



# Future of Verifiable Health Credentials Beyond COVID-19

EU Digital COVID Certificate (EU DCC)

*Joint ITU/WHO Workshop - 11 September 2023*

# What is the EU DCC?

- A framework for the common issuance, verification and acceptance of interoperable vaccination, test and recovery certificates
- **Verifiability:** ensure authenticity, integrity and validity



## Governing principles

- 🇪🇺 Governed by the European Commission & Member States
- ⚖️ Equitable
- 🏠 Data protection
- 🔒 Privacy-preserving

- 🛡️ Secure
- © Openness and transparency
- ↔️ Flexible
- ⚙️ Actionable

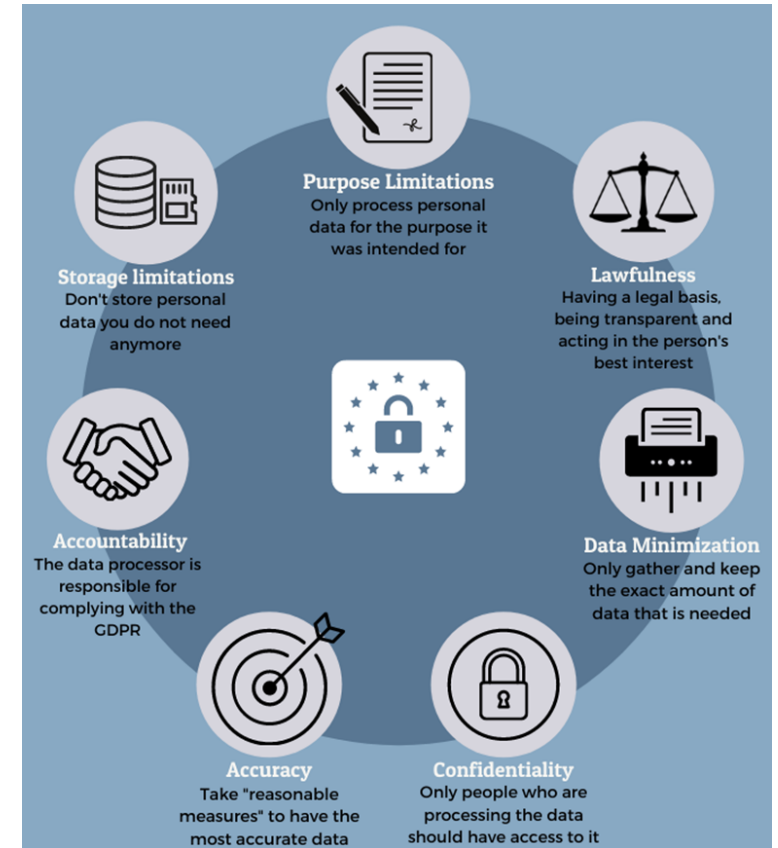
# GDPR: General Data Protection Regulation

Regulation (EU) 2016/679, amended in 2018, lays down rules to process personal data

- Data protection = fundamental right of EU citizens
- Principles to process data →

## Health data: special category of personal data (Art.9)

- Processing and transfer in principle prohibited; exceptions strictly regulated
- Impact on choice of technology for EU DCC and on implementation of revocation feature

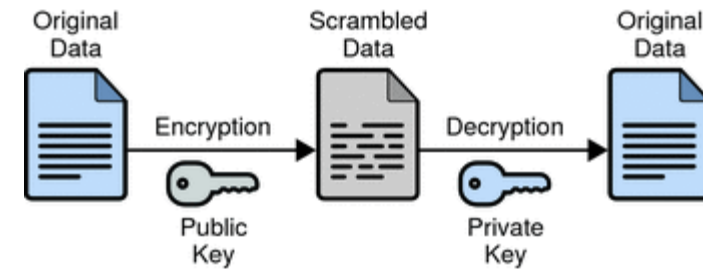


# EU DCC main components



QR code with data

**Public Key Infrastructure** to manage cryptographic certificates



# EU DCC tech specs summary

Common data structure and agreement on the significance of each data field of the payload



