



***2<sup>nd</sup> meeting of the  
WP.11 IWG-dATPc***

***Working group on digital ATP  
certificates***

**2 Security marks of authenticity on the certificate such as E-signatures**

**and**

**3 Use of QR codes and options for securing a reliable link to the correct source of information to prove authenticity**

---

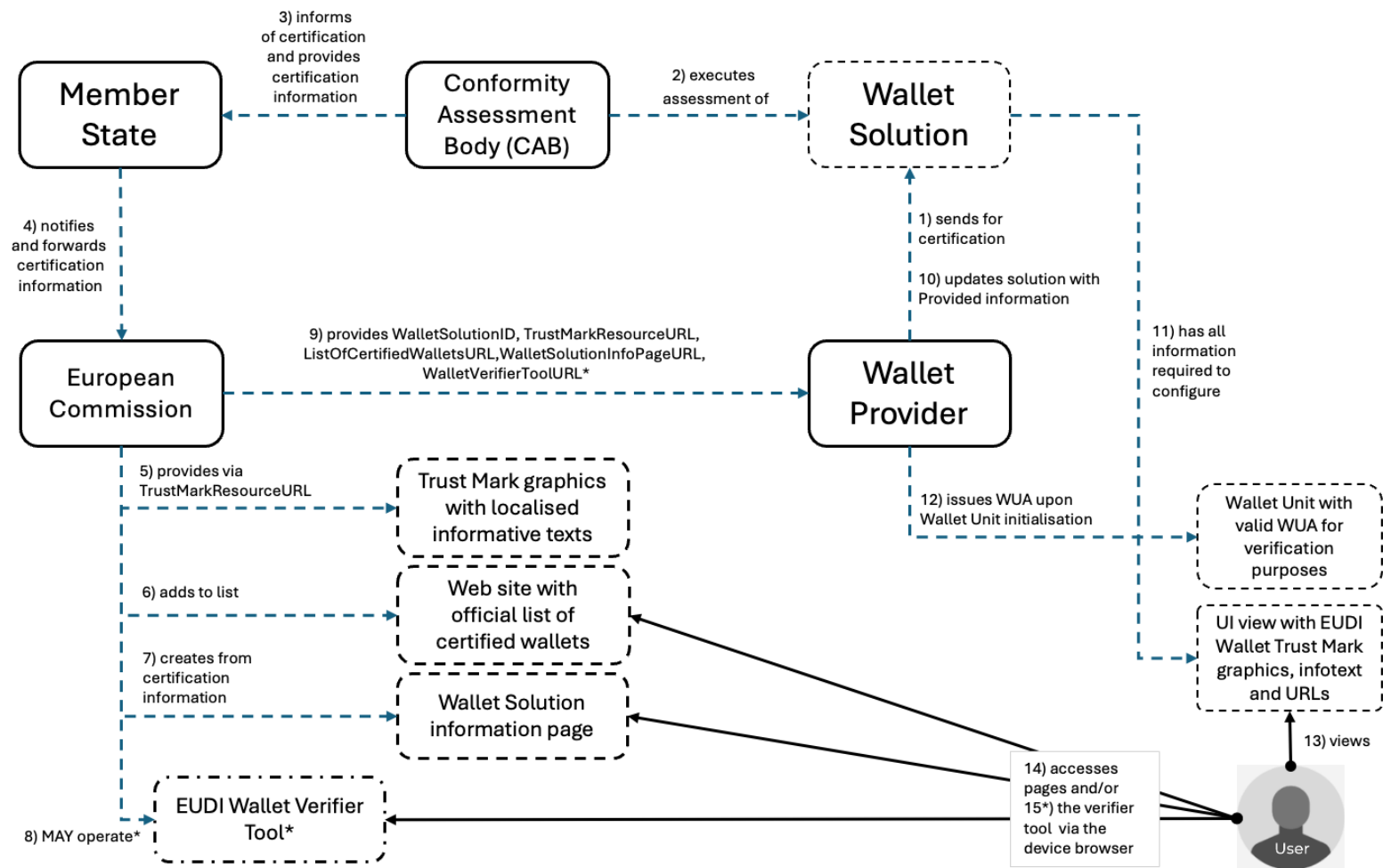
# Previous discussions in WP11

## 5. Addition to the ATP of provisions for the competent authorities of Contracting Parties to publish on their websites lists of all ATP certificates issued

