Appendix 14
Logistics for MKD

In the case of MKD, it must always be kept in mind that cryptographic keys are generated and distributed, which are then later used to encrypt potentially secret or top-secret data. Improper generation of keys or distribution of storage media and smart cards can therefore result in legal consequences and significant damage. For this reason, a "Documented Chain of Custody (CoC)" is very important for MKD.

For MKD using a one-time pad, such an eCoC was developed at the St. Pölten University of Applied Sciences. It was developed by Mr. DI Bernhard Steindl, BSc, and is described in detail by him below.

1 Logistics in physical key distribution, esp. MKD

In MKD, distribution logistics becomes the security-critical path of the entire architecture. The decisive factor is the operational controllability under real-world conditions.

1.1 Normative Logistics Concepts Based on ISO Standards as a Procedural Foundation

The physical transport of storage media and smartcards must not be conducted ad hoc but must be regulated by a seamlessly documented and tamper-proof CoC (Chain of Custody). To ensure this, the logistical processes are grounded in established normative frameworks.

The procedural foundation is formed by the standards ISO 28000 and ISO/IEC 27001, which define requirements for risk management in transportation and information security in administrative processes.

In practice, an eCoC is implemented. This system records every physical handover point of the hardware in a tamper-proof manner using cryptographically signed timestamps, precise location data (gps), and the identification of the responsible logistics personnel. To prevent logistical mix-ups that could lead to a loss of the OTP key synchronization status, storage media and smartcards are labeled with unique matrix codes (e.g., according to ISO/IEC 16022).

The central security requirement of this process mandates the separate transport of the SSD and the smartcard. These components must be transported via different logistics service providers, on different transport routes, or with a significant time offset.

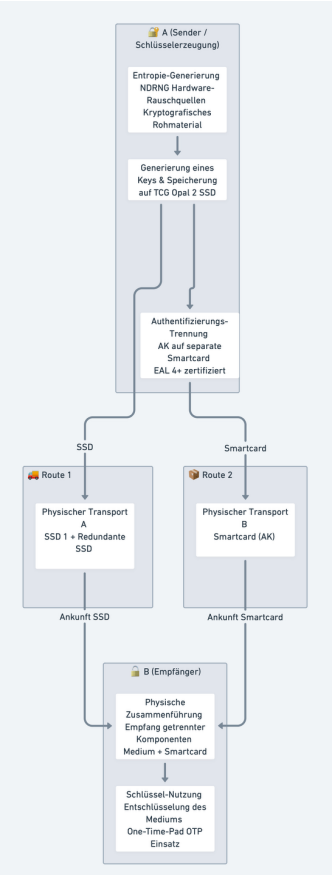


Figure: Process flow of Memory Key Distribution with separate routes and cryptographic details

1.2 Theoretical Attack Vectors During Transport (Man-in-the-Middle, Loss, Manipulation)

By dispensing with network transmission, classical cyberattacks on the key transport are eliminated. Nevertheless, the physical distribution process is subject to specific threat models that must be countered by a combination of technical and organizational countermeasures.

MitM and Interception: An active MitM attack on an MKD infrastructure requires the simultaneous interception of both separate transport routes (the SSD and the corresponding smartcard). If an attacker succeeds only in intercepting the SSD, they face the task of overcoming the AES-256 encryption of the TCG Opal controller without knowledge of the KEK. A passive MitM attack, i.e., the purely informational eavesdropping on the transport route, is physically excluded due to the absence of any electromagnetic data transmission in the resting transport state.

Loss of Hardware: Logistical failures or theft of transport containers represent a realistic operational risk. In the event of loss of the storage medium, the confidentiality of the OTP material remains fully preserved, since the smartcard required for decryption is missing. The affected key dataset is logically revoked in the key management system and removed from rotation. A confidentiality risk for the protected payload data does not arise at any point. The loss leads at most to a restriction in availability (Denial of Service). This risk is mitigated through redundant key distribution: identical key material is maintained on multiple SSDs and transmitted to the receiving side via different transport routes, so that the failure of a single data carrier does not interrupt communication capability.

Physical Manipulation (Tampering and Evil Maid): A highly complex attack vector is the undetected physical modification of hardware during transport. This includes the introduction of hardware Trojans into the controller, as well as attempts to directly read the NAND flash by physically separating the flash chips from the controller board and connecting them to a separate reader (chip-off attack). Since the MEK is stored in the controller and never resides on the flash itself, a chip-off attack yields only AES-256-encrypted data without the corresponding key. To prevent physical manipulation, hardware components are equipped with tamper-evidence seals that visually and irreparably document any physical access. For high-security applications, the storage media are additionally encased in tamper-resistant enclosures conforming to fips 140-2/-3 Level 3 or 4. These enclosures feature active key erasure mechanisms (zeroization): as soon as sensors detect a physical opening attempt, temperature fluctuations beyond defined thresholds, or anomalous voltages, an immediate self-erasure (crypto-erase) of the internal cryptographic parameters is triggered. The hardware irreversibly destroys its key material and becomes unusable.

2 Methodology

The methodological approach of this study follows the dsr framework according to Hevner et al. DSR aims at the iterative construction and evaluation of IT artifacts for solving practice-relevant problems. The process structure follows the DSRM model according to Peffers et al. with the activities: problem identification, objective definition, design, demonstration, evaluation, and communication.

The problem to be solved lies in the secure and traceable physical distribution of storage media and smartcards in MKD. In MKD, the security responsibility shifts to the logistical domain. A purely paper-based implementation is error-prone and offers no non-repudiation. The objective is therefore the conceptualization and prototypical implementation of an eCoC software solution. The methodology is structured into three phases:

1. Requirements analysis
2. Architecture development
3. Evaluation

The following figure shows the mapping of these phases to the DSRM model.

The sixth guideline of Hevner et al. (Design as a Search Process) postulates that artifact development rarely proceeds linearly but rather constitutes an iterative search process of construction and evaluation. In this study, this paradigm manifested particularly in the anomaly detection: the initial implementation was based on a purely reactive timeout detection, which was conceptually contradictory. Since a missed scan typically implies the physical absence of the courier, the subsequent event required for error detection naturally failed to occur. This insight from the first evaluation phase forced a design iteration and led to the implementation of a proactive background process. This sequence illustrates the essence of the DSR search process: practical testing reveals conceptual weaknesses that are systematically eliminated in subsequent iterations.

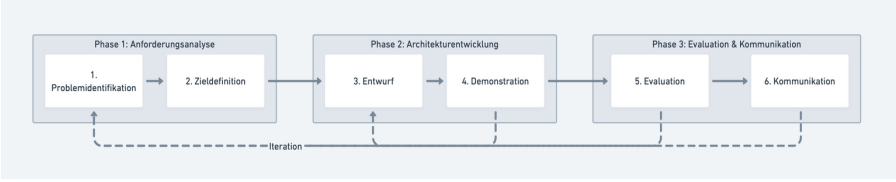


Figure: Mapping of research phases to the DSRM process model

3 Requirements Analysis

The first phase encompasses the systematic elicitation and definition of system requirements for IT-supported logistics in MKD. The requirements are deductively derived from the academic literature, normative specifications on information and supply chain security, and the physical characteristics of the hardware.

3.1 Normative and Conceptual Foundations

The physical distribution of cryptographic key material requires logistics concepts that comply with established normative frameworks (ISO 28000, ISO/IEC 27001). The core component is the CoC, which seamlessly documents the chronological custody, control, and handover of physical or electronic assets. Additionally, the standard ISO 22095 formalizes the requirements for traceability and identity preservation within such chains.

From the mandatory physical separation of storage medium and smartcard during transport, the following requirements for the eCoC software are derived.

3.2 Derivation of Functional and Non-Functional Requirements

The weaknesses of manual distribution systems require the following criteria to be reflected in the system design:

1. **Seamless Traceability (Audit Trail):** Every state change (status, location, responsible person) must be logged in a tamper-proof database structure. Retroactive modification or deletion of records must be cryptographically provable or technically prevented (append-only principle). The coc standard ISO 22095 requires the traceability of every material and informational transfer. This principle is referred to as *Tamper Evidence*: the system cannot prevent manipulation but makes it detectable.
2. **Enforced Separation of Transport:** The eCoC logic must validate that the storage medium and the smartcard remain logistically separated. The system must raise an alarm if scans of both components occur within the same time window at the same gps coordinates by the same person. Formalized: for two assets a_{SSD} and a_{SC} (smartcard) of the same key pair, the following must hold at every point in time t

$$d_{\text{geo}(a_{\text{Speichermedium}}(t), a_{\text{Smartcard}}(t))} > \delta_{\min}$$

where d_{geo} denotes the spatial distance and $\delta_{\min}$ the configurable minimum separation.