Common coordinated data structure is defined through the use of a **JSON schema**

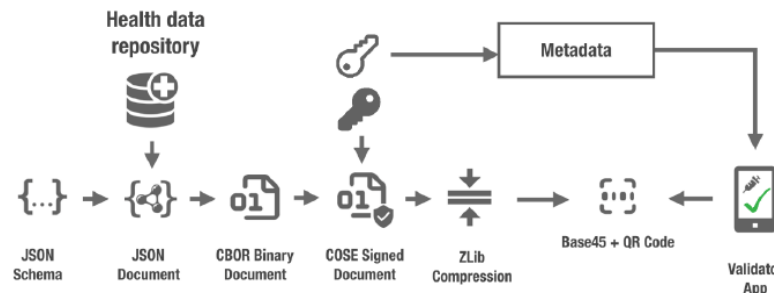
```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema", //example
  "$id": "https://ec.europa.eu/health/dgc/schema/dgc/100.json",
  "title": "Digital Green Certificate",
  "description": "Interoperability Exchange format",
  "type": "object",
  "properties": {
    "person": {
      "description": "The legal name of a person.",
      "type": "string"
    }
  },
  "required": [ "person", "certificateMetadata", "kid", ... ]
}
```

Each QR code contains a **Key Identifier**

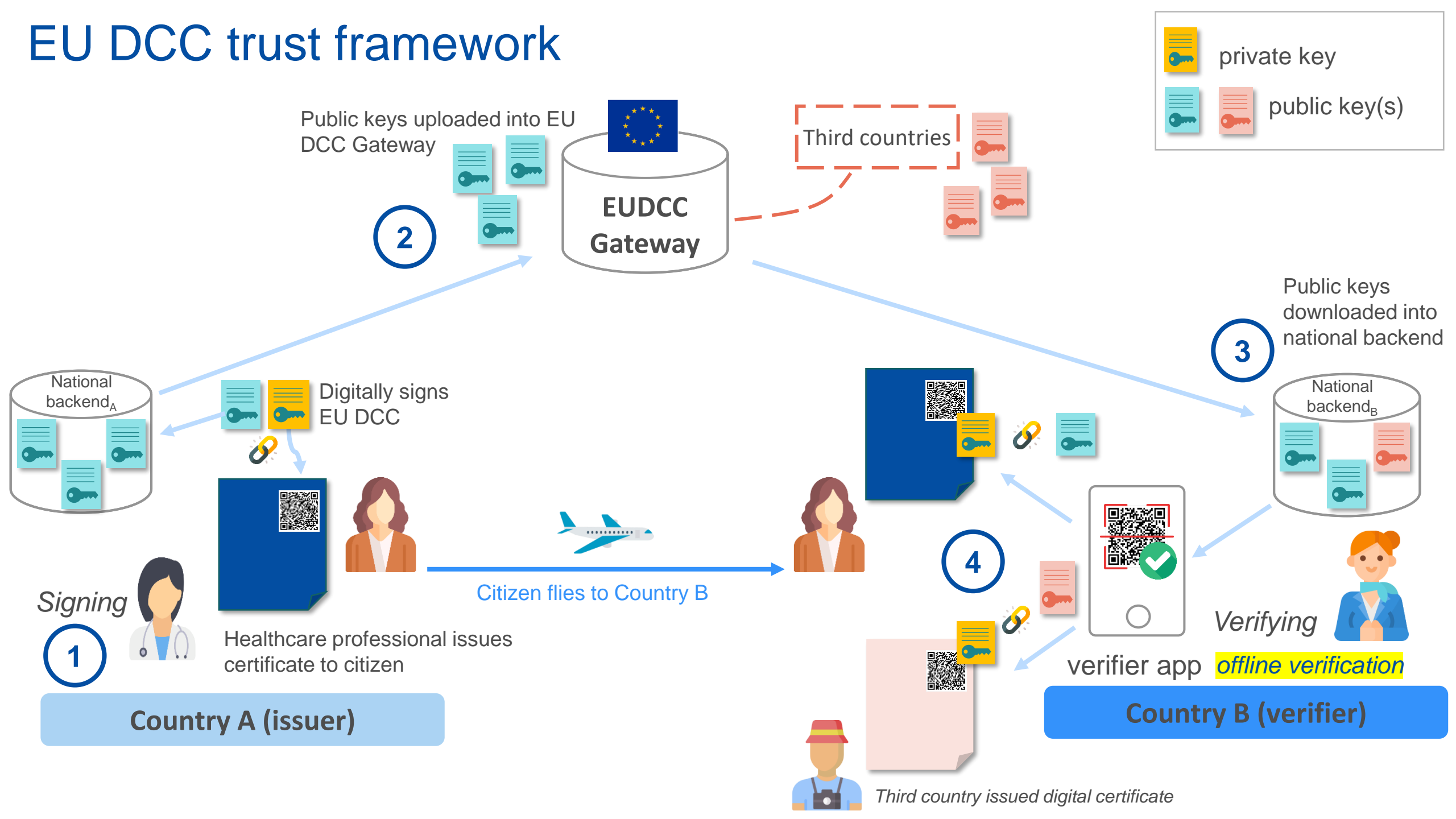
**Aim:** harmonising representation, encoding and signing