*Documents:* ECE/TRANS/WP.11/2020/6 (Russian Federation)  
Informal document INF.18 (Russian Federation)

53. Some delegations expressed their support to the proposal and were of the view that a database sharing certificate information would improve checking of compliance by the police and other enforcement bodies. On the other hand, it was mentioned that considering the time and costs associated with the establishment and updating in real time, national databases regarding ATP certificates issued, the proposal should include other ways of verifying the validity and authenticity of ATP certificates, such as electronic signatures on certificates or including in the certificate a web link with a secure code, among others.

54. The Russian Federation agreed with the comments and submitted a revised proposal in informal document INF.18. The revised proposal was submitted to the vote. It was rejected with five votes in favour (France, Finland, Italy, Russian Federation and Spain) and four votes against (Czechia, Germany, Turkey and United Kingdom)



# EUDI Wallet

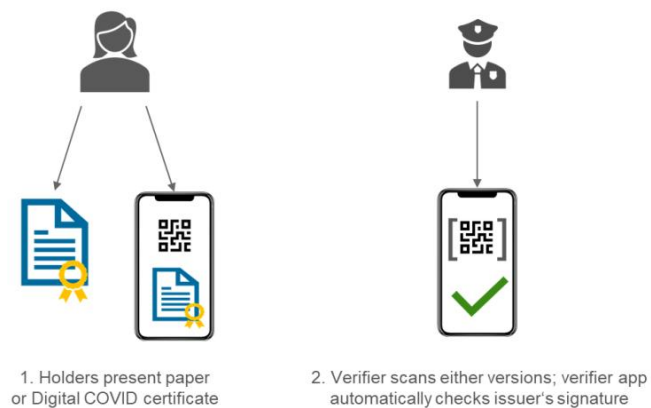


Figure 3: User story 3, offline verification

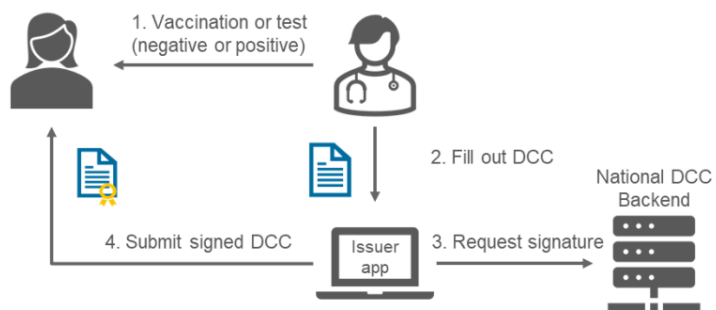


Figure 1: User story 1, issuing a DCC

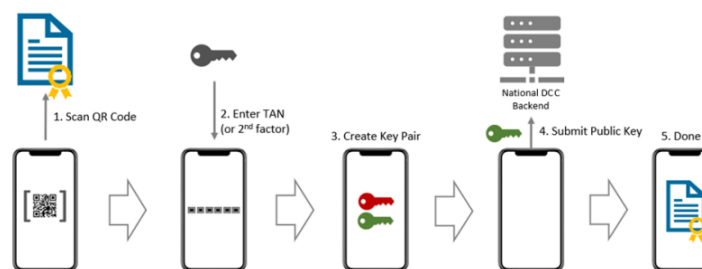
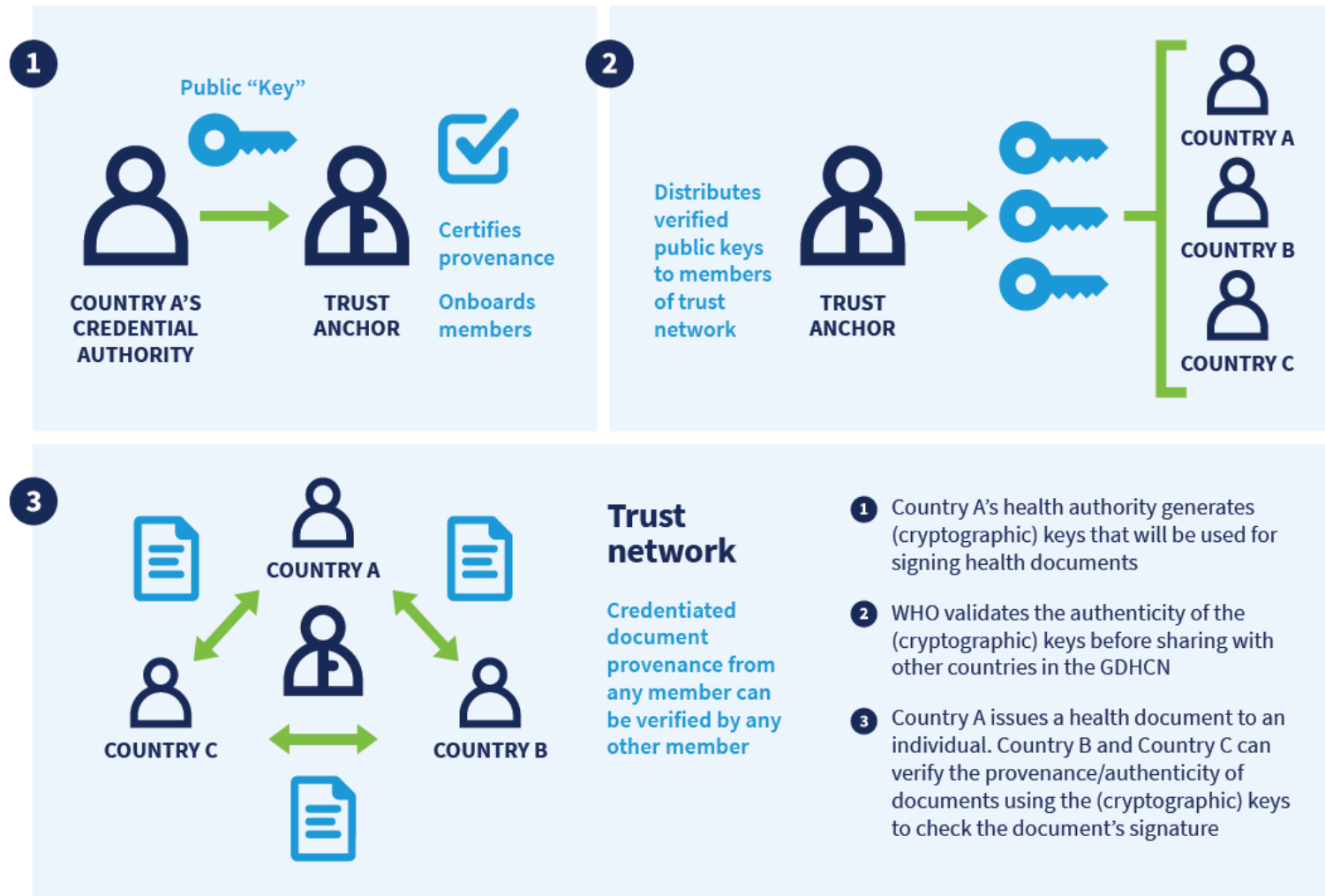


Figure 2: User story 2, transferring a Digital COVID Certificate to the wallet app

# EU Covid certificate(EUDCC)

[Guidelines\\_EU\\_COVID\\_C  
ert](#)



