



THE 21ST EDITION OF THE INTERNATIONAL CONFERENCE
**EUROPEAN INTEGRATION
REALITIES AND PERSPECTIVES**

Cognitive Migration Infrastructure Framework: Blockchain-Based Trust Architecture for the EU Eastern Border

Sergiu-Lucian Șorcaru¹, Alisa-Mihaela Ambrozie², Ionel Sergiu Pirju³, Camelia Aramă (Panfiloiu)⁴

Abstract: The February 2022 Russian military invasion of Ukraine triggered the arrival of over four million displaced persons into the European Union within a compressed timeframe. The identity verification architecture underpinning EU border management had no defined response. EES was not yet operational. ETIAS was inapplicable. The origin-state civil registry, on which both systems depend, was unavailable. Border officers processed millions of third-country nationals without a functioning verification chain, relying on ad hoc national procedures outside existing EU regulation. This article argues that the failure was not operational but architectural. Regulation (EU) 2019/817 builds EU border interoperability on the assumption that the origin state is always reachable. The article identifies this assumption as a Single Point of Failure and proposes the Cognitive Migration Infrastructure Framework (CMIF), a four-layer permissioned blockchain architecture that preserves verified identity continuity at the EU's eastern borders when origin-state authorities are absent. CMIF combines Self-Sovereign Identity credentials, a statutory anomaly filter with final decisions reserved to the human officer, a Delegated Trust Mechanism for absent-state scenarios, and a three-level degraded mode protocol with measurable operational parameters. A formal stress test based on the Ukraine 2022 crisis demonstrates where the current architecture fails and where CMIF remains operational.

Keywords: EU border management; Self-Sovereign Identity; Administrative Discontinuity; permissioned blockchain; EIBM resilience

JEL Classification: O33, F52, F22

1. Introduction

Under Regulation (EU) 2019/817 (European Parliament & Council, 2019), EU border management operates on one architectural assumption that a third-country national's identity can be validated in real time against origin-state civil registers or equivalent issuing authorities. This assumption held as a design

¹ Associate Professor, PhD, Faculty of Media, Design and Technology, Danubius International University, Romania, Address: 3 Galati Blvd., Galați, Romania, Corresponding author: sorcarusergiu@univ-danubius.ro.

² PhD Student, Bucharest University of Economic Studies, Romania, Address: 11 Tache Ionescu Street, Bucharest, Romania, E-mail: ambrozie.alisa@gmail.com.

³ Associate Professor, PhD, Faculty of Media, Design and Technology, Danubius International University, Romania, Address: 3 Galati Blvd., Galați, Romania, E-mail: pirjusergiu@univ-danubius.ro.

⁴ PhD Student, Doctoral School of Physical Education and Sport, Pitești University Center, National University of Science and Technology Politehnica Bucharest, Romania, Address: 7 Școlii Normale Alley, Pitești, Argeș, Romania, E-mail: cameliapanfiloiu@univ-danubius.ro.



parameter for EES and ETIAS under conditions of normal state functionality. It fails under conditions of Administrative Discontinuity, defined here as the sustained incapacity of a sovereign state to issue, authenticate, or transmit civil identity data to external verification systems.

Within 72 hours of Russia's February 2022 invasion, Ukrainian civil registration infrastructure in conflict-affected oblasts became operationally unavailable as an origin-state validation source. Over four million TCNs entered EU territory under the Temporary Protection Directive in the following weeks, a volume that exceeded EES processing capacity projections and for which ETIAS pre-travel authorization was, by design, inapplicable (Council of the European Union, 2022). The event exposed a structural gap that Regulation (EU) 2019/817 does not address: no EIBM mechanism exists for maintaining Trust Continuity, defined here as the verified and legally operative chain of identity assertion between a TCN and EU border systems, when the origin-state authority is unavailable for an indeterminate period.

