

# QRYPPTO

## QRYPPTO Digital Signature Service

Signer | Information | Status

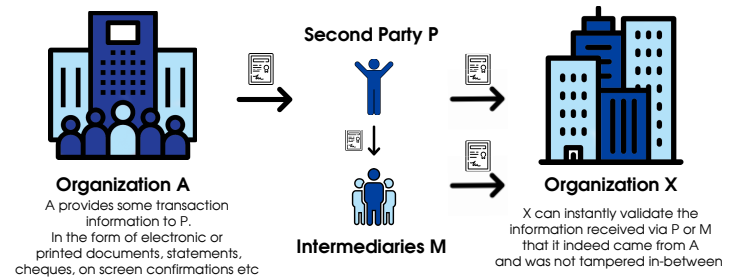
### DEFINITION

QRYPPTO technology has been enabling organizations to secure documents by incorporating a digitally signed secure code providing instant de-centralized validation by third-parties across geographies.

- 01 ▶ QRYPPTO's high-layer model
- 02 ▶ QRYPPTO – Communication flow and protection service
- 03 ▶ QRYPPTO Gateway – Architecture Overview
- 04 ▶ QRYPPTO Gateway – Interfacing with RP's QRYPPTO system
- 05 ▶ QRYPPTO Gateway – Distributing digital signature and authentication information
- 06 ▶ QRYPPTO Gateway – Credential Distribution
- 07 ▶ QRYPPTO App – Issue QRYPPTO code
- 08 ▶ QRYPPTO App – Transfer QRYPPTO code to Wallet app
- 09 ▶ QRYPPTO App – Offline Authentication
- 10 ▶ QRYPPTO application – Architectural model of RP's QRYPPTO system

### THE PROBLEM QRYPPTO SOLVE?

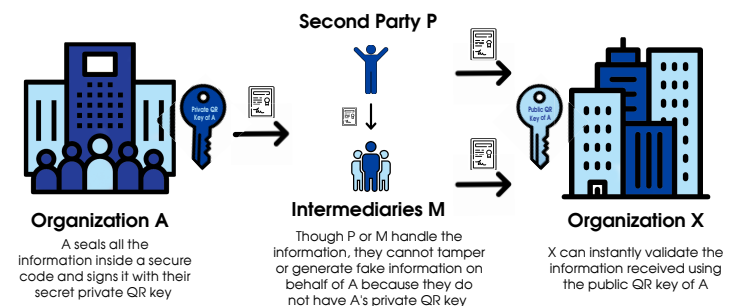
Enable secure sharing of information between institutions via untrusted mediums without the need for system to system integration.





-  Less expensive to build & maintain
-  Better data security
-  Better privacy

### HOW QRYPPTO?

Organizations just need to share their public key to enable third parties to secure all codes QRYPPTO signed by their private key.



-  Based on public key infrastructure
-  Easily scalable by simply sharing public keys

## WHY?

Enabling de-centralized validation and access to structured data by any third-party processing documents reduces fraud, improves efficiency and increases trust.

- ✓ Automated Public Key distribution.
- ✓ Automated processing with validated data.

## HOW TO VERIFY AND INSTALL OPTIONS

### IMPLEMENTATION OPTIONS



Verified by only authorized apps or any QR Reader

Authorized Apps only because:

- Security: prevents QR phishing
- Privacy: avoids leaking of patient information



Offline (PDC Codes) and Online (EDC Codes)

Offline (PDC):

- Offline Validation: needed for air-gapped environments



Cloud and On-premise

Offline (PDC):

- Offline Validation: needed for air-gapped environments

### TYPES OF QCRYPTO CODES

1

Primary Data Codes (PDC)

Capable of Storage, Offline validation

2

Extended Data Codes (EDC)

