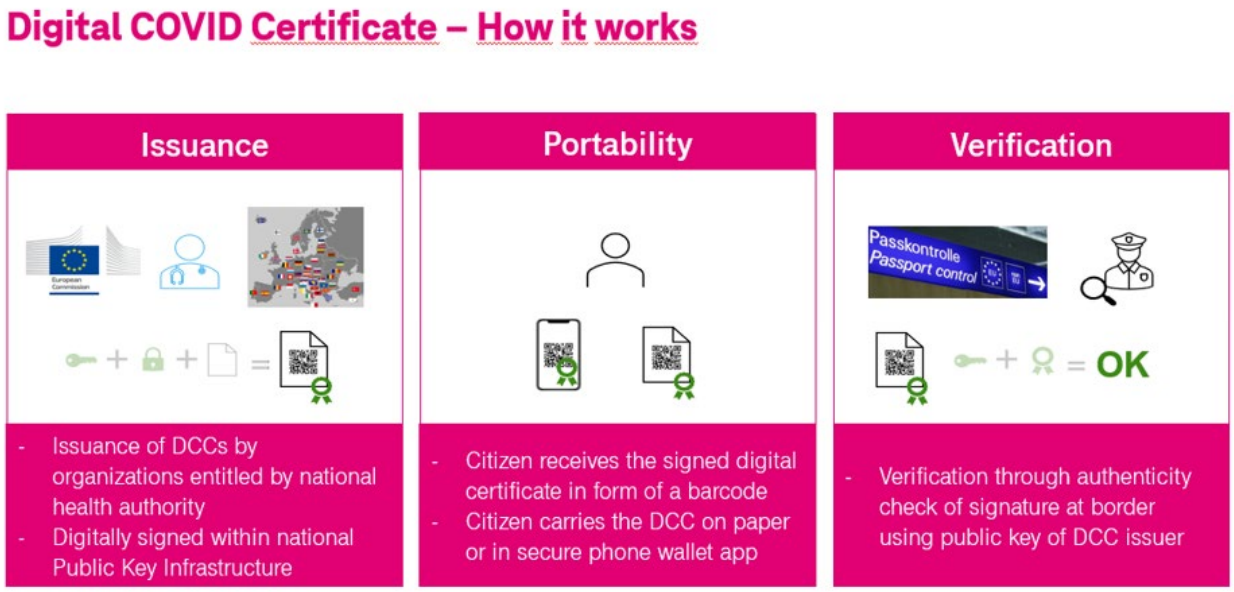

Figure 2: Digital COVID Certificate - How it works

To ensure the interoperability of the issuance of health certificates and their verification the EC together with the Member States has designed and implemented the EU DCC trust framework. This framework allows the secure exchange of information between the participating countries to allow the verification of the DCC with respect to its authenticity and integrity. The full specification for this framework of the EU Digital COVID certificate is available publicly on the eHealth Network website of the European Commission (see [1]):

- https://ec.europa.eu/health/ehealth/covid-19_en.

A detailed overview of the principles and concepts of the trust framework can be found in Interoperability of health certificates - Trust framework (see [2]).

2.2 Technical Overview

In general, the Framework divided into four main components as shown in Figure 3:

