iProov

Enhance Border Control with AI-resistant NFC-reading of fingerprints

EU Justice and Home Affairs in the Age of AI: *Fostering Innovations and Mitigating Risks*
Nov 12-13th 2024, Budapest, Hungary

Setting the scene

01

Remote capturing Challenges

AI-Powered Threats, Exponential rise in deep face technology (face and fingers), Sophisticated presentation attacks, Synthetic identity creation, AI-generated document forgeries

02

Operational Pressures

EES implementation, Growing passenger volumes requiring efficient processing, Resource constraints at border control points, Non-inclusive digital solution, Push for enhanced security without compromising throughput.

03

Regulatory Requirements

Entry/Exit System (EES) compliance mandates, EU AI Act requirements for biometric systems, Data protection and privacy regulations (GDPR), eIDAS 2.0 LoA:High requirements, Cross-border interoperability standards

iProov Development Goals

Seek EU member state partnership for advancement in AI-resistant backend-driven NFC-reading technology built on projects such as Eurostar and Frontex.

Success Stories in Remote Verification

Eurostar, iProov implementation:

- **Challenge:** Securely verify passenger identities pre-travel, manage high volumes, and meet Brexit and international travel requirements.
- **Results:** Customer survey conducted 2024: 62 % of travellers rate the experience Excellent (5/5). Another 20 % as Great (4/5).
  - Why? Make smoother/easier check in-process 74 %, Avoid queues 68 %.
  - Main fear: getting it wrong and not being allowed to travel.

Frontex App for EES - iProov implementation

- **Focus**: Large-scale application of biometrics in border checks, both research and technical focuses.
- **Challanges:**
  - Legal and Ethical Considerations
  - Operational Challenges
  - Technical Complexity:
- **Evolving AI-Threats:** such as sophisticated spoofing techniques and deep fakes are considered severe challenges. Addressing these involves close collaboration between Frontex, technology providers, EU member states, and other stakeholders.

Challenge of Remote Fingerprinting

Current Challenges:

- EES implementation require fingerprints at border processes.
- Supervised manual verification is resource-intensive.
- Remote fingerprint captures are subject to severe AI-powered frauds.

-> Need for efficient, Easy to use, AI-resistant, remote verification securely binding the fingerprint to the identity (and the face)

Critical Requirements of Remote Fingerprinting

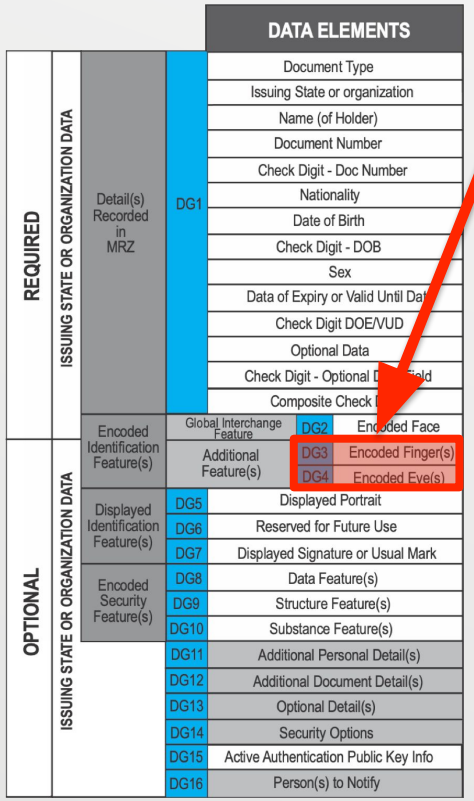
Requirements

- Highest security measurements
- Need for AI-resistant biometric solutions
- Remote fingerprint capture capabilities, e.g. terminal access
- Secure binding of biometric data
- Inclusive to all age groups, background etc.

Key Considerations

- Enable efficient pre-travel verification
- Ensuring regulatory compliance
- Maintaining privacy protection
- Supporting scalable implementation