3. **Cryptographic Verification (Non-Repudiation):** The identification of transport goods is performed via signed matrix codes (QR codes). Although QR codes are physically copyable, the digital signature using ed25519 (eddsa, RFC 8032) prevents their forgery: an attacker can photograph an existing QR code, but cannot generate a valid QR code for a different asset because the private signing key is missing. In combination with an embedded nonce and an expiration timestamp, replay attacks with copied codes are also precluded. Non-repudiation in this context means: no involved person can retroactively deny the receipt or handover of an asset, since every action is bound to their identity through the authenticated user account.
4. **Anomaly Detection through Mandatory Periodic Scans:** During an active transport, the courier must re-scan the asset within a configurable interval Δt_{scan}. Each scan generates a server-side verified proof (QR signature, gps coordinates, timestamp) and is recorded as an entry in the hash chain. If a scan is missed within the interval, the system automatically generates a security incident (SCAN_TIMEOUT). With each scan, the backend checks the GPS position against the defined geo-fencing perimeter of the transport route. For high-risk transports, $\Delta t_{\text{scan}} = 60$ min is recommended, derived from the check-in intervals of high-security logistics pursuant to ISO 28000. This approach offers two advantages over continuous GPS tracking: first, each scan generates a cryptographically verifiable proof (ed25519 signature + audit log entry), whereas pure GPS coordinates can be falsified through spoofing attacks. Second, periodic scanning does not require a permanent network connection, which ensures usability in environments with limited connectivity (tunnels, underground parking garages).
5. **2fa of Personnel:** All personnel involved in the logistics chain must authenticate upon assuming custody of a hardware token. Authentication is based on an enterprise identity factor (oidc-based single sign-on with pkce), supplemented by two-tier rate limiting to secure the authentication endpoints. For future extension, device binding via WebAuthn is envisioned.

The following table summarizes the requirements and maps them to their normative foundations.

Functional (FA) and non-functional (NFA) requirements with normative mapping.

ID	Requirement	Type	Normative Basis
FA-01	Append-only audit trail with hash chaining	Functional	ISO 22095, ISO 28000
FA-02	Transport separation monitoring	Functional	MKD security architecture
FA-03	Cryptographic asset signing (Ed25519)	Functional	Non-repudiation (ISO/IEC 27001)
FA-04	Anomaly detection through mandatory periodic scans (geo-fencing)	Functional	ISO 28000 risk management
FA-05	Two-factor authentication of personnel	Functional	ISO/IEC 27001 access control
NFA-01	Tamper evidence of audit data	Non-functional	ISO 22095
NFA-02	Offline capability of the mobile app	Non-functional	Operational requirement
NFA-03	Scalability for enterprise operation	Non-functional	Practical requirement

4 Architecture and Design Methodology of the Software Solution

Based on the requirements analysis, the software engineering construction of the eCoC proceeds. The methodology is grounded in the principles of Security by Design and employs a client-server architecture to ensure scalability and resilience.

4.1 System Architecture and Cryptographic Design

The architecture follows a multi-tier model consisting of three components: a mobile pwa for couriers handles the QR scan of assets, gps localization, and local signature verification. A web dashboard serves role management and near-real-time status monitoring. A hardened backend service manages the asset lifecycle, performs separation monitoring, and persists the audit log.

To ensure the integrity of the logging (requirements FA-01, NFA-01), hash chaining is applied to the audit log. Each entry e_i contains a cryptographic sha-256 hash computed over the current metadata and the hash of the preceding entry:

$$h_i = SHA - 256\big(h_{i-1} \parallel t_i \parallel \text{gps}_i \parallel \text{uid}_i \parallel d_i\big)$$

The variables denote: h_{i-1} the hash of the predecessor entry, t_i the timestamp in ISO-8601 format, gps_i the geographic coordinates (latitude, longitude), uid_i the actor ID, and d_i the event-specific data (e.g., asset ID, scan type). The operator $\parallel$ denotes the concatenation of the serialized fields. The initial hash h_0 is set as a fixed genesis value.

This chaining ensures that the modification of a single entry e_j invalidates all subsequent hashes h_k with $k > j$. An attacker would have to recompute the entire subsequent chain. With additional server-side signing of the hashes, such a recomputation becomes provably detectable. The principle corresponds to a blockchain-like data structure but is centrally managed, since the MKD infrastructure presupposes a trusted central authority.

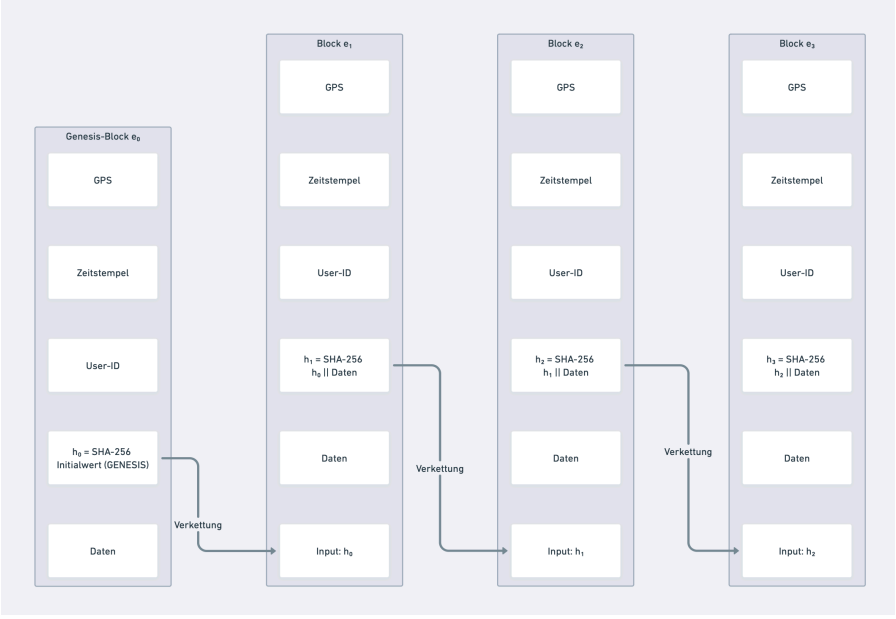


Figure: Schema of hash chaining in the eCoC audit log. Modification of an entry invalidates all subsequent hashes. Generated using DiagramGPT.

4.2 Methodology of the Physical-Digital Binding

The linkage of the physical storage medium with its digital representation (digital twin) in the eCoC database is accomplished through asymmetrically signed QR codes. The objective of the signing is manipulation protection: without a signature, an attacker could print arbitrary QR codes that, when scanned, impersonate a different asset or simulate a handover at a false location. The digital signature ensures that only the backend can generate valid QR codes and that any alteration of the payload (asset ID, destination, time window) causes verification to fail.

The signature scheme uses ed25519 according to RFC 8032. Ed25519 is an instantiation of the eddsa algorithm on Curve25519. The scheme provides a 128-bit security level, produces compact 64-byte signatures, and operates deterministically, i.e., it requires no random number generator during signature generation. The use of pqc signature schemes is currently impractical due to the large signature size on QR codes. An adaptation is reserved for future work.

The signing process comprises four steps:

1. **Payload Generation:** Upon initialization of a transport, the backend generates a payload P consisting of the asset ID a, the destination z, a cryptographic nonce n (a single-use random number to prevent replay attacks), and an expiration timestamp t_{exp}:
$$P = \left(a, z, n, t_{\text{exp}}\right)$$
2. **Signing:** The payload is signed with the backend's private ed25519 key sk:
$$\sigma = Ed25519_{\text{Sign}}\left(\text{sk}, P\right)$$
3. **Encoding:** The QR code encodes the tuple (P, σ) as a Base64-encoded binary string.
4. **Verification:** Upon each scan, the pwa verifies the signature using the backend's public key pk embedded in the app bundle:
$$Ed25519_{\text{Verify}}\left(\text{pk}, P, \sigma\right) \in \{\text{true}, \text{false}\}$$

Since the signature is bound to the specific payload, the nonce n prevents replay attacks, and the expiration timestamp t_{exp} limits temporal validity, cloning and spoofing attacks on the labels are precluded. Without knowledge of the private key sk, no attacker can generate a valid QR code for a different asset or a different destination.