The current architecture presents a Single Point of Failure at the Trust Anchor layer. EES records entries and exits but cannot verify identity in the absence of a readable travel document issued by a functioning state. ETIAS performs pre-screening but requires origin-state data consistency for hit validation. EES and ETIAS share a dependency that sits outside their own architecture: the origin-state civil registry has to be online and responsive. Conflict disrupts that registry, not the EU checkpoint systems themselves. The verification chain does not degrade at the border. It breaks before it gets there (Forti, 2024; Musco Musco Eklund, 2023; Coman, 2025). What fails is not an operational parameter, it is a design assumption.

Although the literature recognises the structural vulnerability of centralised identity verification systems, there is still no operational framework designed for situations in which the origin-state authority becomes unavailable for an extended period. Cybersecurity assessments of border control infrastructure document single-point-of-failure patterns and the exposure of centralised databases to hostile state actors (Chatzis & Stavrou, 2021). SSI frameworks based on W3C DID/VC specifications (World Wide Web Consortium, 2022) offer a credential portability model that decouples identity assertion from origin-state real-time availability, but no published framework has tested SSI under conditions of formal Administrative Discontinuity, nor integrated SSI with operational EIBM, degraded-mode border processing, and simultaneous GDPR/eIDAS 2.0 compliance (Forti, 2021; Matta & Bolli, 2022; Van Den Meerssche, 2022). This gap is the specific contribution of the present article.

This article proposes the Cognitive Migration Infrastructure Framework (CMIF), a four-layer permissioned blockchain architecture designed to maintain Trust Continuity at EU eastern border checkpoints under conditions of Administrative Discontinuity. CMIF is a proposed architectural framework, not an existing standard or deployed system. Its contribution is threefold: it operationalises SSI within EIBM constraints, introduces a Delegated Trust Mechanism for the absent-state scenario, and defines three measurable degradation levels for border processing under progressive connectivity loss.

The article proceeds as follows. Section 2 establishes the terminological boundaries of CMIF, Trust Continuity, and Administrative Discontinuity. Section 3 reviews the literature in a structured sequence from current Smart Borders functionality to the synthesis gap. Section 4 presents the CMIF architecture layer by layer. Section 5 applies a formal stress test using Ukraine 2022 parameters. Section 6 addresses governance implications and declared limitations. Section 7 synthesises the doctrinal contribution.

2. Terminological Boundaries

This section defines exactly three terms that carry distinct technical and legal weight throughout the article. Each term maps to a specific architectural condition that CMIF is designed to address.

Cognitive Migration Infrastructure Framework (CMIF) is a proposed four-layer permissioned blockchain architecture for identity verification at EU eastern border checkpoints. It is designed to maintain a legally operative identity assertion chain for TCNs when the origin-state authority is unavailable for an indeterminate period. CMIF integrates Self-Sovereign Identity credentials, an anomaly detection layer operating as a statutory filter, a selective disclosure mechanism compliant with GDPR and eIDAS 2.0, and a graduated degradation protocol with three measurable operational levels. CMIF is not an existing standard, a deployed system, or an extension of any current eu-LISA architecture. It is a proposed framework subject to formal validation.

Trust Continuity denotes the verified and legally operative chain of identity assertion between a TCN and EU border systems across all operational states, including degraded connectivity and origin-state unavailability. Trust Continuity is maintained when a border officer can complete a verification decision with a legally sufficient confidence level, even in the absence of a real-time response from the origin-state civil registry. It is disrupted when the verification chain depends exclusively on an upstream authority that is operationally unavailable. The distinction between Trust Continuity as a system property and mere connectivity is deliberate. A system can maintain connectivity while losing Trust Continuity if the connected origin-state server returns no valid attestation (Forti, 2021; Shafin & Reno, 2025).

Administrative Discontinuity is defined as the sustained incapacity of a sovereign state to issue, authenticate, or transmit civil identity data to external verification systems. It is distinguished from temporary technical outages by two criteria: duration exceeding the threshold at which degraded-mode processing becomes the operational norm rather than the exception, and causation attributable to structural factors such as armed conflict, occupation, or deliberate disruption of state infrastructure. Ukraine 2022 functions in this article as a formal instantiation of Administrative Discontinuity, not as a narrative case study. The condition is operationally relevant to EIBM because Regulation (EU) 2019/817 (European Parliament & Council, 2019) contains no provision for identity verification when the origin-state Trust Anchor is structurally absent rather than temporarily unavailable.