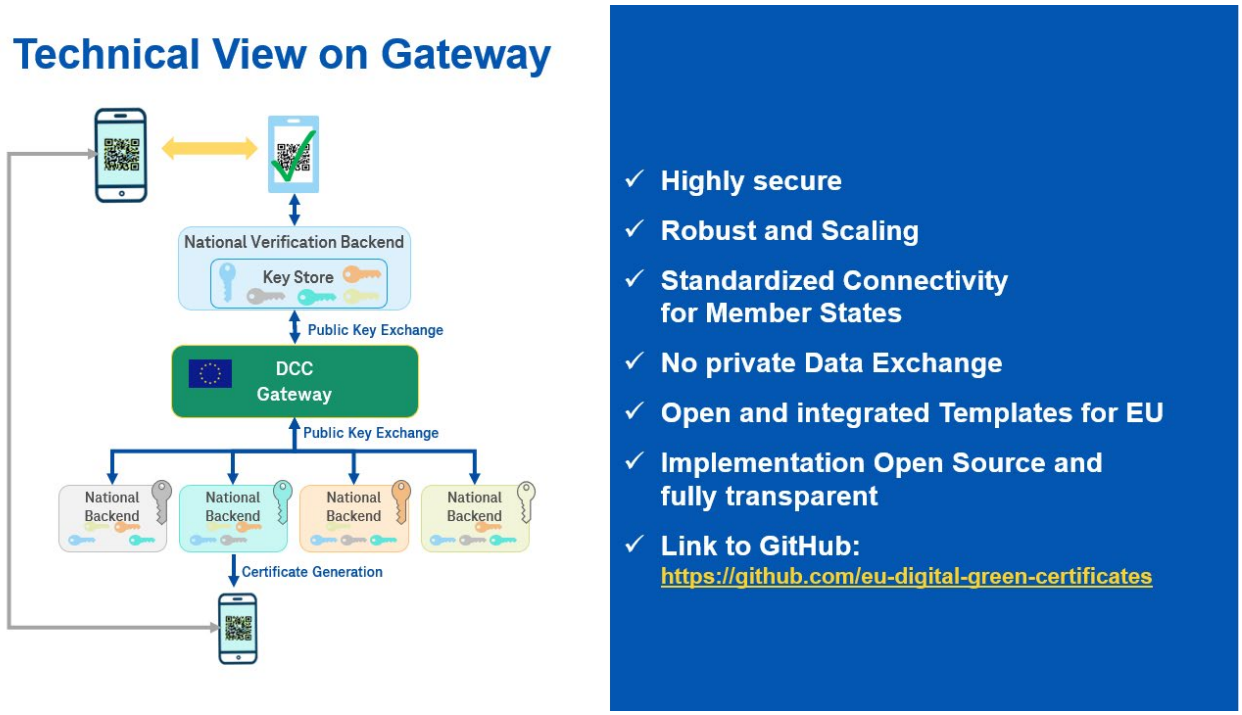

Figure 3: EU DCC Technical View

- **DCCG – Digital COVID Certificate Gateway**
  The Gateway is the central component of the framework. The Gateway is mainly responsible for distributing the public key data of each connected participating country. It is centrally operated by the EC. The National Backends of the participating countries must be connected to the DCCG to ensure the key exchange between the issuing and verification components (see Figure 4). Due to the fact of only holding public key data, which is associated with authorities, there is no personal data stored or processed by the gateway component.

- **DCCA - Digital COVID Certificate Applications**
  There are three different app components, which are combined under the DCCA acronym. These applications must be provided by the participating countries. All applications are available as template open-source implementations on GitHub (see [3]). A joining country may base its national implementation on this openly available source code. The EC however does not provide any support in deploying and operating these applications.

  - **Issuer App**
    With the issuer app, it is possible to create (issue) certificates for a person.

  - **Wallet App**
    The purpose of the wallet app is mainly to store and transport the personal certificates and to provide it for verification.

  - **Verifier App**
    The verifier app is designed to check any given certificate for validity. The verification process uses the public keys distributed by the DCCG to ensure the validity of a Digital COVID Certificate.