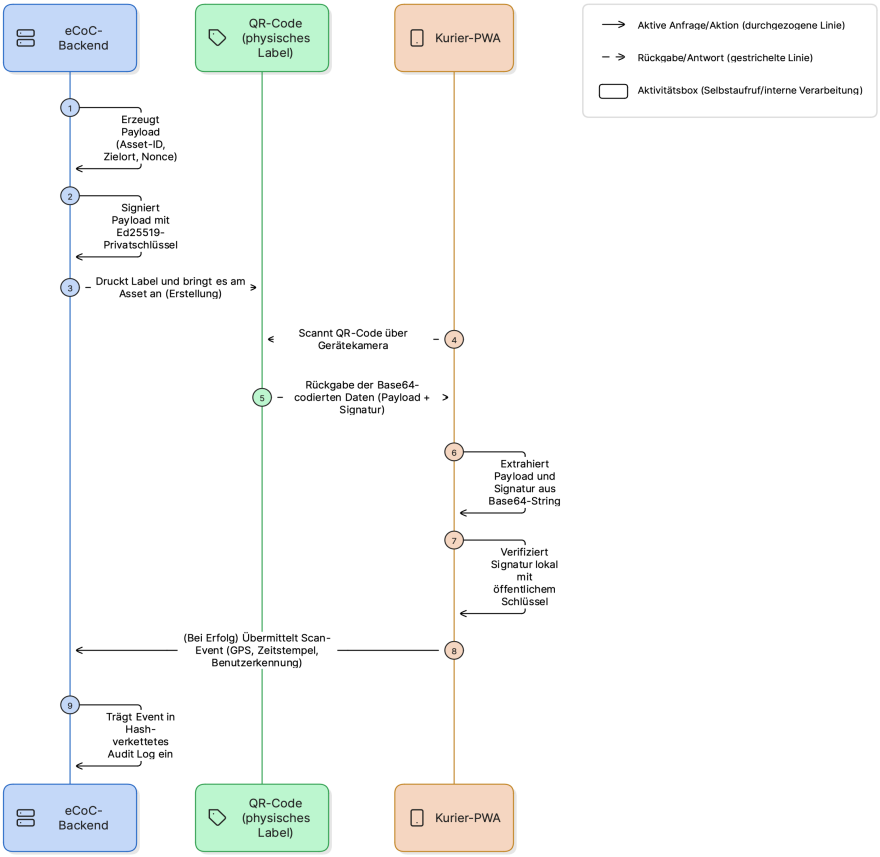


Figure: Sequence diagram of the cryptographically secured QR code lifecycle. Generated using DiagramGPT

5 Evaluation Methodology

The final phase of the dsr cycle constitutes the evaluation of the constructed PoC. Since MKD distribution logistics operates in the high-security domain, the evaluation must demonstrate that the defined protection goals are achieved under realistic conditions and that the solution is operationally manageable. For this purpose, a combined methodology of theoretical security analysis and empirical field testing is applied.

5.1 Security Assessment through Threat Modeling (STRIDE)

To systematically assess the resilience of the architecture, the stride methodology is applied. STRIDE was conceived by Microsoft for systematic threat modeling in software development. The methodology classifies threats into six categories, each addressing a protection goal. The following table maps each category to the MKD-specific attack vectors and the countermeasures implemented in the artifact.

STRIDE threat analysis of the eCoC architecture with assigned countermeasures and protection goals.

STRIDE Category	**Threat in MKD Context**	**Countermeasure**	**Protection Goal**
Spoofing (Identity Forgery)	Attacker impersonates a legitimate courier	2fa via oidc with pkce + two-tier rate limiting (Nginx per IP, Redis per user)	Authenticity
Tampering (Manipulation)	Physical modification of the SSD during transport (Evil Maid Attack)	Tamper-evidence seals, fips 140-2 Level 3 enclosures, cryptographic verification at the recipient	Integrity
Repudiation (Deniability)	Courier denies receipt or handover of the SSD	Hash-chained, server-side signed audit logs (FA-01); mandatory scan upon assumption of custody	Non-repudiation
Information Disclosure (Information Leakage)	Plaintext data about key material on QR codes or in transit	Signed payloads contain only metadata; tls-encrypted transmission	Confidentiality
Denial of Service	Backend overload; transport loss of a data carrier	Rate limiting; redundant key distribution via alternative routes	Availability
Elevation of Privilege	Courier escalates permissions to administrative functions	Role-based access control (oidc scopes); token scoping at function level	Authorization

Figure: Simulation of a Man-in-the-Middle Scenario

A particular focus of the evaluation lies on the simulation of a mitm scenario in the logistics process. Research has documented the vulnerability of gps-based surveillance systems in the automotive domain to such attacks. In the eCoC context, the system's response to three attack scenarios is examined:

Route Deviation: An attacker intercepts the storage medium on the transport route and transports it to an unauthorized location. The expected system behavior is either the triggering of a geo-fencing alarm at the next mandatory scan (FA-04) or the generation of a SCAN_TIMEOUT event if the periodic scan is missed. The maximum detection latency corresponds to the configured scan interval Δt_{scan}.

Retroactive Audit Log Manipulation: An attacker with database access attempts to retroactively modify or delete an existing audit log entry to conceal a transport incident. The expected system behavior is detection through hash chaining (FA-01): since each entry contains the hash of its predecessor, the modification of a single entry invalidates the entire subsequent chain, causing the manipulation to surface at the next integrity check.

QR Code Forgery: An attacker generates a manipulated QR code with an altered asset ID or altered destination to simulate a handover for a different asset or to redirect the transport route. Since the attacker does not possess the backend's private signing key, the ed25519 signature verification (FA-03) fails and the scan is rejected.

The actual system responses (alarm, invalidation, rejection) are evaluated against the defined requirements FA-01 through FA-04.

5.2 Empirical Usability and Process Efficiency Assessment

Beyond security, operational efficiency determines the practical viability of MKD logistics. For evaluation, a comparative experimental design (field test) is implemented.

Experimental Setup: Two distribution scenarios are simulated: the transport of a key pair (nvme-ssd and separate smartcard) over a predefined route with three handover points.

- **Scenario A (Baseline):** Execution according to paper-based ISO-28000 CoC with manual forms and telephone confirmations.
- **Scenario B (Intervention):** Execution with the developed mobile eCoC application.

The following table defines the collected metrics and their operationalization.

Evaluation metrics for the comparative field test.

Metric	Definition	Measurement Method
Checkpoint dwell time	Duration of the logistical halt at the checkpoint (from standstill until departure), caused by the documentation effort	Stopwatch measurement at the checkpoint (seconds)
End-to-end documentation effort	Aggregated time for preparation (printing/setup) and post-processing (digitization/archiving) of the CoC outside of the actual transport time	Stopwatch measurement at origin and destination (seconds)
Information latency	Time span between the actual arrival at the checkpoint and the availability of this information to the receiving person or dispatch	System log analysis or dispatcher logbook (seconds)
Binding degree (non-repudiation)	Degree of forgery resistance and spatial verifiability of the checkpoint passage (time and location)	Ordinal scale: 1 = manual self-entry, 2 = third-party signature, 3 = cryptographically + GPS-secured
Media discontinuity count	Number of system or format changes within the documentation process that carry the risk of information loss	Process flow analysis (absolute count)
Anomaly detection window	Maximum theoretical time span until an unauthorized route deviation or loss is systemically detected	Analytical derivation (duration until the next enforced status update in seconds)

The results serve to demonstrate the extent to which the software solution renders the logistical processes not only more secure but also more time-efficient and manageable for enterprise-scale operations.

6 Results

This chapter presents the results of the evaluation for the eCoC system. The assessment is conducted along three dimensions: security analysis through stride threat modeling, verification of requirements fulfillment, and an operative comparison of the product against conventional systems in a field test.

7 Security Analysis: STRIDE Evaluation

The stride analysis was conducted against the implemented architecture. The following sections evaluate the implemented countermeasures and their effectiveness for each threat category.

7.1 Spoofing: Identity Forgery

The oidc-based authentication delegates identity verification to an external identity provider. The validation of the ID token via JWKS ensures that only tokens signed by the configured provider are accepted. The local shadow user provisioning synchronizes roles at each login. An attacker without valid credentials at the identity provider cannot send authenticated requests to the backend. The two-tier rate limiting limits brute-force attempts on the token exchange endpoint to five requests per minute per IP address.

Limitation: Whether the external identity provider has implemented critical security features such as 2fa or other hardening measures cannot be determined from the application side. The planned device binding could not be implemented. A compromised jwt can therefore be used from any device until it expires. The short token lifetime and user-bound rate limits minimize this residual risk.

7.2 Tampering: Manipulation

The tamper resistance of the audit log was verified through the execution of three scenarios:

Direct Database Manipulation: The attempt to modify an existing audit log entry via an SQL UPDATE statement is rejected by the PostgreSQL trigger `trg_audit_log_immutable` with an exception. DELETE statements are likewise blocked. Only through manipulation of the database configuration could entries be altered.