Policy Challenges to Reading Fingerprints

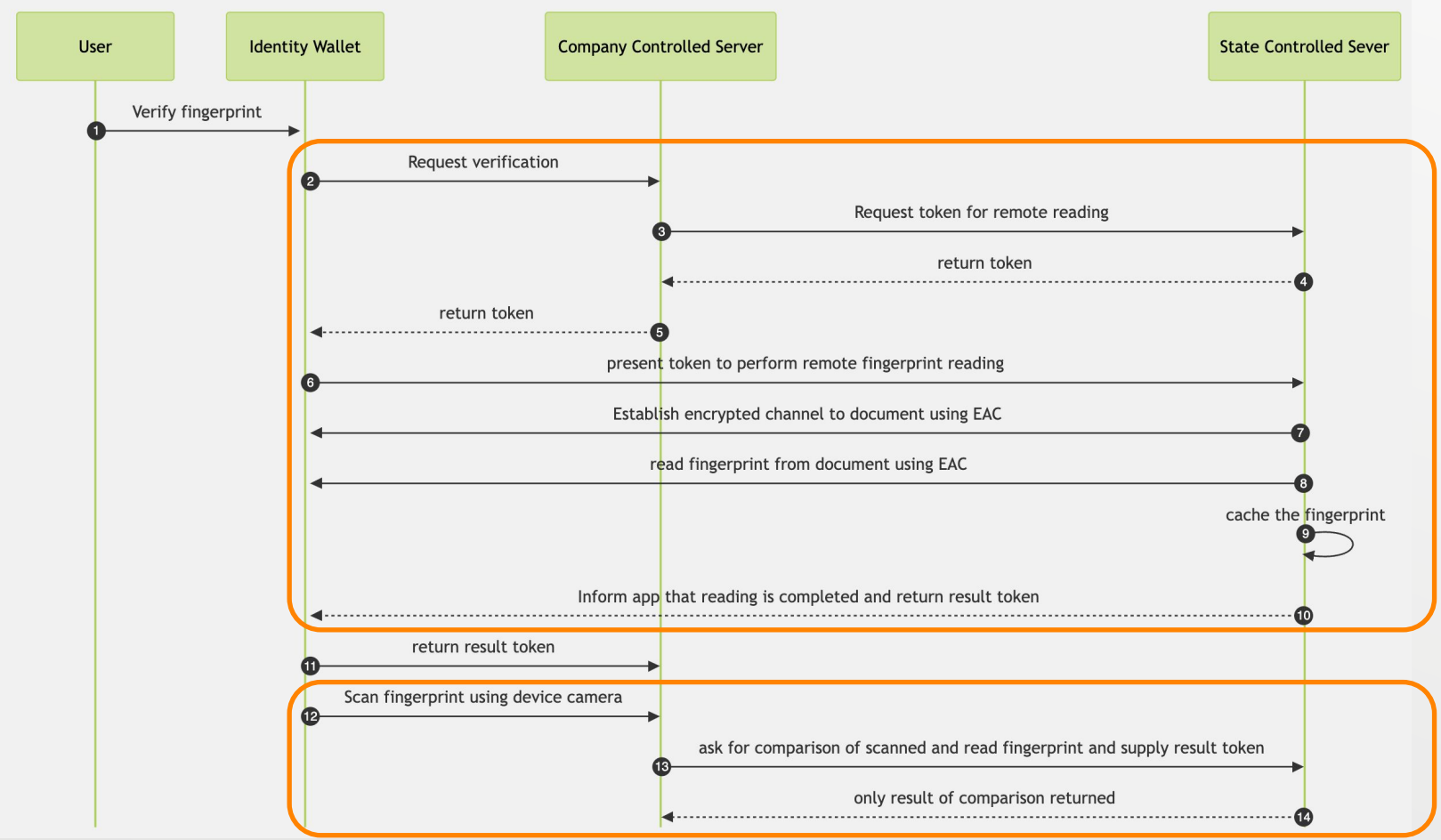


- Fingerprint information in passports are stored in Datagroup 3
- Reading is protected by Extended Access Control (EAC)
- EAC is optional and can only be used by EU member states to read biometric data (fingerprint or iris)

➡ Fingerprints in passports can only be read by EU member states

➡ The service that reads fingerprints needs to be operated and controlled by a Member state and not a private company

How to resolve this? Backend driven NFC!



Reading is done by a Member state through an encrypted channel directly to the document using EAC