Online authentication

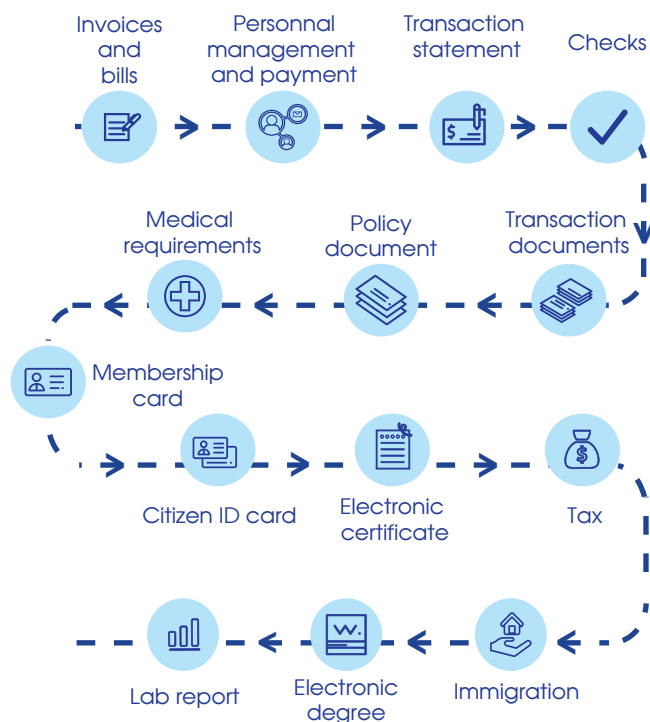
3

Hybrid Data Codes (HDC)

Provides features of both PDC and EDC by including two elements:

On-Code Secure Enclave like PDC and On-line attachments like EDC.

### IMPLEMENTATION APPLICATION



## TRUST MODEL OPTIONS

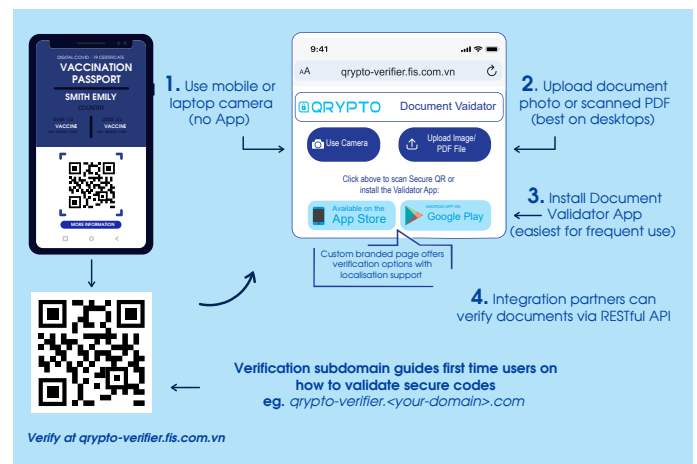
### DOMAIN BASED

- Public Key delivered via verification domain name (qcrypto-verifier.fis.com.vn) managed by QCRYPTO Gateway.
- Faster implementation.
- All types (PDC, EDC, HDC) supported.

### CA BASED

- Generate CSR (Certificate Signing Request) on QCRYPTO.
- Get DSC (Digital Signing Certificate) from QCRYPTO.
- Upload DSC on QCRYPTO.
- Distribute DSC yourself.

## FOUR EASY WAYS OF VERIFICATION



## WHY QCRYPTO?

### SECURITY QR TECHNOLOGY FOR SENSITIVE INFORMATION

- Security & compression: Support for HSM (Hardware Security Modules), Key rotation.
- Standards based: Other countries will find it easy to validate codes generated by you and you will be able to validate their codes.
- No central database:
  - Greater scalability: generate millions of codes with modest infrastructure.
  - Reduces cyber attack surface area.
- De-centralised public key based validation.
- Deployment options: On-premise, AWS, Azure or your preferred infrastructure.

### ENTERPRISE READY

- In production use since 2022 in many markets and use cases.
- Product has gone through evaluations and security audits by demanding customers.
- Backed by comprehensive services to help ensure project success.
- Core technology wrapped in an easy to integrate solution with associated components.