Hash Chain Integrity Check: After manual modification of an entry (with temporary deactivation of the trigger in the test environment), the function `verify_audit_chain` detects the manipulation, since the newly computed hash of the modified entry does not match the stored `previous_hash` of the successor entry. The following figure illustrates this detection.

Genesis Validation: The first entry of the chain is correctly initialized with the predecessor hash `"GENESIS"`. Inserting a manipulated entry before the first legitimate entry would invalidate the entire subsequent hash chain.

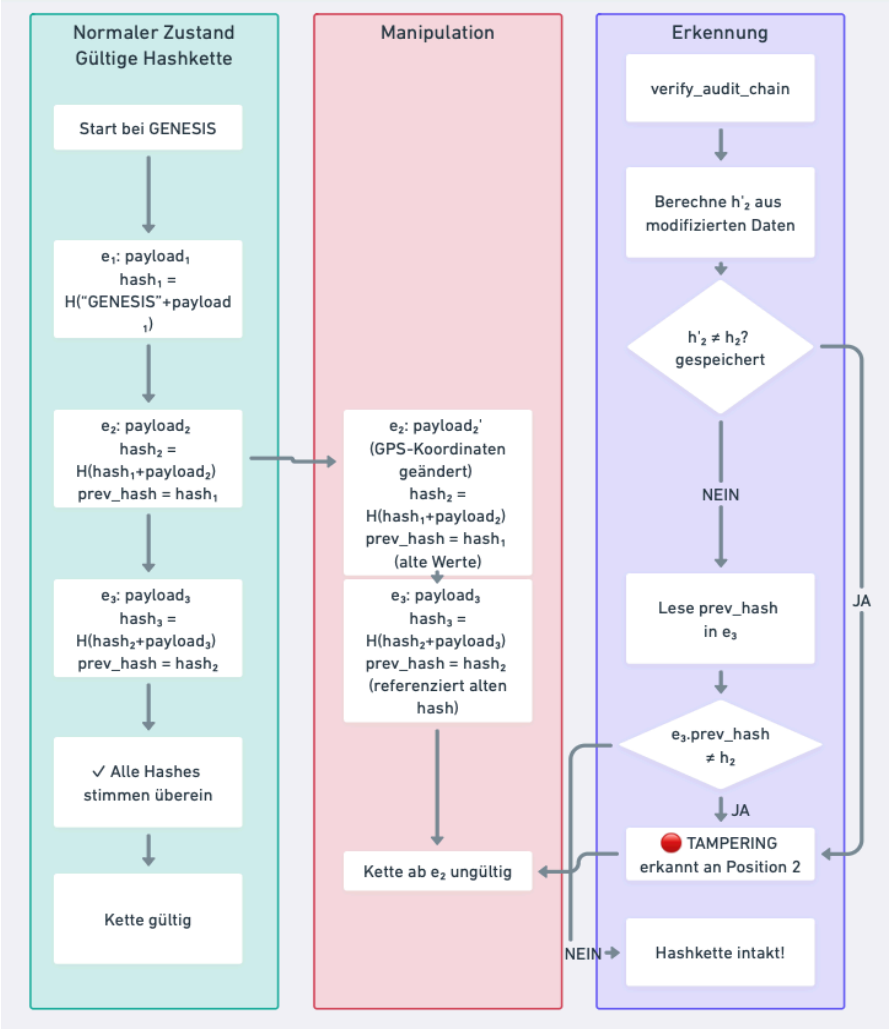


Figure: Schematic representation of a manipulated hash chain

7.3 Repudiation: Deniability

Each audit log entry contains the `actor_id` (UUID of the authenticated person) and the `actor_display_name` (frozen at the time of the entry). Since every action requires prior OIDC authentication and the audit entries cannot be modified due to the PostgreSQL trigger, no involved person can retroactively deny having performed a scan. The compliance confirmation for SCAN_IN and SCAN_TRANSIT events is permanently logged as metadata in the audit entry and provides additional non-repudiation evidence.

7.4 Information Disclosure: Information Leakage

Access control prevents unauthorized information access at multiple levels: couriers see only their own leg transports; parent transports are blocked for the courier role since they would expose the IDs of both assets (SSD and smartcard). The OIDC subject ID (`sub`/`oid`) is not exposed in API responses. The QR code payloads contain exclusively metadata (asset ID, destination, nonce), no information about the key material. tls encryption via Nginx and a restrictive csp protect data transmission.

7.5 Denial of Service

The two-tier rate limiting restricts both unauthenticated (IP-based via Nginx) and authenticated (user-based via Redis) requests. The pwa caching strategy enables the continuation of scan operations even during temporary backend unavailability (NFA-02). The offline queue based on IndexedDB stores scan events locally and transmits them upon restored connectivity.

7.6 Elevation of Privilege

Role-based access control is enforced at two levels. First, the role is read exclusively from the validated ID token of the identity provider. Second, the backend middleware `require_role` checks the role claim of the internal JWT with each request. Couriers cannot create assets or transports (403 Forbidden); transport creation and SCAN_IN are restricted to ADMIN and TRANSPORT_ADMIN. Parent transports do not accept direct status changes via the API (409 Conflict).

8 Attack Scenario Results

The three attack scenarios were evaluated against the product.

8.1 Scenario 1: Route Deviation

Execution: A SCAN_IN was performed at the correct origin coordinates. The subsequent SCAN_OUT was performed at the same location by Bernhard Karl Steindl, although this person was neither the configured recipient nor the authorized location.

Result: The system detected the deviation and generated an incident. The corresponding entry was stored in an audit-proof manner in both the transport documentation and the audit log. The incident appeared in the admin dashboard. Detection was generated within the second in which the scan was performed.

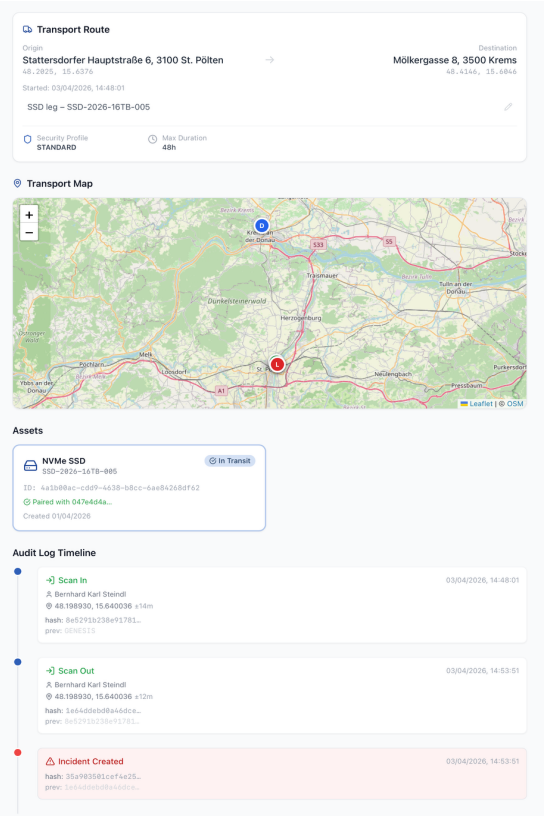


Figure: View of the manipulated transport. Own illustration.

8.2 Scenario 2: Retroactive Audit Log Manipulation

Execution: In the test environment, the PostgreSQL trigger was temporarily deactivated and an existing audit log entry was modified (alteration of the GPS coordinates of a field).

Result: The function `verify_audit_chain` detected the manipulation. The newly computed hash of the modified entry did not match the stored `previous_hash` of the successor entry. Under regular operation (trigger active), the modification is already blocked at the database level and the attempt is rejected with an exception.

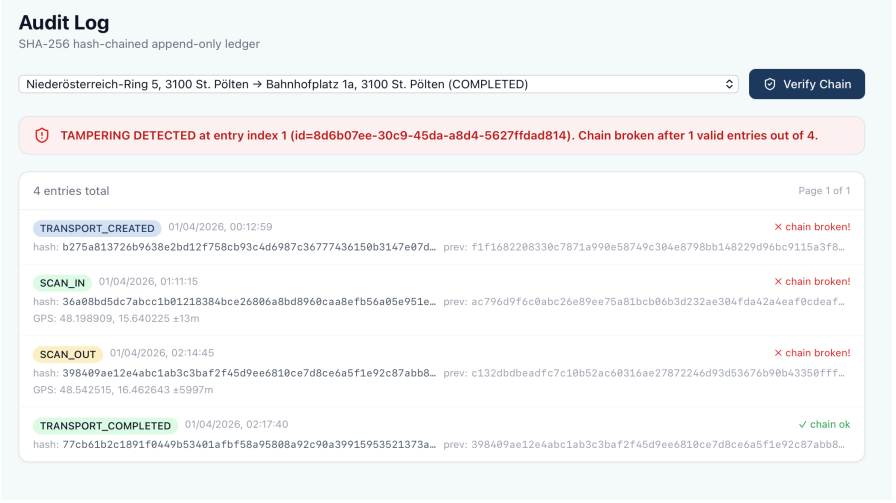


Figure: View of the manipulated hash chain. Own illustration

8.3 Scenario 3: QR Code Forgery

Execution: A QR code was generated with a manipulated asset ID and an invalid Ed25519 signature, and presented to the PWA camera.

