QR code scanner V6

```
graph TD
    %% QR Code Generation
    A[QR Code Generation System] --> B[Store QR Code + Metadata<br>in Vendor Database]
    B --> C[Embed Vendor Validation URL in QR Code]
    C --> D[Cryptographic Signature Engine<br>RSA/ECC Signing]
    D --> E[Physical QR Code<br>Content + Signature + Validation URL]

    %% QR Code Scanning & Validation (Physical)
    E -->|QR Scan| F[Physical QR Scanner/App]
    F --> G[Cryptographic Signature Validation]
    G --> H[Fetch QR Record from Vendor Endpoint]
    H --> I[Check Validation URL Against Threat Intelligence DB]

    %% Validation Outcome
    I --> J{All Validations Passed?}
    J -->|Yes| K[Display Trust Indicator ✅ in Scanner]
    J -->|No| L[Display Warning Indicator ❌ in Scanner]

    %% Node Styling
    style A fill:#BBDEFB,stroke:#0D47A1,stroke-width:2px
    style B fill:#FFF3E0,stroke:#FB8C00,stroke-width:2px
    style C fill:#E3F2FD,stroke:#2196F3,stroke-width:2px
    style D fill:#D1C4E9,stroke:#5E35B1,stroke-width:2px
    style E fill:#DCEDC8,stroke:#689F38,stroke-width:2px
    style F fill:#FFF9C4,stroke:#FBC02D,stroke-width:1px
    style G fill:#E1F5FE,stroke:#03A9F4,stroke-width:1px
    style H fill:#F1F8E9,stroke:#8BC34A,stroke-width:1px
    style I fill:#FFECB3,stroke:#FFC107,stroke-width:1px
    style J fill:#FFE0B2,stroke:#FB8C00,stroke-width:1px
    style K fill:#C5E1A5,stroke:#7CB342,stroke-width:1px
    style L fill:#FFCDD2,stroke:#E53935,stroke-width:1px
```

```
graph TD
    %% QR Code Generation
    A[QR Code Generation System] --> B[Store QR Code + Metadata<br>in Vendor Database]
    B --> C[Embed Vendor Validation URL in QR Code]
    C --> D[Cryptographic Signature Engine<br>RSA/ECC Signing]
    D --> E[Digital QR Code<br>Content + Signature + Validation URL]
```

```
    %% Digital QR Scanning & Validation
    E -->|QR Exchange Protocol| F[Digital QR Scanner/App]
    F --> G[Cryptographic Signature Validation]
    G --> H[Fetch QR Record from Vendor Endpoint]
    H --> I[Check Validation URL Against Threat Intelligence DB]

    %% Validation Outcome
    I --> J{All Validations Passed?}
    J -->|Yes| K[Display Trust Indicator ✅ in Scanner]
    J -->|No| L[Display Warning Indicator ❌ in Scanner]

    %% Updating Digital QR based on Validation
    K -->|QR Exchange Protocol| M[Update Digital QR Code Display]
    L -->|QR Exchange Protocol| M
    M --> N[Show Trust Indicator at center of Digital QR ✅ / ❌]
    M --> O[Show Last Verification Timestamp<br>in whitespace around Digital QR]

    %% Node Styling
    style A fill:#BBDEFB,stroke:#0D47A1,stroke-width:2px
    style B fill:#FFF3E0,stroke:#FB8C00,stroke-width:2px
    style C fill:#E3F2FD,stroke:#2196F3,stroke-width:2px
    style D fill:#D1C4E9,stroke:#5E35B1,stroke-width:2px
    style E fill:#DCEDC8,stroke:#689F38,stroke-width:2px
    style F fill:#FFF9C4,stroke:#FBC02D,stroke-width:1px
    style G fill:#E1F5FE,stroke:#03A9F4,stroke-width:1px
    style H fill:#F1F8E9,stroke:#8BC34A,stroke-width:1px
    style I fill:#FFECB3,stroke:#FFC107,stroke-width:1px
    style J fill:#FFE0B2,stroke:#FB8C00,stroke-width:1px
    style K fill:#C5E1A5,stroke:#7CB342,stroke-width:1px
    style L fill:#FFCDD2,stroke:#E53935,stroke-width:1px
    style M fill:#B2DFDB,stroke:#00796B,stroke-width:1px
    style N fill:#DCEDC8,stroke:#689F38,stroke-width:1px
    style O fill:#FFF59D,stroke:#FDD835,stroke-width:1px


sequenceDiagram
    participant QG as QR Generator System
    participant VD as Vendor DB
    participant CSG as Cryptographic Signature Generator
    participant QS as QR Scanner/App
    participant CSV as Cryptographic Signature Validator
    participant VE as Vendor Endpoint
    participant TDB as Threat Intelligence DB
```

```
%% QR Code Generation Process
rect rgb(232,245,233)
QG->>VD: Store QR Metadata (Payload + Timestamp)
VD-->>QG: Return Vendor Validation URL
QG->>QG: Embed Validation URL into Payload
QG->>CSG: Request Signature (Payload + URL + Timestamp)
CSG->>CSG: Compute Hash and Sign using Private Key
CSG-->>QG: Return Digital Signature
QG->>QG: Embed Signature into QR Code
end

%% QR Scan and Signature Validation
rect rgb(227,242,253)
QS->>CSV: Validate Signature (Payload + URL + Timestamp + Signature)
CSV->>CSV: Compute & Verify Signature using Public Key
alt Signature Valid
    CSV-->>QS: Signature Verified ✅
else Invalid Signature
    CSV-->>QS: Signature Invalid ❌
end
end

%% Compare Payload and Threat Validation
rect rgb(255,249,196)
QS->>VE: Fetch Original Payload using Vendor Validation URL
VE-->>QS: Return Original Payload
QS->>QS: Compare Scanned Payload with Vendor Payload
alt Payloads Match
    QS->>TDB: Check URL in Payload Against Threat Intelligence DB
    TDB-->>QS: Return Threat Analysis Result
    alt URL Safe
        QS-->>QS: Display Trust Indicator ✅
    else URL Malicious or Suspicious
        QS-->>QS: Display Warning ❌
    end
else Payload Mismatch
    QS-->>QS: Display Tampering Alert ❌
end
end
```