3. Literature Review

The Smart Borders architecture managed by eu-LISA works, under normal conditions, as a layered verification chain. EES records biometric entry and exit data for TCNs and detects overstays. ETIAS screens travellers against six interoperable databases before arrival. The Shared Biometric Matching Service cross-checks fingerprints and facial images across SIS, VIS, and Eurodac. The Multiple Identity Detector flags document fraud at the checkpoint (Coman, 2025). All four components presuppose the same thing: the origin-state civil registry is reachable and can authenticate the identity presented. When it is not, nothing in the architecture accounts for what happens next.

Csatlós (2025) traces how ETIAS shifts the issuance of travel authorisations to the direct administrative level, with Member State National Units stepping in only when the system registers a hit. What a hit triggers is a manual procedure with a 96-hour decision window, conducted under national law in the absence of common standards on security or illegal immigration risk (Csatlós, 2025). The human officer who reviews the hit does not have access to the algorithmic filtering that produced it. Musco Eklund

(2023) identifies this as a structural problem not a procedural one. The screening rules algorithm transfers normative power from legislative text to technical configuration. The actual content of the decision is determined by the specific risk indicators developed by Frontex and eu-LISA, not by law. Musco Eklund (2023) calls this algorithmic discretion. The officer at the end of the chain is reviewing a classification they did not produce, whose criteria they cannot inspect, and whose logic the ETIAS Regulation does not constrain with sufficient specificity.

Van Den Meerssche (2022) takes the analysis further. The distributive effects of risk scoring at the virtual border do not map onto existing non-discrimination categories. The inequalities produced are relational and correlational, generated by pattern detection rather than by explicit group-based classification. This makes them politically illegible and legally unreachable. The human-in-the-loop figure that EU strategy presents as an accountability safeguard is, in Van Den Meerssche's reading, a fiction. The loop closes on a classification that cannot be meaningfully reviewed by a person who cannot see into it. Forti (2024) documents the material consequence: data-driven border control errors harm migrants, refugees, and asylum seekers in ways that produce no legal remedy, because the opacity of the processing chain blocks both detection of the error and attribution of responsibility.

The structural vulnerability that underlies all of this is the centralisation of identity data. Chatzis and Stavrou (2021) map the cyberthreat landscape of border control infrastructure using expert interviews and ENISA risk methodology. They identify seven categories of threat actors. Nation-states appear among them because they have the resources and technical capability to target centralised identity repositories at scale. The attack surface spans physical, cyber, and human layers simultaneously. A centralised database is not simply a target. It is a single point whose failure propagates across every system that depends on it.

SSI addresses this at the design level. Under the W3C DID specification (World Wide Web Consortium, 2022), a decentralised identifier resolves to a document containing cryptographic material, and the controller proves identity by generating a proof against that material without querying any registry. Matta and Bolli (2022) confirm this architecture operates across permissioned blockchain networks through distributed identity registries. Selective attribute disclosure follows from this foundation: a TCN presents proof of nationality at a checkpoint without revealing biometric data, travel history, or any other personal attribute the verifying authority has no legal basis to request (Forti, 2021). On the compliance side, Akhison (2025) shows that storing biometric templates off-chain while anchoring only revocable cryptographic proofs on the ledger resolves the conflict between blockchain immutability and the right to erasure under Article 17 GDPR. The European Blockchain Services Infrastructure provides an active deployment context for W3C-compliant credentials within the EU regulatory perimeter (Matta & Bolli, 2022; Akhison, 2025). Blockchain applications in governance contexts beyond finance, including logistics and public administration frameworks, confirm the technology's adaptability to institutional compliance requirements across jurisdictions (Ambrozic & Şorcaru, 2022).