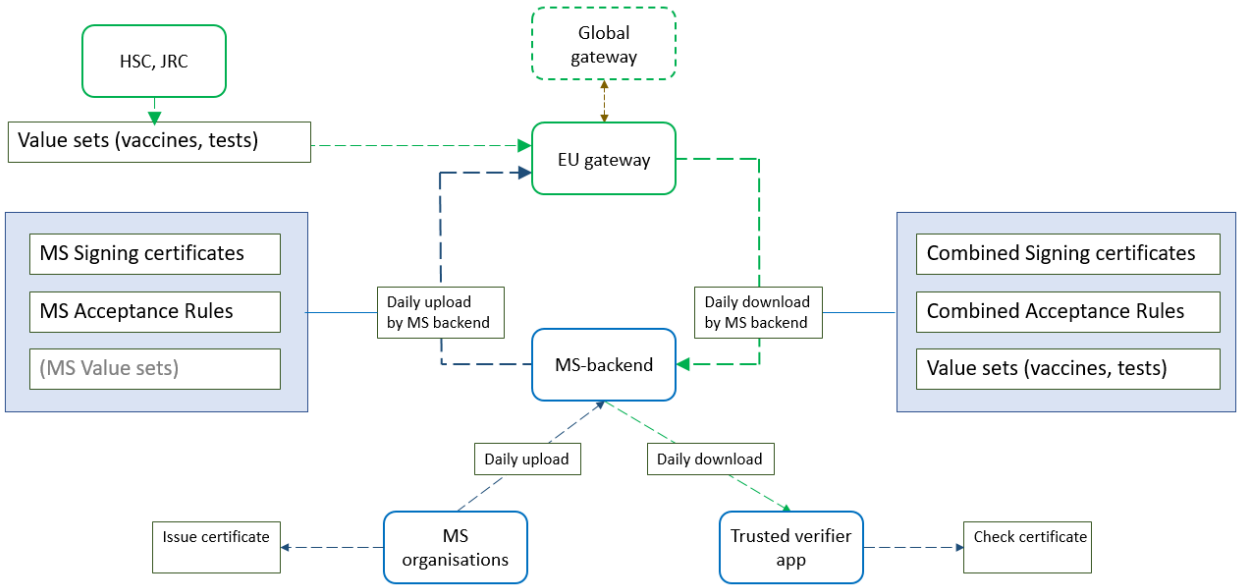

Figure 4: Data exchange between EU gateway and national backend

Hence your national solution consists of following components

- Your national backend
- Depending on the use cases you will support
    - Your issuing service/app
    - Your Wallet app
    - Your validation service/app.

The national backend is the key component you need to provide in order to be able to connect to the EU DCC framework (see Figure 4). Your national backend is communicating with the EU DCC gateway and thus enables the exchange of information between the participating countries.

This results in the following technical use cases your national backend must serve:

- On the one hand, you can upload information from your country to the gateway. This includes:
    - The upload of your Document Signer Certificates (DSCs) which are used by your issuing service to sign the 2D barcodes.
    - The upload of your acceptance rules for 2D barcodes. The DCC gateway supports acceptance rules starting with the release 1.1.
- On the other hand, you can download information from the gateway for use of your verification services. Your backend must distribute this fully autonomously to your verification services. The downloaded information includes:
    - The Document Signer Certificates (DSCs) from other countries. This information allows your verification service to verify the authenticity of a 2D barcode.
    - Acceptance Rules from other countries. This allows that you can check under which conditions your issued 2D barcodes will be accepted by other countries. The DCC gateway supports acceptance rules starting with the release 1.1.
    - Centrally maintained Value Sets (see [4]).

As stated above you can base your national implementation of your applications on the template open-source implementations on GitHub (see [3]). The EC however does not provide any support in deploying and operating these applications.

2.3 Technical specifications and information

The EU DCC gateway is an Open Source implementation. Therefore, the specification is publicly available as well as the code for the template implementation and corresponding documentation.

The full specification for this framework of the EU Digital COVID certificate is published publicly on the eHealth Network website of the European Commission (see [1]):

- https://ec.europa.eu/health/ehealth/covid-19_en.

Within this website, the eHealth Network and the European Commission have published detailed technical specifications describing the mechanisms of interoperability of the key components of the framework:

- Volume 1: formats and trust management
- Volume 2: EU Digital COVID Certificate Gateway
- Volume 3: 2D Barcode Specifications
- Volume 4: EU Digital COVID Certificate Applications
- Volume 5: Public Key Certificate Governance
- EU DCC Validation Rules

To ensure the interoperability for issuing and verification of QR codes these elements must follow a common technical structure. The semantic specification for the underlying JSON schema of the QR codes used for EU DCC (see [5]) and the value sets to be used (see [4]) are given in:

- https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-certificate_json_specification_en.pdf
- https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-value-sets_en.pdf.