Standardised signed **CBOR** data structure which is represented in a 2D Code

Primary (**ECDSA**) and secondary (**RSA**) algorithms



# EU DCC trust framework



# Documents authentication in practice



## Certificate request

The citizen requests a document from a document issuer/public entity

## Data storage

The issuer draws the necessary information from a national (or regional/local) database



## Storage

The citizen can store the digital document & QR code in their e-wallet

## Issuance

The document issuer/public entity issues a document (digital/paper) containing a QR code



## Presentation

The citizen presents the document /certificate to a requesting entity

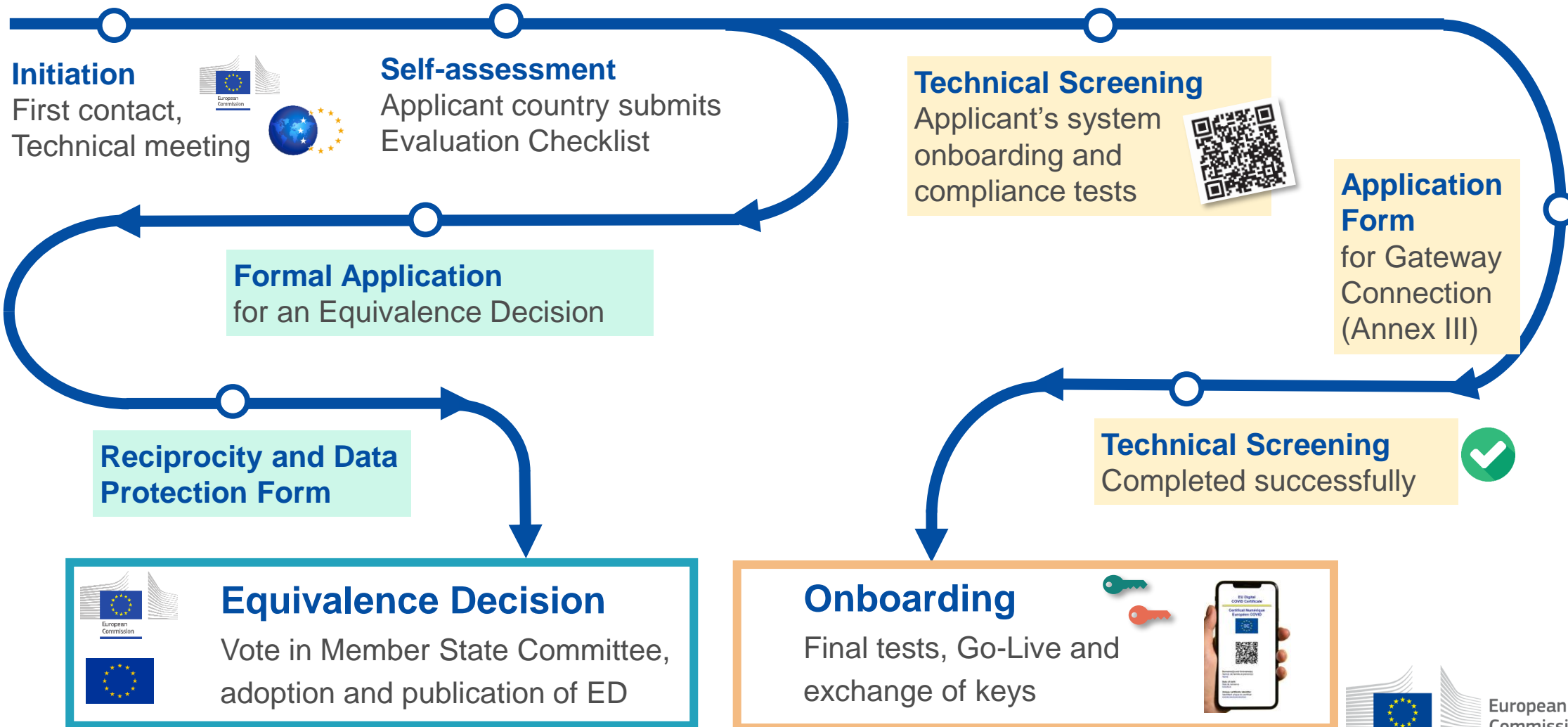


## Verification

The entity's verifier checks the authenticity, integrity and validity of the document/QR code



# The equivalence decision process





# Governance Framework – EU DCC

## EU Institutions:

- Commission
- Council
- Parliament

EU/EEA experts of  
eHealth Network



EU Health Security  
Committee

Representatives  
of third countries

European Commission  
Technical experts - TSI



# The technical onboarding process (1)

## Initial contacts and self-evaluation

1. Applicant Country submits the **Evaluation Checklist + sample QR codes**
2. Feedback of the EC + explanation of next steps - **Technical Meeting**

## Technical screening

1. **Planning Call** with SAP/T-Systems
2. Pre-requisites for onboarding: **provision of certificates** (NB-TLS (Authentication), NB-UP (upload), NB-CSCA (CSCA identification) for each screening environment)

# The technical onboarding process (2)

## DCC Environments: TST, ACC, PROD

- 1. Test environment (TST)** → used to connect a test instance of country's National Backend to a test instance of the EU DCC gateway
  - Country provides certificates (TLS, UP, CSCA) via email, receives PKI certificates (DGCG-TLS (Authentication), DGCG-TA (signature for trust list)), proceeds with **connectivity test**.
- 2. Acceptance environment (ACC)** → used for Integration Test + Quality Assurance (QR code validation)
  - Country provides and uploads certificates to circaBC, passes Integration Testing
  - Applicant Country submits Annex III – Formal Request to connect to the EUDCC Gateway

# The technical onboarding process (3)

## DCC Environments: TST, ACC, PROD

3. **Production environment (PROD)** → used for operational check-up before going live
  - Exchange of certificates (as for ACC) and whitelisting, Production Readiness Questionnaire, operational check-up with TSI = upload, download and deletion of DSCs in PROD
4. **Final onboarding confirmation:** approval for Go-Live