At the performance level, Shafin and Reno (2025) confirm that a permissioned Hyperledger Fabric architecture sustains 1,202 transactions per second with Byzantine fault tolerance, achieving 97.3% document verification accuracy and zero undetected forged document submissions across a 90-day pilot deployment at EU border checkpoints. The figures establish that permissioned blockchain is technically validated for EIBM, not merely theoretical.

Beduschi (2021) identifies the governance deficit that limits these advances. Digital identity tools in migration management are deployed without adequate international human rights law frameworks to govern errors and without mechanisms for structurally weaker states to participate in decisions that

affect their nationals. The deficit is compounded by a gap that none of the reviewed frameworks closes. No published study tests SSI under formal Administrative Discontinuity. No published framework integrates SSI with an operational EIBM processing flow that includes graduated degraded-mode operation. No published framework simultaneously addresses credential portability, EIBM constraints, offline processing thresholds, and GDPR/eIDAS 2.0 compliance when the origin-state Trust Anchor is structurally absent. Matta and Bolli (2022) and Shafin and Reno (2025) presuppose a functioning issuing authority. Forti (2021) and Van Den Meerssche (2022) address governance and rights but propose no technical architecture. The synthesis does not exist. This is the gap CMIF addresses.

4. CMIF Architecture

The CMIF architecture is presented in Figure 1. It comprises four layers, each addressing a distinct failure mode identified in the literature review. The layers do not operate in isolation: each one depends on the layer below it and constrains the layer above it. The architecture is read bottom-up at enrolment and top-down at verification.

Layer	Functional Role	Vulnerability Addressed	Technical Standard
Layer 4 Degraded Mode Protocol	Defines three sequential operational levels (Standard / Intermittent / Blackout) with measurable activation parameters and explicit capability sets per level	Absence of any defined EU-level degraded-mode protocol for TCN identity verification under Administrative Discontinuity	Internal CMIF protocol; Merkle proof caching; local DID public key cache
Layer 3 SSI & Selective Disclosure	Issues W3C DID/VC credentials at enrolment; verifies credential cryptographic proof at checkpoint without querying origin-state server; activates Delegated Trust Mechanism under confirmed Administrative Discontinuity	Dependency of EES/ETIAS on live origin-state registry availability; absence of legal Trust Anchor for EU candidate states under eIDAS 2.0	W3C DID Core v1.0; W3C VC Data Model v1.1; eIDAS 2.0 (Regulation EU 2024/1183); Hyperledger Aries/Indy
Layer 2 Anomaly Detection	Performs statistical anomaly detection on incoming verification requests; generates flags for human review; does not produce decisions or assign risk scores with legal consequences; final authority reserved exclusively to the border officer	Algorithmic discretion (Musco Eklund, 2023); de facto legal force of automated classifications without legislative constraint; absence of meaningful human oversight in current ETIAS architecture	EU AI Act Art. 14 (human oversight, high-risk systems); federated node deployment; anomaly flag output only

Layer 1 Permissioned Blockchain	Anchors identity hash of each enrolled TCN on a permissioned ledger; produces cryptographic non-repudiation verifiable without origin-state server; off-chain encrypted storage for all personal data; hash pointer links on-chain proof to off-chain record	Single Point of Failure in centralised identity repositories; nation-state capability to target centralised databases (Chatzis & Stavrou, 2021); GDPR Articles 5(1)(c) and 17 tension with on-chain personal data storage	Hyperledger Fabric v2.5+; PBFT consensus $N \geq 3f+1$; AES-256-GCM off-chain encryption; SHA-256 hash anchoring
Data flow: Bottom-up at enrolment (Layer 1 → Layer 4) Top-down at verification (Layer 4 → Layer 1) Layers operate interdependently			

Figure 1. CMIF Four-Layer Architecture: Functional Roles, Vulnerabilities Addressed, and Technical Standards

Layer 1. Permissioned Blockchain: Integrity Registry

Layer 1 anchors the identity hash of each enrolled TCN on a permissioned blockchain using a Proof-of-Authority consensus mechanism. A classical distributed database can be queried, but query results require a trusted third party to countersign them before they carry any evidentiary weight. A permissioned blockchain bypasses that dependency. The proof is anchored in the ledger itself, signed by the validator nodes at the moment of writing, and remains verifiable regardless of whether any upstream authority is reachable at the time of verification (Shafin & Reno, 2025). This is the specific property that justifies the design choice over a conventional database in the absent-state scenario.