Technical information on the schema (see [6]) are provided in:

- https://github.com/ehn-dcc-development/ehn-dcc-schema.

In case of your validation app/service you must ensure that it is backward compatible also to older versions of the JSON schema. The reason for this is that there might be QR codes in the field which were issued with that older version. On the other hand, your issuing service/app must strictly follow the current schema version.

The code of the open source template implementation and the corresponding technical documentation is published on the official GitHub Organization of the EU Digital COVID Certificates (EU DCC) project (see [3]):

- https://github.com/eu-digital-green-certificates.

Following repositories within this project shall be used as a starting point to find relevant information:

- dgc-overview: This repository provides an overview of the EU DCC project and refers to relevant information, especially:

- DGC Public Key Certificate Governance: This document describes the general governance for the Public Key Certificates (see [7] and [8])

Since the source code of the EU DCC Gateway and the source code of the (national) reference implementation are open source, the project is nurtured by contributions of the open source community. The EU DCC community uses following communication channels:

- Slack Workspace LF Public Health: to get in contact with the community please contribute to the channels in this workspace, especially:
  - #eu-digital-green-certificates-dev: get in contact with the community on development related topics (see [9])
  - #eu-digital-green-certificates-schema: get in contact with the community on schema related topics (see [10]).
- GitHub: please report your contributions or detected issues via the corresponding functions in GitHub:
  - Issues
  - Pull requests.

3 Technical onboarding process and support

3.1 General prerequisites

Before getting onboarded onto the EU DCC environment you as new participating country should check on some general prerequisites to ensure a smooth onboarding.

1. **Contact and general agreement with EC on onboarding:** follow the procedure to self-evaluate your solution. The information collected in the Evaluation Checklist is a prerequisite to get onboarded onto the Production Environment of EU DCC gateway.
2. **Availability and compliance of your national solution:** To be onboarded in due time your national solution needs to be fully developed and available. Within the Evaluation Checklist (see [11]) you must confirm the compliance of your national solution with the specifications of the EU DCC framework (see Chapter 2.3 and refer to [1]).
3. **Connectivity of your national solution to EU DCC gateway**: To be technically connected to the environments of DCC gateway you must provide for each environment three types of certificates:
   - NB_{TLS} (Authentication)
   - NB_{UP} (upload)
   - NB_{CSCA} (CSCA identification).

   Please ensure that the certificates are available when you start the onboarding process of the respective environment. The certificates must follow all the Volume 5: Public Key Certificate Governance (see [7]) and following additional policies

   - [reserved for future additional policies, if any].

4. **Request access to circaBC:** For the Acceptance and the Production environment the EC uses the tool circaBC to exchange safely and trustfully the communication certificates NB_{TLS}

(Authentication), NB_{UP} (upload), NB_{CSCA} (CSCA identification) with the countries. The usage of the tool is described in the manual for circaBC (refer to [12]). It is provided to you together with this document and after the preparation call. Please request access to this tool before the onboarding process is started.

3.2 Technical onboarding process onto DCC environments

The EU DCC Gateway universe exists of three different environments for different purposes.

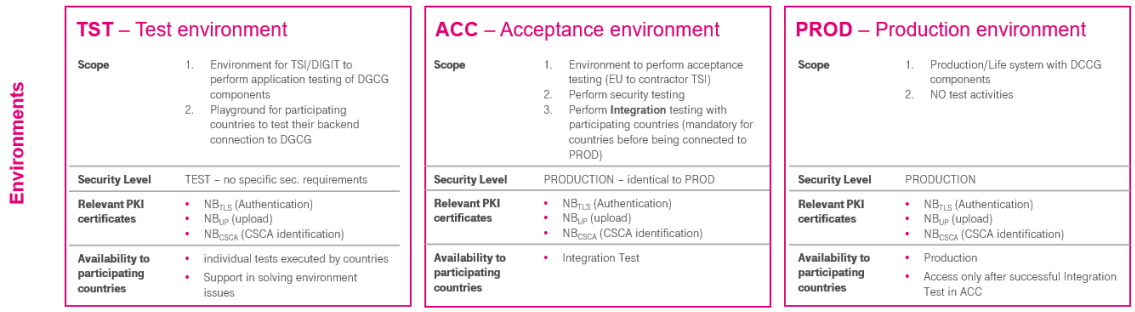

Figure 5: Overview on Environments

Within the repository *dgc-participating-countries* of the EU DCC project you find technical information for the technical onboarding of participating countries, especially:

- Onboarding Checklist: This provides a technical guideline on how to successfully connect to the gateway (see [13]). The organizational process for onboarding is described in chapter 3 *Technical onboarding process and* support.
- Information for the certificate preparation: This provides a guideline to generate Public Key Certificates including minimal required fields (see [14]).

3.2.1 TST – Test environment

The Test environment TST can be used by the participating countries to connect a test instance of their National Backend to a test instance of the EU DCC gateway. Once your country is connected to this environment you can use it for your individual testing purposes.

For the test environment TSI support is limited to the technical connection. TSI will not provide any support for your testing activities, nor will TSI provide analysis or issue resolution for your own developments.

The use of the Test environment mandatory prior to integration test on ACC.

The Onboarding procedure for the Test environment TST is depicted in Figure 6.

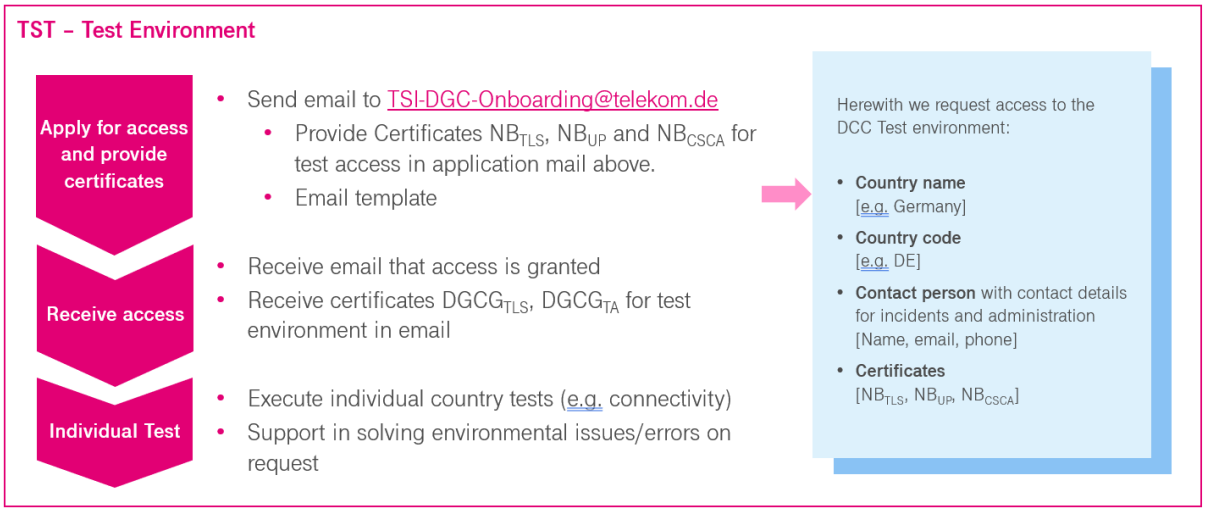

Figure 6: Onboarding procedure for Test environment

As a pre-requisite for establishing connection, you must provide three certificates types:

- NB_{TLS} (Authentication): 1 certificate (see [7])
- NB_{UP} (upload): 1 certificate (see [7])
- NB_{CSCA} (CSCA identification): 1 to n certificate (see [7]).

Please send these certificates to TSI following the procedure in Figure 6. After being configured you will also receive PKI certificates DCCG ➔ MS for Test environment via email

- $DGCG_{TLS}$ (Authentication): 1 certificate (see [7])
- $DGCG_{TA}$ (signature for trust list): 1 certificate.

