NotaryLive STATE VITAL RECORDS

Scalable Security for Digital Vital Records Issuance

Joshua Stankard
CEO
NotaryLive

Why Digital Issuance Now

Rising demand for fast digital services

- Paper workflows slowing operations
- Fraud pressure and higher convenience expectations

Core Security Challenge

- High sensitivity identity data at volume
  - Balancing convenience, compliance, trust

NotaryLive STATE VITAL RECORDS

Layered Security Overview

Defense-in-depth across systems, data, user access

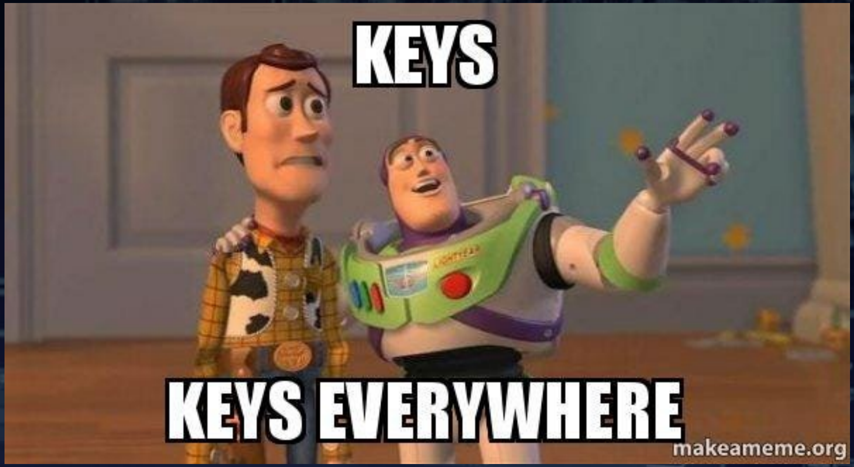
Secure Document Design

Anti tamper controls

- Cryptographic signatures
- Online verification portals

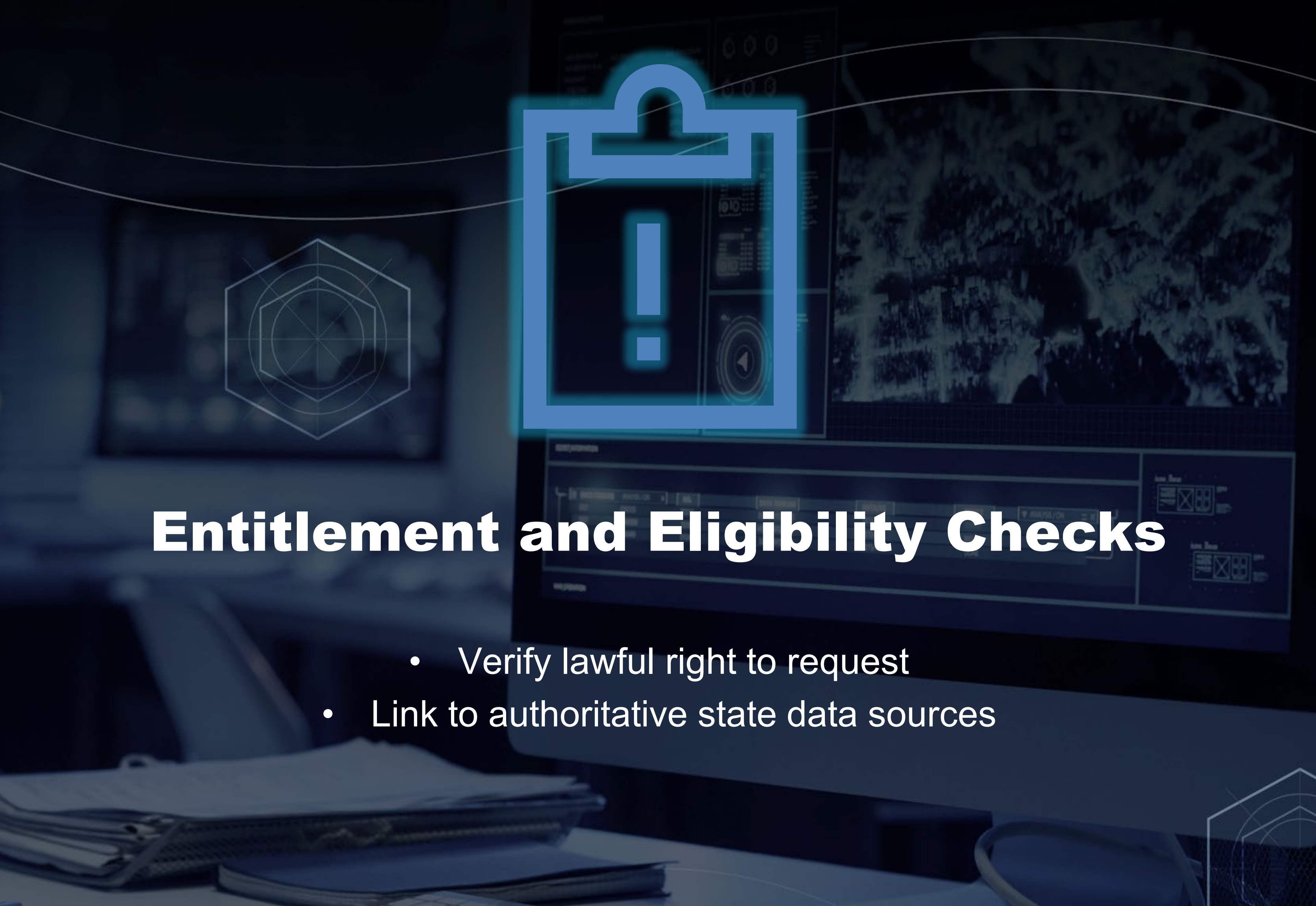
Cryptographic Protections

- Encryption at rest and in transit
  - Strong key management
  - Integrity validation



Identity Proofing

- Risk based workflows
  - Remote and in person options
  - Reuse trusted credentials



Entitlement and Eligibility Checks

- Verify lawful right to request
- Link to authoritative state data sources

Access Control and Role Management

- Least privilege access
  - Segregation of duties
  - Monitor privileged actions

Auditability and Logging

- Full traceability for each issuance
  - Anomaly detection
  - Support investigations

Vendor Risk Management

- Defined security requirements
  - Strict data handling standards
  - Continuous vendor monitoring

Scalability Considerations

- High volume architecture patterns
  - API driven issuance
  - Resilience and redundancy

Future of Digital Vital Records

Smart documents

- Digital wallets and vaults
- Interoperable verification

Balancing Public Trust

- Transparency
  - Compliance alignment
  - Privacy by design

CLOSING & QUESTIONS

Key takeaways

Discussion prompts