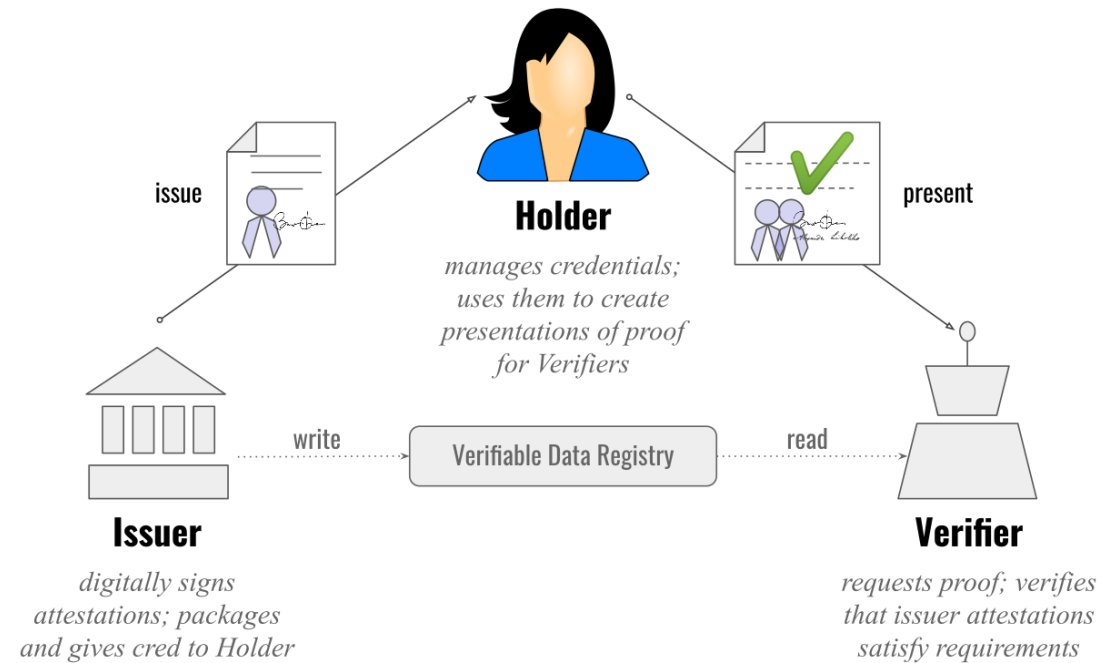


# WHO Global Digital Health Certification Network (GDHCN)

[Global Digital Health Certification Network](#)

# VERIFICATION = TRUST BASED PROCES

## Verifiable Credentials principle:



# VERIFICATION = TRUST BASED PROCES

---

- Direct Verifier System and Indirect Verifier System are verification strategies.
- DVS and IVS define how verification is performed.





# Direct Verifier System

## Direct Verifier System (DVS)

- A Direct Verifier System allows a verifier to validate a credential locally and autonomously, using cryptographic material (public keys, trust lists) that is obtained in advance.
- The verifier does not need to contact the issuer or any central system at verification time.
- *Typical Use Cases:*
  - EU Digital COVID Certificate
  - Digital calibration certificates
  - Education diplomas
  - Professional licenses
  - Product passports (DPP)
  - Cross-border verification

# Indirect Verifier System

## Indirect Verifier System (IVS)

- An Indirect Verifier System requires the verifier to perform an online check against a third-party system (issuer registry, central database, validation API) during verification.
- The verifier delegates trust and validation logic to an external authority in real time.
- *Typical Use Cases:*
  - Banking (KYC, AML checks)
  - Government registries
  - Access control systems
  - Loyalty programs
  - Subscription validation

# Direct Verifier System and Indirect Verifier System

A Direct Verifier System is optimal when:

- scalability is critical
- privacy is a priority
- cross-border or multi-stakeholder trust is required

An Indirect Verifier System is suitable when:

- real-time policy enforcement is needed
- central authority control is required
- offline operation is not necessary

Dimension	Direct Verifier System (DVS)	Indirect Verifier System (IVS)
Verification mode	Local, cryptographic (offline or near-offline)	Centralized, online
Network dependency	Not required at verification time	Mandatory
Trust model	Cryptography + trust registry	Central authority
Privacy level	Very high	Medium to low
Scalability	Very high	Limited by central infrastructure
Typical use cases	EU Digital COVID Certificate, diplomas, calibration certificates	Banking KYC, government registries, access control
Speed of policy changes	Slower – changes require: <ul style="list-style-type: none"><li>• trust list updates</li><li>• verifier rule updates</li><li>• transition periods</li></ul>	Very fast – policy changes applied centrally and effective immediately
Speed of document issuance	Fast – issuance is a local issuer process, no central confirmation required	Variable – often tied to central workflows and approvals
Ability to change already issued documents	Low – re-issuance required or validity controlled by expiry (immutability by design)	High – document or status can be changed centrally without re-issuance
Suitability for dynamic policies	Low to moderate	Very high
Suitability for long-term evidence	Very high	Moderate

# ATP CERTIFICATE VERIFICATION FLOW?



**4 Available regulations and standards for the safe checks on the issuance of digital certificates -**

**eFTI Regulation**

---



## 5 Options for the use of a digital ATP certificate of compliance in the light of paperless transport such as eCMR-

- e-CMR