3.2.2 ACC – Acceptance environment

The Acceptance environment is used especially for the mandatory Integration Test as well as additional Quality Assurance activities with the participating countries (e.g. QR code validation). The testing activities are described in detail in chapter 4. The environment is identical to the Production environment.

TSI will provide support for Integration tests and additional QA activities (see chapter 4). TSI will not provide analysis or issue resolution for your own developments.

Successful testing on the Acceptance environment is **mandatory** with respect to connect to the Production Environment (see chapter 4).

The Onboarding procedure for the Acceptance environment ACC is depicted in Figure 7.

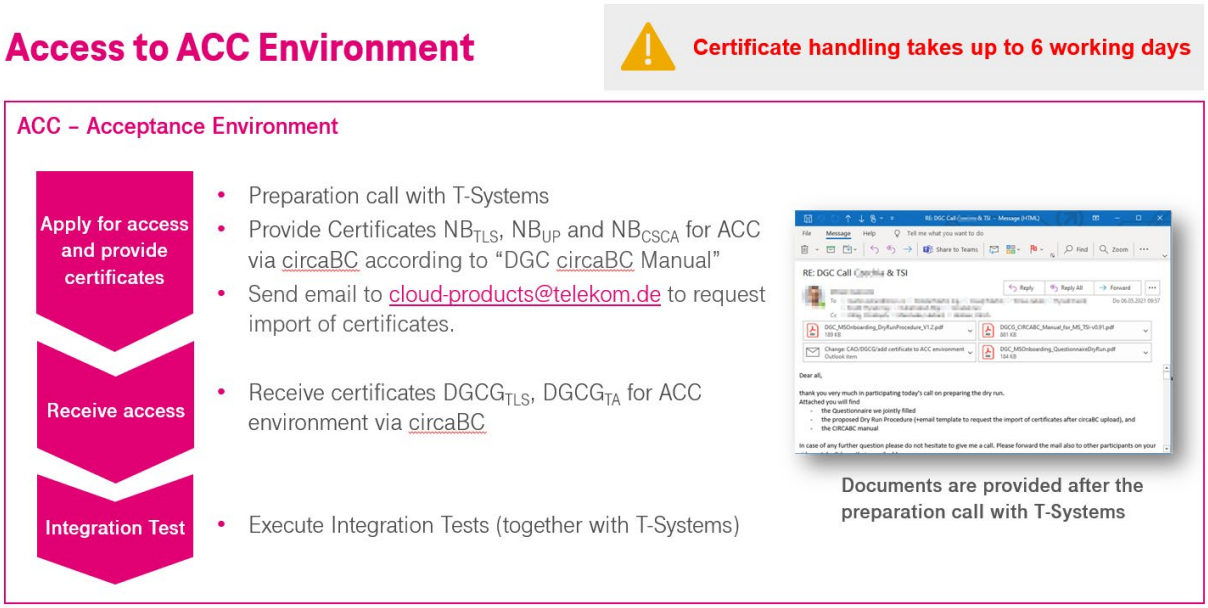

Figure 7: Onboarding procedure for Acceptance environment

The onboarding process is initiated with a preparation call. Within this call the planning and organizational topics with respect to the onboarding as well as to the mandatory Integration Test are aligned. Prerequisite for the preparation call is that a general confirmation from the EC that the onboarding activities with your country can start.

As a pre-requisite for onboarding, three types of certificates need to be provided:

- NB_{TLS} (Authentication): 1 certificate (see [7])
- NB_{UP} (upload): 1 certificate (see [7])
- NB_{CSCA} (CSCA identification): 1 to n certificate(s) (see [7]).

The certificates must be transferred to TSI via circaBC. The manual for circaBC (refer to [12]) is provided to you together with this document and also after the preparation call.

In order to kick-off the technical onboarding process a pre-filled email template need to be submitted (see [15]). You find the email template in the additional documents for this guide. It will be provided to you also after the preparation call.

After being configured you will receive PKI certificates DCCG ➔ MS for Acceptance environment via circaBC:

- $DGCG_{TLS}$ (Authentication): 1 certificate (see [7])
- $DGCG_{TA}$ (signature for trust list): 1 certificate.