The specific vulnerability this layer addresses is hostile state actor interference. As Chatzis and Stavrou (2021) establish, nation-states have both the capability and the documented intent to target centralised identity repositories. Layer 1 mitigates this through architectural separation. Cryptographic hashes go on-chain. Biometric templates, travel document details, and personal identifiers stay in off-chain encrypted storage, linked to the on-chain record through a hash pointer. The blockchain carries mathematical proof, not data. This design satisfies the GDPR data minimisation principle under Article 5(1)(c) and the right to erasure under Article 17 by making the on-chain element a non-personal cryptographic artefact (Akhison, 2025). The applicable technical standard is Hyperledger Fabric v2.5+, operating with PBFT consensus at $N \geq 3f + 1$ fault tolerance, consistent with the performance parameters validated by Shafin and Reno (2025) at EU border checkpoints.

Layer 2. Anomaly Detection: Statutory Filter

Layer 2 performs statistical anomaly detection on incoming verification requests. Its functional role is narrow and deliberately constrained: it flags requests that deviate from established behavioural patterns for escalation to human review. It does not produce decisions. It does not assign risk scores with legal consequences. It generates flags.

This distinction is not semantic. It is the architectural response to the problem identified by Musco Eklund (2023) and Van Den Meerssche (2022): when a system layer produces classifications that carry de facto legal force without being subject to legislative constraint, the result is algorithmic discretion. Layer 2 avoids this by design. Flagged or not, the verification decision belongs to the border officer. Layer 2 produces an input to that decision, not a replacement for it. The EU AI Act, for high-risk systems in border control contexts, requires exactly this: human oversight with final authority reserved to a natural person.

The layer itself avoids becoming a Single Point of Failure through federated deployment across multiple border checkpoint nodes. No single node holds the full anomaly detection model. Each node holds a local instance trained on anonymised cross-checkpoint data, and model updates are propagated through the same permissioned network as Layer 1. If a node fails, adjacent nodes absorb its verification load within the degradation parameters defined in Layer 4.

Layer 3. SSI and Selective Disclosure: Trust Continuity Layer

Layer 3 implements the Self-Sovereign Identity credential model based on W3C DID/VC specifications (World Wide Web Consortium, 2022). A TCN enrolled in CMIF holds a digital wallet containing Verifiable Credentials issued by an authorised state authority at the time of enrolment. At a border checkpoint, the TCN presents a cryptographic proof derived from those credentials. The proof is verified against the hash anchored in Layer 1. The origin-state server is not queried. Trust Continuity is maintained because the verification chain runs from the credential in the TCN's wallet to the blockchain record, not through a live connection to the issuing authority.

The tension between selective disclosure and Frontex reporting obligations is a genuine one. Frontex requires aggregated crossing data, risk indicators, and identity confirmation for operational and statistical purposes under Regulation (EU) 2019/1896. Selective disclosure, by design, limits what the verifying authority receives. The resolution proposed by CMIF is a Delegated Trust Mechanism at EU level: in the absent-state scenario, a designated EU-level Trust Anchor, operating under eu-LISA governance, issues a delegated attestation that binds the TCN's credential to a minimum legally sufficient identity assertion. This attestation carries the legal weight of the absent state's certification for the duration of the Administrative Discontinuity condition. The mechanism draws on the eIDAS 2.0 framework (European Union Digital Identity Architecture and Reference Framework, 2024), which provides the technical and legal basis for trust delegation across Member State boundaries. The applicable standards are W3C DID Core v1.0 and W3C Verifiable Credentials Data Model v1.1, with off-chain storage compliant with Hyperledger Aries/Indy best practices as documented by Akhison (2025).