Result: The signature verification failed both client-side (TweetNaCl in the PWA) and server-side (PyNaCl in the backend). The system automatically generated a `SCAN_FORGERY_ATTEMPT` incident with severity CRITICAL and logged the attempt in the audit log with all available metadata (GPS, timestamp, actor). The forged QR code was rejected and no status change was made to the transport.

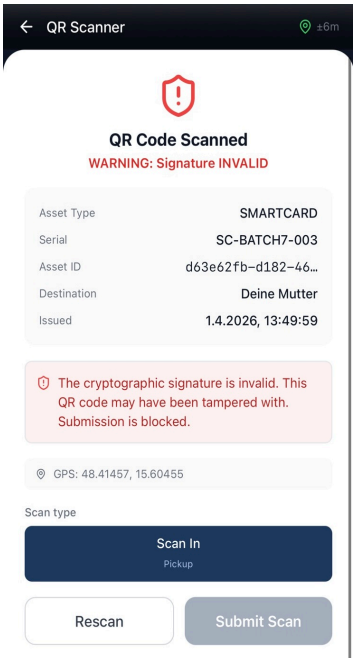


Figure: Manipulated QR code is blocked due to invalid signature. Own illustration

The above figure shows the error dialog displayed during the scan attempt. The rejection occurred within milliseconds, as the client-side TweetNaCl verification immediately rejected the forged QR code. The server-side verification via PyNaCl confirmed this result and logged the incident in an audit-proof manner.

The following table summarizes the results of the three scenarios.

Summary of attack scenario results.

Scenario	Attack	System Response	Requirement
1	Route deviation	INCIDENT created, visible in dashboard, stored in audit-proof manner in audit log	FA-04
2	Audit log manipulation	Hash chain invalidated; PG trigger blocks under normal operation	FA-01, NFA-01
3	QR code forgery	Warning created (CRITICAL); scan rejected	FA-03

9 Requirements Fulfillment

The following table presents the degree of fulfillment of the functional and non-functional requirements and references the respective implementation components.

Degree of fulfillment of the functional and non-functional requirements.

ID	Requirement	Status	Implementation and Notes
FA-01	Append-only audit trail with hash chaining	Fulfilled	PG trigger + sha-256 chaining; `verify_audit_chain` for integrity verification
FA-02	Transport separation monitoring	Fulfilled	PostGIS `ST_DWithin` with configurable distance (500 m) and time window (24 h)
FA-03	Cryptographic asset signing (Ed25519)	Fulfilled	PyNaCl (backend) + TweetNaCl (frontend); QR v2 without expiration; replay protection via state machine
FA-04	Anomaly detection	Fulfilled	Geo-fencing and scan sequencing implemented; proactive SCAN_TIMEOUT background process implemented
FA-05	Two-factor authentication	Partially fulfilled	OIDC pkce + rate limiting; device binding and step-up auth. not implemented
NFA-01	Tamper evidence of audit data	Fulfilled	PG trigger blocks UPDATE/DELETE; hash chain verifiable
NFA-02	Offline capability of mobile app	Fulfilled	Workbox caching + IndexedDB offline queue with timestamp preservation
NFA-03	Scalability for enterprise operation	Partially fulfilled	Single-process operation stable; distributed locks for hash chain not implemented

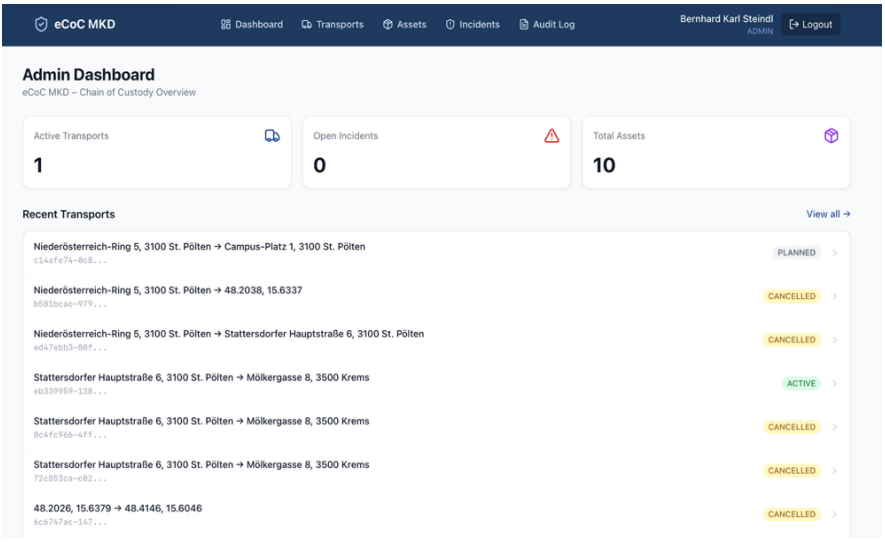
Of the eight defined requirements, six are fully fulfilled (FA-01, FA-02, FA-03, FA-04, NFA-01, NFA-02) and two are partially fulfilled (FA-05, NFA-03). The partially fulfilled requirements concern aspects that exceed the scope of a poc (distributed

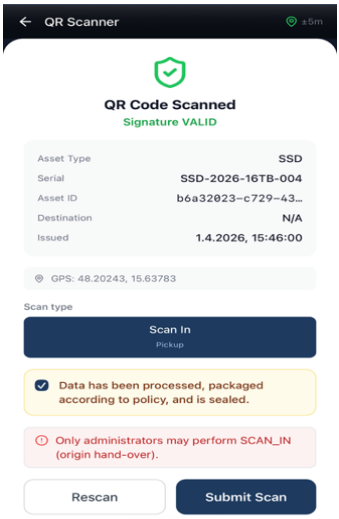
synchronization for cluster operation) or are conditioned by limitations of the deployed identity provider (2FA enforcement not verifiable, step-up authentication).

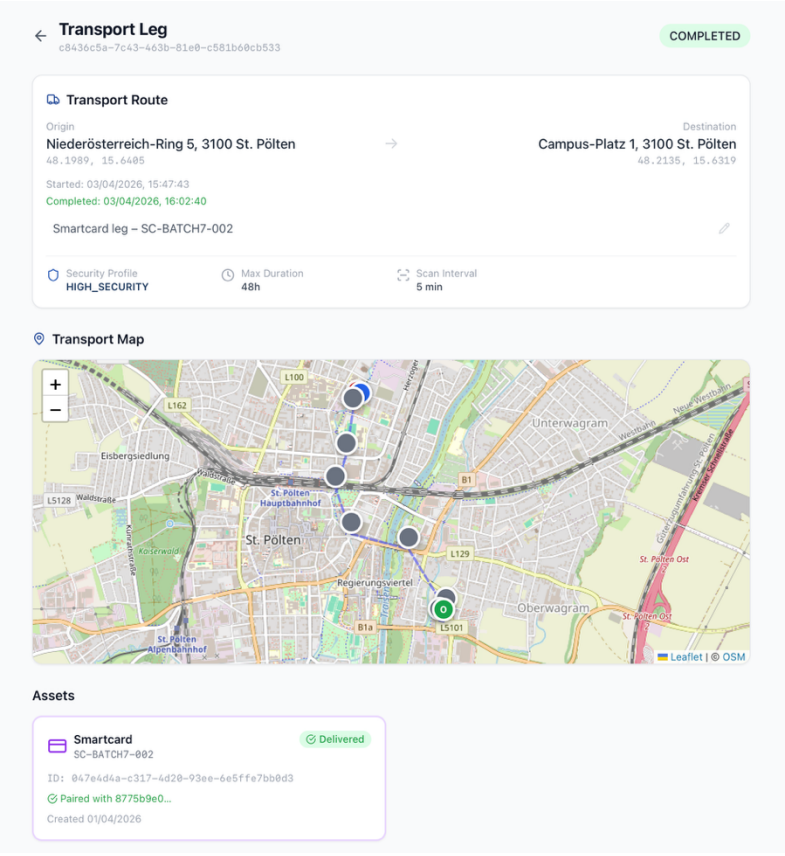
It should be noted that the partially fulfilled requirements do not impair the core functionality of the system: FA-05 ensures a high security level through OIDC and rate limiting; NFA-03 is sufficient for operation in smaller environments.