# DCC in numbers

**1.8bn+** people worldwide

**78**

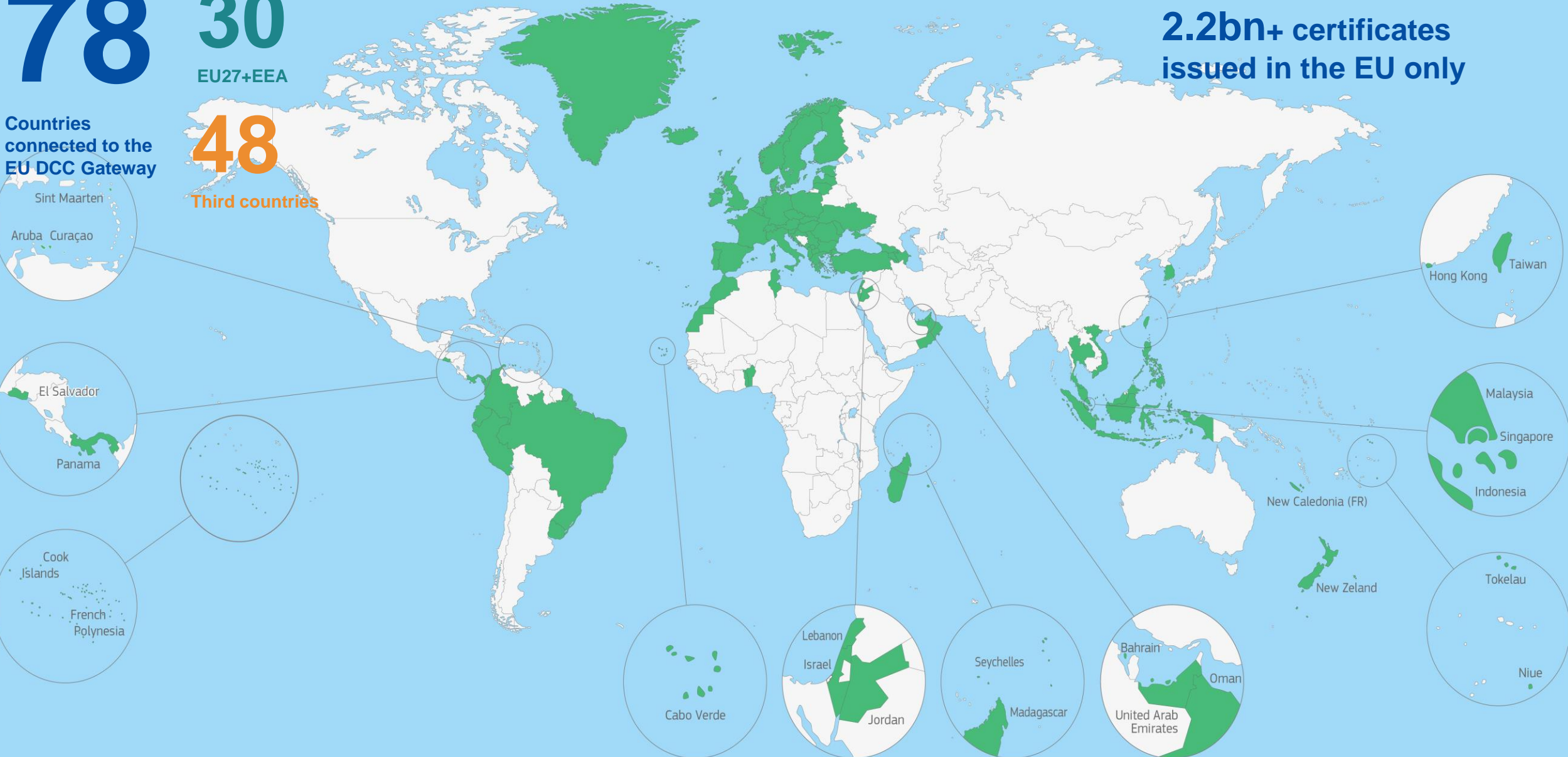
**30**  
EU27+EEA

Countries  
connected to the  
EU DCC Gateway

**48**

Third countries

**2.2bn+** certificates  
issued in the EU only



# Current status

- [Regulation \(EU\) 2021/953](#) (the EU Digital COVID Certificate regulation) expired on 30.6.2023
- On 27 June 2023, the Council of the EU adopted [Recommendation \(EU\) 2023/1339](#) on joining the global digital health certification network established by the World Health Organization and on temporary arrangements to facilitate international travel in view of the expiry of Regulation (EU) 2021/953
- The EU DCC system will stay operational until 31 December 2023, to provide continuity while its participants are onboarding the WHO Global Digital Health Certification Network.

# Questions?



© European Union 2023

Unless otherwise noted the reuse of this presentation is authorised under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license. For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.