Layer 4. Degraded Mode Protocol: Operational Resilience

Layer 4 is the most original technical contribution of this framework. It defines three operational levels that activate sequentially as connectivity to the CMIF network degrades. The levels are not descriptive states. They are protocol conditions with measurable activation parameters, defined capability sets, and explicit limitations. Figure 2 presents the three levels in structured form.

Level 1: Standard Operation. Network connectivity to the permissioned blockchain is full. Verification latency is below 800 milliseconds, consistent with the performance parameters of Shafin and Reno (2025). All four layers are active. The Delegated Trust Mechanism is available but not required. The border officer receives a full verification output including credential validity, anomaly flag status, and Frontex-reportable data packet.

Level 2: Intermittent Connectivity. Response latency above 3,000 milliseconds or packet loss above 15% over any 60-second window triggers a shift in Layer 1 from live blockchain query to a locally cached Merkle proof, valid for 72 hours from the last confirmed synchronisation. Layer 2 anomaly detection operates on the local node model without cross-checkpoint updates. Layer 3 credential verification proceeds from the TCN's wallet without blockchain confirmation, with the credential cryptographic signature serving as the primary trust anchor. The border officer receives a Level 2 verification output clearly marked as operating under reduced confirmation. The Delegated Trust Mechanism activates automatically when the absent-state condition is confirmed.

Level 3: Blackout. Network connectivity is fully unavailable. No blockchain query is possible. No cross-node communication is available. Layer 1 and Layer 2 are suspended. Layer 3 operates in standalone mode: the border officer verifies the TCN's credential cryptographic signature against the Trust Anchor public key of the issuing authority, permanently stored in the local cache of the border checkpoint system. Trust Anchor public keys are limited in number, stable over extended periods, and pre-installed at each node independently of network connectivity. The verification output is a binary result: credential signature valid or invalid. No anomaly detection, no Frontex data packet, no Delegated Trust Mechanism output. The border officer retains full and exclusive decision authority. All Level 3 verification events are logged locally and synchronised to the network immediately upon connectivity restoration. Level 3 is not a normal operating condition. It is a defined failure state with a documented decision protocol, not an architectural gap.

Criterion	Level 1 Standard Operation	Level 2 Intermittent Connectivity	Level 3 Blackout
Activation Parameter	Latency < 800 ms Packet loss: 0% Full network connectivity to CMIF permissioned blockchain	Latency > 3,000 ms OR packet loss > 15% over 60-second window Partial or intermittent blockchain connectivity	Full network unavailability No blockchain query possible No cross-node communication available
Active Layers	Layer 1. Full blockchain verification Layer 2. Anomaly detection (cross-checkpoint) Layer 3. SSI credential + blockchain confirmation Layer 4. Protocol active	Layer 1. Locally cached Merkle proof (72-hour validity window) Layer 2. Local node model only (no cross-checkpoint updates) Layer 3. SSI credential signature as primary trust anchor Layer 4. Protocol active	Layer 3 (standalone). Credential signature verified against Trust Anchor public key of issuing authority, permanently stored in local cache Layers 1, 2, 4: Suspended
Suspended Capabilities	None	Real-time blockchain query Cross-checkpoint anomaly model updates	Blockchain verification (Layer 1) Anomaly detection (Layer 2)

		Blockchain confirmation of credential	Delegated Trust Mechanism output Frontex data packet generation
Verification Output	Full output: credential validity + anomaly flag + Frontex-reportable data packet	Level 2 output (marked as reduced confirmation): credential validity + local anomaly flag + Delegated Trust Mechanism if absent-state condition confirmed	Binary output: credential signature valid / invalid No anomaly flag, no Frontex packet, no Delegated Trust output
Decision Authority	Border officer retains final authority in all cases	Border officer retains final authority in all cases	Border officer retains full and exclusive decision authority
Data Synchronisation	Continuous real-time sync	Merkle proof cache refreshed at each successful connection window	All Level 3 events logged locally; synchronised to network immediately upon connectivity restoration

Figure 2. CMIF Degraded Mode Protocol: Activation Parameters, Layer Status, and Decision Authority Across Three Operational Levels