10 Demonstration in a Logistical Deployment Scenario

The eCoC product was deployed as a containerized application and evaluated in a simulated transport scenario. The demonstration covered the complete lifecycle of an MKD distribution: creation of a parent transport with two leg transports (storage medium and smartcard), registration of the assets with ed25519-signed QR codes, execution of scan events at various locations, and the analysis of the resulting audit log.




QR Scanner
±5m
QR Code Scanned
Signature VALID
Asset Type
SSD
Serial
SSD-2026-16TB-004
Asset ID
b6a32023-c729-43...
Destination
N/A
Issued
1.4.2026, 15:46:00
GPS: 48.20243, 15.63783
Scan type
Scan In
Pickup
Data has been processed, packaged according to policy, and is sealed.
Only administrators may perform SCAN_IN (origin hand-over).
Rescan
Submit Scan


Transport Leg
c8436c5a-7c43-463b-81e0-c581b60cb533
COMPLETED
Transport Route
Origin
Niederösterreich-Ring 5, 3100 St. Pölten
48.1989, 15.6405
Destination
Campus-Platz 1, 3100 St. Pölten
48.2135, 15.6319
Started: 03/04/2026, 15:47:43
Completed: 03/04/2026, 16:02:40
Smartcard leg – SC-BATCH7-002
Security Profile
HIGH_SECURITY
Max Duration
48h
Scan Interval
5 min
Transport Map
L100
L162
Eisbergsiedlung
L5128
Waldstraße
St. Pölten Hauptbahnhof
St. Pölten
Kurparkstraße
Kurerwald
Regierungsviertel
B1
L129
Unterwagram
Oberwagram
B1a
L5101
St. Pölten Ost
St. Pölten Alpenbahnhof
Leaflet | OSM
Assets
Smartcard
SC-BATCH7-002
Delivered
ID: 047e4d4a-c317-4d20-93ee-6e5ffe7bb0d3
Paired with 8775b9e0...
Created 01/04/2026

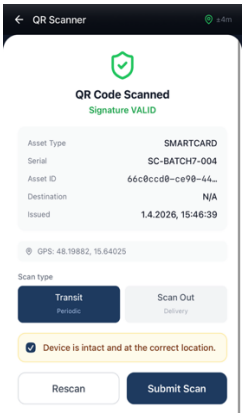


Figure: User interface of the eCoC PWA: Dashboard (top left), QR Scan-In (top right), Transport overview (bottom left), QR Scan-Out (bottom right). Own illustration.

The workflow of a complete MKD distribution in the HIGH_SECURITY profile comprises the following steps:

1. **Transport Creation:** A transport administrator creates a parent transport via the dashboard and assigns the SSD and the smartcard as separate leg transports. Origin and destination coordinates are set via an interactive map picker or text-based address entry. For each leg, a courier and a recipient are assigned.
2. **Asset Registration:** The physical storage media are registered in the system and equipped with Ed25519-signed QR labels. The QR code contains the asset ID, type, serial number, destination, and a cryptographic nonce.
3. **Pickup (SCAN_IN):** The sending person (ADMIN or TRANSPORT_ADMIN) scans the QR code of the asset. The system verifies the Ed25519 signature, checks the gps position against the origin location (geo-fencing), and creates the first hash-chained audit log entry with the genesis hash. The transport status changes from PLANNED to ACTIVE, the asset status from IN_STORAGE to IN_TRANSIT.
4. **Transit Scans (SCAN_TRANSIT):** The courier scans the asset periodically at the configured interval. Each scan generates a hash-chained audit entry with GPS coordinates. The transport trail map on the detail page updates accordingly.
5. **Delivery (SCAN_OUT):** The configured recipient scans the QR code at the destination. The system verifies that the scanning person is the configured recipient and that the sender and receiver are different. After successful verification, the leg status changes to COMPLETED and the asset status to DELIVERED. The parent transport status is automatically updated.

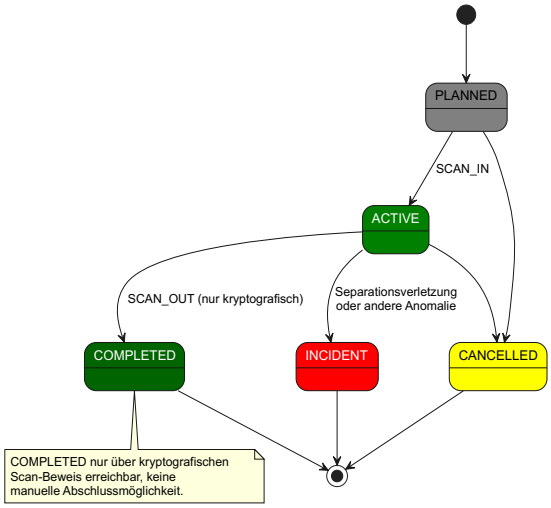


Figure: Workflow of a transport in the eCoC system. Own illustration

10.1 Empirical Field Test Based on an Example in St. Poelten

Beyond security, operational efficiency determines the practical viability of MKD logistics. For evaluation, a comparative experiment was conducted.

Experimental Setup: Two distribution scenarios are simulated: the transport of a key pair (nvme-ssd and separate smartcard) over a predefined route with four checkpoints. The route runs between two addresses in St. Poelten, namely Niederoesterreich-Ring 5, 3100 St. Poelten (hereinafter referred to as *Origin*) and the location of the University of Applied Sciences St. Poelten, Campus-Platz 1, 3100 St. Poelten (*Destination*). The distance is 2.7 km.

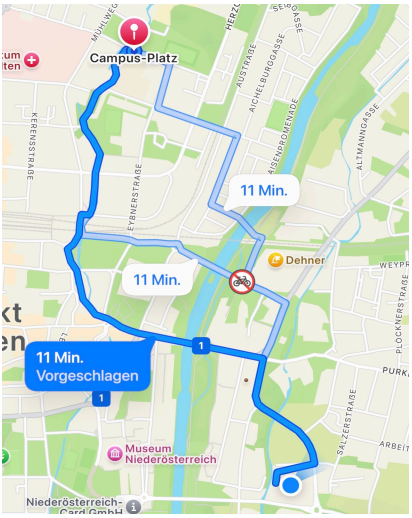


Figure: Routes used for the field test. Map data: © OpenStreetMap contributors (ODbL)

The route can be traversed by a standard bicycle in 11 minutes. To comply with the security prerequisites of MKD, the route was traversed 4 times:

1. Transport of the SSD from origin to destination with paper-based chain of custody
2. Transport of the smartcard from origin to destination with paper-based chain of custody
3. Transport of the SSD from origin to destination with electronic chain of custody
4. Transport of the smartcard from origin to destination with electronic chain of custody

To ensure comparability, the following modifications were made relative to the original processes:

- Reduction of the geo-fencing threshold from 500 to 250 m, minimum time duration reduced from 24 h to one hour (for eCoC)
- Traversal of the same route for all 4 runs, to compensate for anomalies and collect more measurement points

The following checkpoints were defined along the route to ensure comparability:

1. Checkpoint “Chinese Restaurant” (48.203718, 15.636911)
2. Checkpoint “Neugebäudeplatz” (48.204748, 15.630937)
3. Checkpoint “Westbahnbrücke” (48.207855, 15.629380)
4. Checkpoint “Bettelampel” (48.210089, 15.630418)

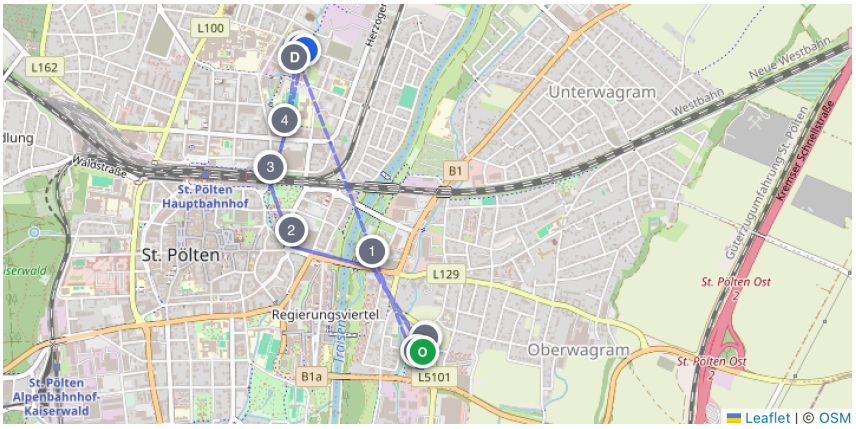


Figure: Overview of checkpoints for the field test, dashed line indicates direct straight-line distance. Map data: © OpenStreetMap contributors (ODbL). Own illustration

- **Scenario A (Baseline):** Execution according to paper-based ISO-28000 CoC with manual forms and telephone confirmations.
- **Scenario B (Intervention):** Execution with the developed mobile eCoC application.

