University Library of Southern Denmark

Computer Engineering

Douglas Pablo Bracale Celestino

Digital Ticket Validation, Security Analysis

Odense - Denmark

January, 2026

1. Executive Summary

This report presents an academic security analysis of **digital ticket validation systems** used in **proof-of-payment public transport models**, with a focus on scenarios where ticket validity is determined primarily through **visual inspection**.

The analysis identifies that when no **machine-verifiable authenticity mechanism** is present, visually replicated tickets may become indistinguishable from legitimate ones. This introduces risks related to **replication**, **replay**, and **scalability of misuse**, especially if such techniques become widely known.

The report proposes **practical, low-friction security improvements**, prioritizing solutions that preserve the usability and operational efficiency of proof-of-payment systems, such as **cryptographically signed QR codes with offline verification**.

---

2. System Context

2.1 Proof-of-Payment Model

In proof-of-payment transport systems, passengers purchase a ticket prior to boarding and may be checked by inspectors at random intervals. Unlike gated systems, there is no mandatory validation at entry points. Compliance is enforced through trust and periodic inspection.

This model offers several advantages:

- Reduced infrastructure cost
- Faster passenger flow
- Improved user experience

However, it also places strong reliance on the **robustness of ticket validation mechanisms**.

2.2 Assumed Validation Method

This analysis focuses on systems where ticket validity is verified primarily through **visual inspection** on a passenger’s mobile device. In such scenarios, inspectors assess elements such as:

- Visual layout
- Displayed timestamps
- Status indicators (e.g., “valid” or “expired”)

No automated or cryptographic verification is assumed in this context.

---

3. Scope and Methodology

3.1 Scope

The scope of this study includes:

- Visual-only digital ticket validation mechanisms
- High-level threat modeling
- UI-based proof-of-concept demonstration
- Risk and impact analysis
- Security-by-design recommendations

3.2 Out of Scope

The following are explicitly out of scope:

- Backend systems and databases
- Real-world exploitation
- Automated bypass techniques
- Publication of sensitive or operational details

3.3 Methodology

The analysis was conducted using:

- Threat modeling (attacker, assets, attack surface)
- Qualitative risk assessment (likelihood × impact)
- Review of industry best practices in secure ticketing systems

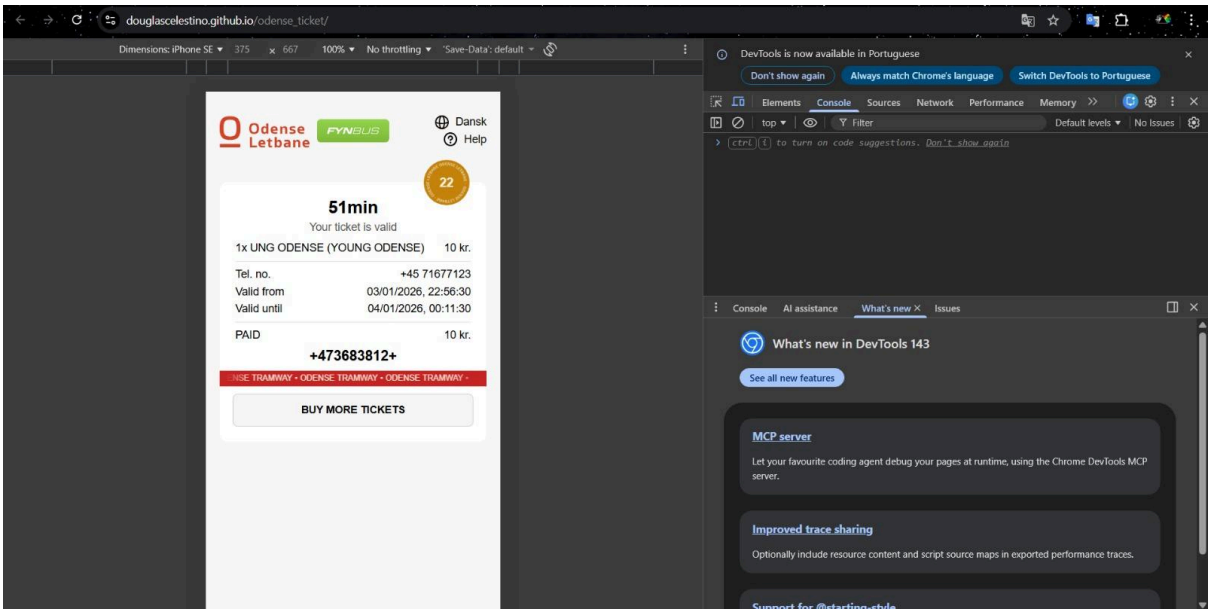

Figure 1 - Visual proof-of-concept of a digital ticket UI used exclusively for academic demonstration purposes

---

4. Threat Model

4.1 Attacker Profile

The assumed attacker is a motivated user with **basic web development knowledge** (HTML, CSS, JavaScript), capable of reproducing user interfaces and presenting them on a mobile device.

4.2 Assets to Protect

Key assets include:

- Fare revenue integrity
- Trust in the ticketing system

- Operational efficiency of inspection processes

4.3 Attack Surface

The primary attack surface identified is the **presentation layer of the ticket UI**, particularly in scenarios where no machine-verifiable proof of authenticity exists.

---

5. Key Findings

Finding 1 — Visual-only validation enables replication risk

When ticket authenticity is determined solely by appearance, it becomes possible to reproduce the interface with dynamically updated timestamps and status indicators.

Finding 2 — Lack of verifiable authenticity prevents objective checks

Without cryptographic signatures or verifiable tokens, inspectors lack an objective method to distinguish legitimate tickets from visually identical replicas.

Finding 3 — Risk increases with scalability

If replication techniques become widely known, the potential for misuse scales rapidly, increasing enforcement costs and reducing system efficiency.

---

6. Impact Assessment

6.1 Operational Impact

- Increased probability of fare evasion
- Higher workload for inspectors
- Pressure to adopt stricter validation mechanisms

6.2 Trust and Reputation Impact

- Reduced perceived fairness among compliant users
- Potential reputational damage if vulnerabilities are exposed without mitigation

---

7. Recommendations (Security-by-Design)

7.1 Recommended Solution

The most balanced solution is the introduction of a **cryptographically signed QR code or token**, embedded in the ticket and verifiable offline by an inspector's application.

Key characteristics:

- Server-side generation
- Digital signature using public/private key cryptography
- Offline validation capability

7.2 Additional Hardening Measures

- Short-lived rotating tokens (e.g., 2–5 minutes)
- Replay resistance using unique ticket identifiers
- Optional online verification when connectivity is available

---

7.3 Usability Considerations

All proposed solutions aim to:

- Preserve low-friction boarding
- Maintain offline inspection capability

- Minimize latency and operational overhead

---

8. Ethics and Responsible Disclosure

This project follows responsible disclosure principles:

- No real-world misuse was performed
- No sensitive technical details are published
- The proof-of-concept is strictly demonstrative

A detailed disclosure statement is available in the repository documentation.

---

9. Conclusion

Visual-only ticket validation offers operational efficiency but introduces inherent security risks. This analysis demonstrates that introducing **minimal cryptographic verification mechanisms** can significantly improve robustness while preserving the benefits of proof-of-payment systems.

---

10. Appendix

A. Repository Overview

- `src/` — Visual proof-of-concept (static demo)
- `docs/` — Disclosure and analysis documentation