5. Ukraine 2022: Stress Test Parameters and Comparative Assessment

Russia's invasion on 24 February 2022 at 05:00 CET took Ukrainian civil registration infrastructure in conflict-affected oblasts offline as a validation source. This article uses that event as a parameter set, not a narrative. It remained unavailable for over 30 days. Within that period, approximately 4.1 million TCNs entered EU territory under the Temporary Protection Directive (Council of the European Union, 2022). ETIAS was not yet deployed. EES operational status: delayed, scheduled implementation not completed. SIS operational status: functional, but dependent on Member State data entry, not origin-state registry query. Existing EIBM response to absent-state Trust Anchor: none defined under Regulation (EU) 2019/817 (European Parliament & Council, 2019).

These parameters establish a scenario in which the current architecture had no defined degraded-mode response. Border officers processed four million TCNs over thirty days without a functioning identity verification chain on the origin side. The operational consequence was not a system failure in the technical sense. It was a sustained condition of unresolved Trust Continuity, handled through ad hoc national procedures in the absence of any EU-level framework.

Table 1 presents a structured comparison of current EIBM performance against projected CMIF performance across five criteria under the Ukraine 2022 parameters.

Table 1. Comparative Assessment: Current EIBM versus CMIF under Administrative Discontinuity Conditions

Criterion	Current EIBM	CMIF
Verification speed under normal conditions	Sub-second with functional origin-state registry	Sub-800ms, consistent with Shafin & Reno (2025) Level 1 parameters
Offline capability	None. Verification chain collapses when origin-state registry is unavailable	Level 2: 72-hour Merkle proof cache. Level 3: standalone cryptographic signature verification
False identity resistance	Dependent on INTERPOL SLTD database and origin-state document authenticity	Cryptographic non-repudiation anchored in permissioned blockchain; hash mismatch detected at Layer 1 regardless of origin-state availability
Trust level without origin server	Zero. No defined mechanism. Ad hoc national procedures applied	Delegated Trust Mechanism at EU level activates under confirmed Administrative Discontinuity; credential cryptographic signature serves as primary trust anchor
GDPR compliance under crisis conditions	No specific provision. Temporary Protection Directive applied without data minimisation protocol	Off-chain storage architecture maintains GDPR compliance at all three degradation levels; on-chain record contains no personal data

The scenario has limits that must be stated explicitly. CMIF's Level 2 and Level 3 operations have not been tested in a live deployment. The 72-hour Merkle proof cache validity window is a design parameter derived from the performance benchmarks of Shafin and Reno (2025) and the operational requirements of EIBM, not from empirical testing under Administrative Discontinuity conditions. The Delegated Trust Mechanism at EU level presupposes a governance decision by eu-LISA and the relevant Council working group to designate a Trust Anchor for the absent-state scenario. That decision does not currently exist. CMIF would fail under two conditions that the stress test does not resolve: first, if enrolment of the affected TCN population had not occurred prior to the onset of Administrative Discontinuity, because no CMIF credential exists to verify; second, if the permissioned blockchain network itself were compromised by the same hostile actor responsible for the Administrative Discontinuity, a scenario that Byzantine fault tolerance mitigates but does not eliminate at f values exceeding $\lfloor (N-1)/3 \rfloor$ (Shafin & Reno, 2025). Both conditions represent open research problems that CMIF does not claim to solve.

6. Governance and Limitations

CMIF operates at the intersection of two threat vectors that EU border management policy has not yet addressed jointly: Administrative Discontinuity as a technical failure condition, and fabricated identity as a hybrid threat instrument. The production of synthetic identities through deepfake documents and compromised civil registries is documented as a component of hybrid warfare directed at EU Member States (Chatzis & Stavrou, 2021). When a state-level actor deliberately disrupts the origin-state registry while simultaneously injecting fabricated identity records into the verification chain, the attack exploits precisely the gap that current EIBM architecture leaves open. CMIF's Layer 1 non-repudiation design addresses this vector directly: a fabricated identity that was not enrolled in the permissioned blockchain prior to the onset of Administrative Discontinuity produces no valid hash, and a hash that was not present at enrolment cannot be retroactively inserted without Byzantine consensus among the network's validator nodes. This is not a complete defence against hybrid identity threats, but it removes the specific vulnerability that the absent-state scenario creates.