The following table defines the collected metrics and their operationalization.

Evaluation metrics for the comparative field test.

Metric	Definition	Measurement Method
Checkpoint dwell time	Duration of the logistical halt at the checkpoint (from bicycle standstill until departure), caused by the documentation effort	Stopwatch measurement at the checkpoint (in seconds)
End-to-end documentation effort	Aggregated time for preparation (printing/setup) and post-processing (digitization/archiving) of the CoC outside of the actual transport time	Stopwatch measurement at origin and destination (in seconds)
Information latency	Time span between the actual arrival at the checkpoint and the availability of this information to the receiving person (destination) or the dispatch.	System log analysis (eCoC) vs. dispatcher logbook/telephone call (baseline) (in seconds)

Metric	Definition	Measurement Method
Binding degree (non-repudiation)	Degree of forgery resistance and spatial verifiability of the checkpoint passage (time and location)	Ordinal scale (1 = manual self-entry, 2 = third-party signature, 3 = cryptographically + GPS-secured)
Media discontinuity count	Number of system or format changes within the documentation process (e.g., physical to digital, verbal to written) that carry the risk of information loss	Process flow analysis (absolute count)
Anomaly detection window	Maximum theoretical time span until an unauthorized route deviation or loss of the component is systemically detected.	Analytical derivation (duration until the next enforced status update in seconds).

10.2 Scenario A (Baseline) – Paper-Based Chain of Custody System

First, a transport was simulated in accordance with the guidelines defined by ISO 28000 for security management systems in the supply chain. The standard establishes the fundamental framework for seamless traceability and the protection of transport goods against manipulation or loss. However, since ISO 28000 does not prescribe specific, binding form layouts but rather sets procedural requirements for the documentation obligation, a standardized physical transport protocol was designed for this field test. This protocol aims to document the integrity of the cryptographic key material (NVMe SSD and smartcard) across the entire route and to unambiguously clarify the responsibilities (*non-repudiation*) at every control point.

The paper-based CoC document used for the baseline enforces the systematic capture of all security-critical metadata by the courier. It logically structures the transport into four phases: preparation and authorization at the starting point (*origin*), the ongoing checkpoint logbook, a dedicated protocol for any anomalies, and the final receipt and identity verification at the destination. At each of the four defined checkpoints, the courier must stop, visually verify the integrity of the security container or seal, make a brief phone call to the recipient, record the exact time, and countersign this procedure with a handwritten signature.

Although this analog procedure meets the theoretical documentation requirements of the ISO standard, it introduces systemic weaknesses in operational

practice. The process is not only highly susceptible to human error, such as illegible entries or iterative documentation mistakes, but also forces the courier into repeated media discontinuities. The manual reading and noting of timestamps under weather conditions creates a significant administrative overhead (dwell time). More critically, however, is the high information latency: since status updates are not transmitted to the dispatch in a timely manner, an unauthorized route deviation or compromise attempt is only detected retrospectively at the destination, as these cannot be determined via telephone. The temporal window for anomaly detection under this baseline is therefore maximally large.

Results

The corresponding transport was conducted on 03.04.2026.

Evaluation metrics for the comparative field test.

Metric	Measurement Method	Result
Checkpoint dwell time	Stopwatch measurement at the checkpoint (in seconds)	Smartcard: 1 (118s), 2 (78s), 3 (43s), 4 (49s) SSD: 1 (61s), 2 (55s), 3 (50s), 4 (44s)
End-to-end documentation effort	Stopwatch measurement at origin and destination (in seconds)	Smartcard: Origin: 51s, Destination 38s SSD: Origin: 44s, Destination (not documented)
Information latency	System log analysis (eCoC) vs. dispatcher logbook/telephone call (baseline) (in seconds)	Only upon arrival at destination (SC: 21 minutes, SSD: 20 minutes)
Binding degree (non-repudiation)	Ordinal scale (1 = manual self-entry, 2 = third-party signature, 3 = cryptographically + GPS-secured)	1 (protocol) 2 (phone calls + handover)
Media discontinuity count	Process flow analysis (absolute count)	4 signatures (2 each at handover), 4 phone calls
Anomaly detection window	Analytical derivation (duration until the next enforced status update in seconds).	Phone call frequency at each checkpoint, but no audit-proof documentation

The total duration of the paper-based transports amounted to 21 minutes (smartcard) and 20 minutes (SSD), each including preparation and post-processing. The pure cycling time for the route is approximately 11 minutes. The difference is attributable to administrative overhead: at each of the four checkpoints, the courier had to stop, verify the integrity of the transport container, make a phone call to the recipient, manually document the time and location, and countersign with a signature. The first checkpoint of the smartcard transport particularly illustrates the high effort: 118 seconds dwell time, since this was the first instance of handling the protocol form under real conditions (clipboard on the bicycle, wind). With increasing routine, the dwell time decreased to 43 to 49 seconds. The aggregated checkpoint dwell time amounts to 288 seconds (4.8 minutes) for the smartcard and 210 seconds (3.5 minutes) for the SSD.

A significant disadvantage of the paper-based procedure is the lack of timely status information: the receiving side only gained knowledge of the transport progress upon the physical arrival of the courier. The telephone check-ins at the checkpoints offered a rudimentary status channel but were neither audit-proof nor backed by precise GPS coordinates.

10.3 Scenario B (Developed Electronic Chain of Custody System)

First, the transports were created in the system. The corresponding assets (smartcard and SSD) were labeled with QR codes and packaged accordingly. The corresponding protocols were all created automatically.

The transport durations were extracted from the automatically generated audit logs of the eCoC system. The smartcard transport was started at 15:47:43 (SCAN_IN by the sending person Bernhard Karl Steindl) and completed at 16:02:40 (SCAN_OUT by the recipient Doug Hefferman), resulting in a total duration of 14 minutes and 57 seconds. The SSD transport was started at 17:37:14 and completed at 17:51:42 (total duration: 14 minutes and 28 seconds). Both transports were conducted in the HIGH_SECURITY profile with a scan interval of 5 minutes.

At each of the four defined checkpoints, a SCAN_TRANSIT event was triggered. The entire scan process (stopping, unlocking the smartphone, scanning the QR code, confirming the event type, confirming the compliance checkbox, submitting) required less than 15 seconds each. Since the scan submission timestamps reflect server processing rather than the exact moment of stopping, the checkpoint dwell time was estimated from the difference between the scan submission and the interpolated arrival time.

Concurrently with the transport operations, the SCAN_TIMEOUT background process was active. The container logs confirm correct functionality: the scheduler

checked the status of both active transports every 5 minutes and confirmed that the scan intervals were being maintained.

Evaluation metrics for the field test with the eCoC system (Scenario B).

Metric	Measurement Method	Result
Checkpoint dwell time	Audit log analysis and estimation (in seconds)	Smartcard: approx. 10–15s each SSD: approx. 10–15s each
End-to-end documentation effort	Audit log analysis (in seconds)	Smartcard: Origin: 10s, Destination: 10s SSD: Origin: 10s, Destination: 10s
Information latency	System log analysis (eCoC) vs. dispatcher logbook/telephone call (baseline) (in seconds)	Information available in near-real-time via eCoC and traceable
Binding degree (non-repudiation)	Ordinal scale (1 = manual self-entry, 2 = third-party signature, 3 = cryptographically + GPS-secured)	3
Media discontinuity count	Process flow analysis (absolute count)	2 (affixing QR code labels on package)
Anomaly detection window	Analytical derivation (duration until the next enforced status update in seconds).	At most 5 minutes; for forgeries (geo-fencing, recipient) earlier

The eCoC solution reduced the documentation effort at each checkpoint to a fraction of the paper-based procedure. Instead of handwritten documentation, telephone check-ins, and signatures, the scan process required only scanning the QR code with the smartphone and confirming a preselected event type. The automatic capture of GPS coordinates, timestamps, and actor ID completely eliminated manual data entry.

10.4 Comparison of Scenarios

The following table contrasts the results of both scenarios.

Comparison of evaluation metrics: paper-based CoC (Scenario A) vs. eCoC system (Scenario B).