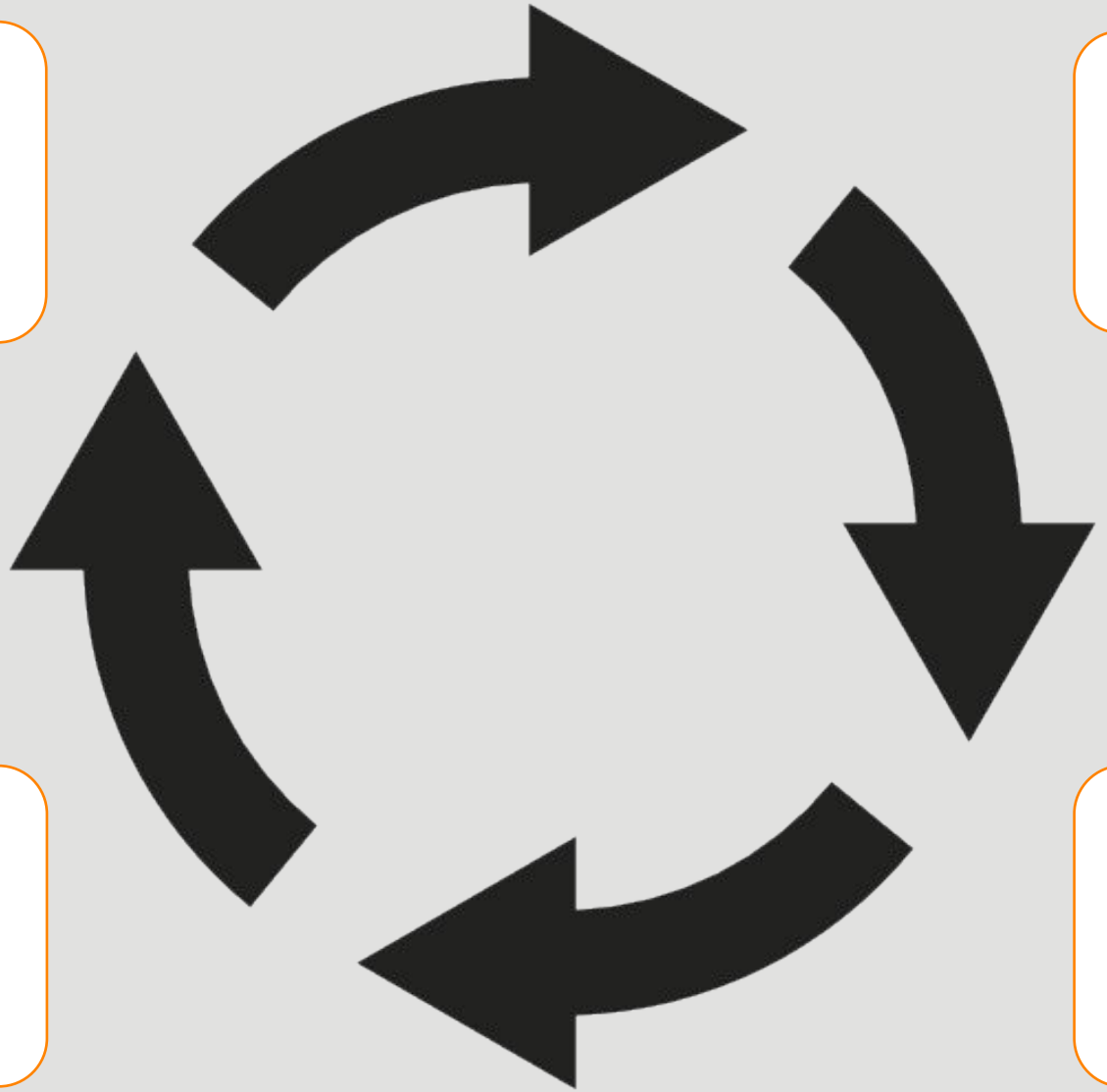
The evaluation of the scanned fingerprint is done by the Member state

Four-way Identity Wallet Binding

iProov

Device & App

Identity data



Finger Print

User Liveness

Backend driven NFC-reading

Secure Biometric Access	Backend NFC enables remote ePassport data access without widespread terminal distribution
Privacy-Preserving Matching	Secure fingerprint matching on government backend, returning only match results
Dual Access NFC	iProov manages credentials - fingerprint reading /validation; EU member states handles authentication & fingerprint matching

Backend-driven NFC enables AI-resistant biometric verification and face binding with fingerprint, enabling pre-journey enrolment for EU border (EES) control without exposing sensitive ePassport data

Development project

Development Goals

1. MRR technology enhancement to MRL 5/6
2. Integration capabilities expansion
3. Security feature advancement
4. Complete end-2-end solution

Policy Considerations

1. Supervised Onboarding
2. Controlled environment
3. Secure verification process
4. Regulatory compliance
5. Privacy protection

Comprehensive Capabilities

1. Face matching
2. Liveness detection
3. Fingerprint capture
4. NFC scanning
5. Physical Access hardware
6. Identity wallet solutions

Risk Mitigation

1. False rejection handling
2. Anti-spoofing measures
3. Data protection protocols
4. Compliance framework

Conclusions - Enhancing Border Control with Backend driven NFC-reading

1. EU AI Act compliance (Low Risk 1:1)
2. Privacy-preserving architecture
3. Proven implementation success
4. Comprehensive security measures

iProov

Thank You

Real Person Right Person Right Now