A. Secure Digital Signature Embedded QR Codes (with Vendor Verification)

Concept:

Embed a digital signature within the QR code payload using asymmetric cryptography (e.g., RSA or ECC), along with a vendor-hosted validation URL. This ensures the authenticity and integrity of the QR contents and allows verification via a trusted vendor endpoint.

How it works:

- **QR Payload Structure:**
  [Content/URL] + [Timestamp] + [Vendor Validation URL] + [Digital Signature (Signed with Private Key)]
- **QR Code Generation Process:**
  1. QR Generator stores the payload and timestamp in the **Vendor Database**.
  2. The **Vendor Validation URL** returned is embedded into the payload.
  3. The final payload (including the URL) is hashed (SHA-256).
  4. The hash is signed using a **Cryptographic Signature Generator** with a private key (RSA/ECC).
  5. The signed QR code is generated with the payload and the digital signature.
- **Validation Process (at scanning):**
  1. QR Scanner extracts the payload, URL, timestamp, and digital signature.
  2. Signature is validated using the **Cryptographic Signature Validator** and public key.
  3. If valid, the scanner calls the **Vendor Endpoint** (URL) to retrieve the original stored payload.
  4. The scanner compares the **scanned payload** to the **vendor-supplied payload**.
  5. If matching, the **URL is checked against a Threat Intelligence DB** to assess safety.

Scanning Compatibility:

- **Standard QR scanners** read only the embedded content/URL.
- **Secure scanner apps** validate the signature and payload using vendor records and threat analysis.

B. Visible Trust Indicator (No AI Visual Watermark)

Updated Concept:

Instead of AI-generated visual watermarks, the system uses cryptographic validation + vendor verification + threat analysis to generate a **visible trust indicator** within the digital QR code UI (not in the QR pixels).

Implementation Details:

- **Visual Trust Feedback Loop:**
  - After scanning, and successful:
    - Signature validation

        - Payload integrity check with vendor
        - Threat analysis (URL safe)
    - A ✅ (Trust Indicator) is visually shown in the **center** of the digital QR code.
    - **Timestamp** of the last successful validation is displayed around the QR code whitespace.
- If any step fails (invalid signature, mismatched payload, or malicious URL):
    - A ❌ (Warning Indicator) is shown in the center.
    - The failed validation attempt is **timestamped** and shown as well.

User Benefits:

- Immediate visual feedback for **trustworthiness** without reading payload.
- Cryptographically secured without relying on complex AI watermark models.

C. Threat Validation via Vendor + Threat Intelligence DB

Concept:

A deterministic validation flow replaces AI-based heuristics, using trusted vendor payload records and well-maintained threat intelligence databases.