The Integration Test finalizes the onboarding onto Acceptance environment. It is described in chapter 4.

3.2.3 PROD – Production environment

The onboarding onto Production environment is the final step.

The Onboarding procedure for the Production environment PROD is depicted in Figure 8.

Figure 8: Onboarding process for Production environment

For Production, the onboarding process is started by submitting the official Application Form (see [16]) to the European Commission (EU-DIGITAL-COVID-CERTIFICATE-COMMITTEE@ec.europa.eu) for approval. Pre-requisites for approval are the provisioning of consistent information within the form and that you successfully passed the Integration Test on Acceptance (see chapter 4). Be aware that the technical onboarding onto Production is only started after approval of your application.

As a prerequisite for the technical onboarding, you must provide three types of certificates:

- NB_{TLS} (Authentication): 1 certificate (see [7])
- NB_{UP} (upload): 1 certificate (see [7])
- NB_{CSCA} (CSCA identification): 1 to n certificate(s) (see [7]).

The certificates must be transferred to TSI via circaBC. The manual for circaBC (refer to [12]) will be provided to you together with this document and also after the preparation call.

After being configured you will receive PKI certificates DCCG ➔ MS for Production environment via circaBC

- $DGCG_{TLS}$ (Authentication): 1 certificate (see [7])
- $DGCG_{TA}$ (signature for trust list): 1 certificate.

The onboarding process is being finalized by a short operational check-up. For this you will receive a short Production readiness questionnaire via email from TSI after you were successfully configured. For the operational check-up you need to download, upload and delete (also known as revocation) a DSC on the productive gateway. If the check-up was successful you will receive welcome mails and the process is finished.

4 Quality Checks and approval for Go-Live

In order to support a smooth Go-Live of the connection of your national implementation with the EU DCC gateway there are a few Quality checks and approvals throughout the onboarding process described in chapter 3.

Individual testing – optional

Participating countries can perform individual testing of their national implementation in integration with a test instance of the EU DCC gateway in the Test environment TST (see chapter 3). This quality measure is optional. Countries can execute tests upon their need. On this environment TSI will support on best effort in case you face problems with the environment, but there is no SLA neither for issue resolution nor for environment availability. TSI will not provide support for your testing activities, nor will TSI provide analysis or issue resolution for your own developments.

Integration Testing - mandatory

Integration Testing on the Acceptance environment ACC (see chapter 3) is a mandatory quality step prior to onboarding onto the Production environment. You are only eligible to get access to Production if you have passed the Integration Test successfully. Integration Test confirms connectivity of your national implementation to EU DCC gateway and especially the functionality of up- and downloading public keys and Acceptance Rules. If you have agreed with EC that you will validate QR codes, then as a mandatory part within the Integration Test the interoperability of your validation app with reference QR codes of other countries is tested. The process of onboarding continues depending on the results of the Integration Test.

The test procedure for Integration Test (see [17]) is available in the additional documents attached to this document and you will also receive it after the preparation call.

Quality Assurance of the QR code interoperability

After you are successfully onboarded on ACC you will be regularly invited to test your validator app in combination with reference QR codes from other countries. This quality measure continues the optional interoperability test from the Integration Testing. Parallel we request that you provide:

- three reference QR codes, one for each type (VAC, TEST, REC)
- issued by your issuing service
- which represents a kind of standard (no special case!)
- signed with a DSC of your country which is available on the gateway in ACC
- which is valid at the time of provision.

The QR codes must be provided via pull request to the QA repository on GitHub (see [18])

- dcc-quality-assurance.

TSI will validate your submitted QR codes

- with respect to formal checks
- check them with the current Validator template app of TSI.

If the check is successful, your submitted QR codes are merged into the main branch of the QA repository on GitHub.

Based on the QA repository you will be regularly requested to test/retest the reference QR codes with the current implementation of your verifier app and provide feedback to TSI.