Metric	Scenario A (Paper CoC)	Scenario B (eCoC)
Checkpoint dwell time	SC: 72s mean (43–118s) SSD: 53s mean (44–61s)	approx. 10–15s per checkpoint (reduction by approx. 80%)
End-to-end documentation	SC: 89s (origin + destination) SSD: 82s (estimated)	approx. 20s (scan in + scan out) (reduction by approx. 78%)
Information latency	Only upon arrival at destination (SC: 21 min, SSD: 20 min)	Near-real-time (< 2s after scan)
Binding degree	Level 1–2 (self-entry, third-party signature)	Level 3 (cryptographic + GPS)
Media discontinuities	8 (4 signatures + 4 phone calls)	2 (affixing QR labels)
Anomaly detection window	Maximum transport duration (20–21 min) No audit-proof documentation	Maximum 5 min (configured scan interval) For forgery/recipient: immediate
Total transport duration	SC: 21 min, SSD: 20 min	SC: 15 min, SSD: 14.5 min

The comparison shows that the eCoC system achieves improvements over the paper-based procedure in all six metrics. The checkpoint dwell time was reduced by approximately 80%, the information latency was lowered from the order of minutes to less than two seconds, and the binding degree was elevated from manual self-entry to cryptographically secured attestations. Particularly significant is the reduction of the anomaly detection window: whereas under the paper-based procedure a route deviation is detected at the earliest upon arrival at the destination, the eCoC system detects deviations at the latest by the next enforced scan (in the field test: 5 minutes) or immediately in the case of recipient and signature violations.

11 Discussion

This chapter contextualizes the presented results within the scientific framework and evaluates the security architecture of the eCoC system. Finally, the limitations of the field trial and threats to validity are reflected upon.

12 Security Assessment: Remediation of Logistical Vulnerabilities through the eCoC System

The stride analysis following Shostack has shown that the eCoC system implements effective countermeasures for each of the six threat categories. The system's response to the three simulated attack scenarios (route deviation, audit log manipulation, QR code forgery) confirms the functionality of the implemented protection mechanisms under controlled conditions. The central security aspects are evaluated in detail below.

12.1 Cryptographic Integrity of the Audit Trail

The hash chaining of the audit log following the append-only principle constitutes a central differentiating feature compared to conventional (database) logs. Through the combination of sha-256 chaining and PostgreSQL triggers, a two-layer tamper evidence is achieved: the cryptographic layer makes manipulations detectable, the database layer prevents them at the SQL level. This architecture corresponds to the concept of a centralized blockchain-like structure, as recommended by Badiye et al. for forensic chain of custody, while dispensing with the overhead of a distributed consensus mechanism, since the MKD infrastructure presupposes a trusted central authority.

As a caveat, it should be noted that an attacker with direct access to the database level (e.g., through compromise of the database server) could deactivate the PostgreSQL trigger and subsequently recompute the hash chain in its entirety. This residual risk is addressed through the combination of physical server security, role-based database access control pursuant to ISO/IEC 27001, and the possibility of periodic external hash chain audits (using `verify_audit_chain`), but is not entirely eliminated. A more advanced safeguard would be achievable through the regular publication of anchor hashes in an external, independent system (e.g., a public blockchain network).

12.2 Effectiveness of the QR Signature and the State Machine

The ed25519 signing (RFC 8032, based on Curve25519) of QR code payloads addresses the attack vector of asset forgery. Since the physical QR labels are copyable but not forgeable without the private signing key, the physical-digital binding is cryptographically secured. The design decision made in the product to omit the expiration timestamp (t_{exp}) and instead realize replay protection via the

server-side state machine proves to be practicable: physical QR labels can be printed at registration and used indefinitely without requiring regeneration before each transport.

The dual signature verification on both client and server side increases security in the sense of defense-in-depth but requires the precise maintenance of cryptographic libraries on both platforms. At the same time, the canonical JSON serialization ensures that data is processed identically across platforms. However, since this strict formatting is merely an unwritten contract between frontend and backend, it carries a risk of errors during future refactorings.

An architectural limitation of this serialization logic concerns the handling of nested objects: the sorting implemented in the TypeScript frontend via `Object.keys(payload).sort()` operates exclusively on the topmost hierarchy level of the JSON object. In the current payload format, this is non-critical since all fields are flat-structured. However, if the payload were to contain nested objects or arrays in the future, the key ordering within nested structures could vary depending on the JavaScript engine, which would lead to non-deterministic serializations and consequently to failing signature verifications. As a robust long-term solution, the adoption of a formal standard such as RFC 8785 (JSON Canonicalization Scheme, JCS) would be advisable, which specifies recursive key sorting and a normalized number representation.

12.3 Separation Monitoring and Geo-Fencing

The PostGIS-based separation monitoring implements the requirement for enforced separation of transport (FA-02). The dual condition (spatial proximity *and* temporal proximity) avoids false alarms during sequential use of the same transport route, which is common in practice. The configuration used in the field test (500 meters minimum distance, adjusted to 250 meters; 24 hours time window, adjusted to 1 hour) demonstrates the configurability of the system for different risk levels.

The accuracy of the geo-fencing checks depends on the gps precision of the deployed mobile devices. In the field test, accuracies of 4 to 18 meters were observed. For urban environments, this is sufficient; in scenarios with limited GPS reception (indoors, underground parking garages), the position data is less reliable. Since the system uses GPS positions only as supplementary evidence and not as the sole authentication feature, this limitation does not substantially impair overall security.

12.4 Proactive Anomaly Detection

The implementation of the SCAN_TIMEOUT background process closes a significant gap of the initial product. Reactive detection, where timeouts are only identified by the next incoming scan, is conceptually contradictory: if the courier is absent, precisely this triggering subsequent scan fails to occur, leaving the timeout unnoticed. Proactive checking through the APScheduler-based background process ensures that missing scans are detected within the configured check interval (default: 5 minutes). The idempotency logic (one incident per missed interval, progressive catch-up) prevents flooding of the incident system during prolonged outages.

13 Comparison: eCoC vs. Paper-Based Process

The comparative field test provides evidence for the superiority of the software-supported approach over the paper-based procedure across all six collected metrics. ISO 28000 defines requirements for security management systems in the supply chain, yet without specific specifications for cryptographic integrity proofs – a gap that the eCoC system addresses. The field test results are contextualized below.

13.1 Reduction of Administrative Overhead

The checkpoint dwell time was reduced from an average of 62 seconds (paper) to an estimated 10 to 15 seconds (eCoC), corresponding to a reduction of approximately 80%. The cause lies in the elimination of manual documentation steps: whereas the paper-based process requires handwritten entries, telephone confirmations, and signatures, the eCoC workflow is limited to the QR scan with automatic data capture. The total transport duration decreased from 20 to 21 minutes to 14.5 to 15 minutes, even though the eCoC transports were configured in the HIGH_SECURITY profile with additional intermediate scans.

As a caveat, the field test was conducted with a route of merely 2.5 km and four checkpoints. Extrapolation to longer distances and more frequent handovers is likely to disproportionately amplify the efficiency gain, since the paper-based overhead increases linearly with each additional checkpoint, while the eCoC scan effort remains nearly constant.

13.2 Information Latency and Timely Availability

The most significant difference lies in information latency. Under the paper-based procedure, the receiving side obtained a complete status overview only upon the physical arrival of the courier (after 20 to 21 minutes). The telephone check-ins offered a rudimentary status channel but were neither audit-proof nor backed by precise location data. The eCoC system, in contrast, made every scan event available in the dashboard within less than two seconds, including cryptographically secured GPS coordinates and a hash-chained audit entry.

This timely availability is critical for anomaly detection: whereas a route deviation under the paper-based procedure is detected at the earliest upon arrival at the destination, the eCoC system reduces the detection window to the configured scan interval (in the field test: 5 minutes) or detects certain anomalies (signature violations, recipient deviations) immediately.

13.3 Binding Degree and Non-Repudiation

The binding degree was elevated from Level 1 to 2 (manual self-entry, third-party signature via telephone) to Level 3 (cryptographically + GPS-secured). Each scan event in the eCoC system is quadruply secured through the ed25519 signature of the QR payload, the oidc-based authentication of the actor, the GPS coordinates, and the hash-chained audit entry. A courier can neither deny the execution nor the location of a scan without invalidating the entire subsequent hash chain.

In contrast, the non-repudiation of the paper-based procedure relies exclusively on handwritten signatures, which are easily forgeable and offer no cryptographic integrity proof. The transport protocols illustrate the vulnerability: timestamps and locations are entered by the courier themselves and are not independently verifiable. Moreover, in the haste of transport, one confirmation on the protocol remained unfilled – which is impossible with elec