Implementation Flow (During Scanning):

1. **Signature Validation** – Confirms the integrity of the QR using public key.
2. **Vendor Validation** – QR scanner uses the embedded **Vendor URL** to retrieve the original signed payload.
3. **Payload Comparison** – Confirms that the scanned and stored payloads match (ensuring no tampering).
4. **Threat DB Check** – The URL in the payload is checked against phishing/malware blacklists or reputation services.

Outcome:

- If all validations pass:
  ✅ Trust Indicator + Timestamp is embedded in the display.
- If any validation fails:
  ❌ Warning with failure reason + timestamp is shown clearly.

Novelty (Revised)

1. **Combined Cryptographic Signature and Vendor-Backed Payload Validation**
    - Leverages **asymmetric cryptography (RSA/ECC)** to embed digital signatures within QR code payloads, ensuring authenticity and integrity.
    - Uniquely combines **signature validation with vendor-hosted payload retrieval**, allowing tamper-proof verification through trusted

endpoints.

2. **Vendor-Side QR Payload Integrity Verification**
    - Introduces a novel mechanism where the **scanned QR payload is cross-validated** against the **original payload retrieved via embedded vendor URL**.
    - This ensures that no intermediate tampering occurs between generation and scanning, elevating trust in static and dynamic QR use cases.
3. **Threat Intelligence-Integrated URL Validation**
    - Instead of relying on AI heuristics, the system performs **deterministic threat validation** by checking embedded URLs against:
        - **Phishing databases**
        - **Malicious domain blacklists**
        - **Enterprise-grade threat intelligence sources**
    - Ensures high-confidence, explainable outcomes in real-time.
4. **Dynamic Trust Indicators in Digital QR Code Interfaces**
    - Upon scanning and successful multi-step validation, the system updates the **digital QR UI** to show:
        - A **trust indicator** (✅ or ❌) in the center
        - A **timestamp** of the last validation around the QR code
    - Provides **visible, verifiable assurance** to end-users, enhancing QR code security UX without altering the QR image itself.

QR Exchange Protocol (Revised)

Definition:

The **QR Exchange Protocol** is a secure communication mechanism enabling QR scanners to validate and optionally update digital QR code displays. It ensures real-time cryptographic validation, vendor-backed payload integrity checks, and URL threat analysis—delivering visual trust feedback to users.

It adapts based on QR type:

- **Unidirectional (Physical QR):**
  Scanner validates QR code content without modifying the code itself.
- **Bidirectional (Digital QR):**
  Scanner validates the QR, compares with vendor data, performs threat checks, and **visually updates the QR display** with a trust status and timestamp.

📩 Protocol Message Structure

✅ Request Message (Scanner → Backend)

Field	Description	Example

QR_Payload	Embedded content in QR code	https://vendor.com/validate?id=123
Timestamp	Timestamp of QR generation	2025-03-17T14:00Z
Signature	RSA/ECC digital signature (base64 encoded)	Base64String...
Scanner ID	*(Optional)* Identifier for scanner device/app	ScannerApp_v2.1

✅ **Vendor & Threat Validation Message (Scanner → Vendor Endpoint)**

Field	Description	Example
Validation URL	Vendor endpoint embedded in QR payload	https://vendor.com/qr/validate/123

✅ **Response Message (Backend/Vendor → Scanner)**

Field	Description	Example
Signature Status	Result of cryptographic signature verification	Valid / Invalid
Payload Match	Comparison result between scanned and vendor payload	Match / Mismatch
Threat Status	URL threat check (blacklist, phishing DBs, etc.)	Safe / Unsafe: Blacklisted
Overall Status	Final trust status after all checks	Trusted ✅ / Untrusted ❌
Verification Time	Timestamp when validation occurred	2025-03-17T15:42:30Z
Recommended Action	Suggested next step if validation fails	Block, Warn, Proceed with caution

🖥️ Dynamic Digital QR Update (Scanner → Digital QR Display)

(Applicable only for digital QR scenarios with display UI)

Field	Description	Example
Validation Status	Trust indicator shown at QR center	✅ / ❌

Verification Time	Timestamp displayed around QR whitespace	2025-03-17T15:42 UTC

🖥️ Usage: Physical vs. Digital QR

QR Type	Communication Flow	Direction	Dynamic Visual Update
Physical QR	Signature + Vendor + Threat validation	Uni-directional	❌ No update
Digital QR	Full validation + UI update	Bi-directional	✅ Trust symbol & timestamp

- **Physical QR:**
  Scanner validates silently; QR code content is not modified post-scan.
- **Digital QR:**
  Trust validation results are visually reflected on the **QR UI**, including:
  - ✅ / ❌ at the center
  - Timestamp in surrounding area