Parallel to the managed QA repository the EU DCC project on GitHub contain a second repository for QR test data:

- dgc-testdata: this repository (see [19]) contains all kind of test data for QR codes of the countries. This test data is used for individual interoperability tests of the countries as well as to support the automation of the generation and validation tests of the codes. You are kindly requested to contribute as much as you can to these kinds of activities.

Application for access to Production – mandatory

As described in chapter 3 your onboarding onto Production environment is initiated by your submission of the properly filled application form (see [16]) to EC. Within this approval step your eligibility to get access to Production is checked. Your eligibility is among others dependent on the successful execution of the Integration Test on Acceptance environment. The technical onboarding onto PROD is only started if your application is approved positively.

Operational check-up

Your onboarding onto Production environment is closed by successfully passing the operational check-up (see chapter 3). If you have passed it, you reached your initial goal to connect your initial implementation to the gateway.

Welcome on the EU DCC gateway.

References and additional documents

[1] "General specifications EU Digital COVID Certificate," 2021. [Online]. Available: https://ec.europa.eu/health/ehealth/covid-19_en.

[2] "Outline: Interoperability of health certificates - Trust Framework," 2021. [Online]. Available: https://ec.europa.eu/health/sites/health/files/ehealth/docs/trust-framework_interoperability_certificates_en.pdf.

[3] "GitHub eu-digital-green-certificates," 2021. [Online]. Available: https://github.com/eu-digital-green-certificates.

[4] "Guidelines on Value Sets for Digital Green Certificates," 2021. [Online]. Available: https://ec.europa.eu/health/sites/health/files/ehealth/docs/digital-green-value-sets_en.pdf.

[5] "Technical Specifications for EU Digital COVID Certificates - JSON Schema Specification," 2021. [Online]. Available: https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_json_specification_en.pdf.

[6] "Digital Covid Certificate Schema," 2021. [Online]. Available: https://github.com/ehn-dcc-development/ehn-dcc-schema.

[7] "Volume 5: Public Key Certificate Governance," 2021. [Online]. Available: https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v5_en.pdf.

[8] "Digital Green Certificate – Public Key Certificate Governance," 2021. [Online]. Available: https://github.com/eu-digital-green-certificates/dgc-overview/blob/main/guides/certificate-governance.md.

[9] "Slack channel #eu-digital-green-certificates-dev," 2021. [Online]. Available: https://app.slack.com/client/T01382K7DLP/C01UZFNU3M0.

[10] "Slack channel #eu-digital-green-certificates-schema," 2021. [Online]. Available: https://app.slack.com/client/T01382K7DLP/C01V8GX69K5.

[11] *Third Country EU Digital COVID certificate Equivalence Decision procedure (Annex I),* 2021.

[12] "DGCG - CIRCABC Manual for MS," 2021. [Online]. Available: provided during Preparation Call.

[13] "Digital Green Certificate - Onboarding Checklist," 2021. [Online]. Available: https://github.com/eu-digital-green-certificates/dgc-participating-countries/blob/main/gateway/OnboardingChecklist.md.

[14] "Information for the certificate preparation," 2021. [Online]. Available: https://github.com/eu-digital-green-certificates/dgc-participating-countries/blob/main/gateway/CertificatePreperation.md.

[15] *email Template: Change - DGCG CAO DGCG - add certificate to ACC environment.msg,* 2021.

[16] *Third Country EU Digital COVID certificate Equivalence Decision procedure (Annex III),* 2021.

[17] *Procedure for Integration Test of DCCG and National Backends of participating Countries: DCC_Onboarding_IntegrationTestProcedure,* 2021.

[18] *GitHub dcc-quality-assurance,* https://github.com/eu-digital-green-certificates/dcc-quality-assurance, 2021.

[19] "DGC Test Data Repository for Test Automation," 2021. [Online]. Available: https://github.com/eu-digital-green-certificates/dgc-testdata.

[20] "DGCG - CIRCABC Manual for MS," 2021. [Online].

[21] "Technical Specifications for Digital Green Certificates Volume 1"," 2021. [Online]. Available: https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v1_en.pdf.