The eIDAS 2.0 and GDPR tension in the absent-state scenario is the most significant legal problem CMIF raises. Under eIDAS 2.0, a Trust Anchor must be a recognised legal entity within an EU Member State or an entity operating under a trust framework recognised by the Commission (European Union, 2024). When the origin state is Ukraine, currently an EU candidate state but not a Member State, the Delegated Trust Mechanism proposed in Layer 3 has no direct legal basis in the current eIDAS 2.0 framework. The resolution CMIF proposes is the designation by the Council of a temporary EU-level Trust Anchor under an emergency governance instrument, analogous in structure to the Council Implementing Decision that activated the Temporary Protection Directive in March 2022 (Council of the European Union, 2022). This is a doctrinal proposal, not an existing legal mechanism. It requires a Council decision, a eu-LISA technical implementation mandate, and a GDPR-compliant data processing agreement specifying the conditions under which the delegated attestation is issued, retained, and revoked.

The declared limitations of CMIF are four. First, the framework has no empirical validation. The degradation level parameters in Layer 4 are derived from technical benchmarks and operational requirements, not from a live deployment under Administrative Discontinuity conditions. Second, CMIF presupposes prior enrolment of the TCN population. A TCN who was never enrolled in the system holds no credential that CMIF can verify, which means the framework does not resolve the identification problem for populations displaced before any enrolment infrastructure was established. Third, the Delegated Trust Mechanism requires a governance decision that does not currently exist and whose political feasibility depends on factors outside the scope of this framework. Fourth, CMIF does not address the re-enrolment problem: if a TCN's credential was issued by a state authority that has since fabricated or modified records under occupation, the credential may be cryptographically valid but factually incorrect. Layer 1 guarantees the integrity of what was enrolled, not the truth of it.

The concrete validation pathway for CMIF consists of three steps. A formalised tabletop exercise conducted by eu-LISA and at least two Member State border agencies, using synthetic data and simulated Administrative Discontinuity parameters derived from the Ukraine 2022 event. A synthetic data simulation of Layer 4 degradation levels, specifically testing the 72-hour Merkle proof cache validity under high-volume processing conditions comparable to the March 2022 crossing rates. A pilot under an EU innovation programme, potentially under the Horizon Europe Digital Security and Trust cluster, using a controlled deployment at a single eastern border checkpoint with a defined TCN enrolment cohort. The institutional capacity of EU candidate states to participate in such pilot programmes varies significantly and conditions the feasibility of any enrolment infrastructure built on their civil registration systems (Şorcaru et al., 2023). None of these steps constitutes deployment. Each one generates the empirical data that CMIF currently lacks and that any formal validation by eu-LISA would require before integration into the EIBM architecture could be considered.

7. Conclusion

The structural vulnerability that CMIF addresses is not a gap in border security policy. It is a gap in identity architecture. Regulation (EU) 2019/817 (European Parliament & Council, 2019) builds the interoperability of EU border management on an assumption of origin-state availability that the Ukraine 2022 event demonstrated cannot be treated as a permanent condition. When the origin-state civil registry is unavailable, the current architecture has no defined response. Trust Continuity collapses, and border officers process millions of TCNs through ad hoc national procedures that Regulation (EU) 2019/817 neither anticipated nor governs.

CMIF proposes a technically grounded and legally bounded response to this condition. Layer 1 anchors identity hashes in a permissioned blockchain that produces cryptographic non-repudiation without requiring the origin-state server to be online. Layer 2 positions anomaly detection as a statutory filter with final authority reserved exclusively to the human officer, consistent with the AI Act requirements for high-risk border control systems and with the accountability critique developed by Musco Eklund (2023) and Van Den Meerssche (2022). Layer 3 implements W3C DID/VC credentials with selective disclosure, resolves the GDPR compliance problem through off-chain storage, and introduces the Delegated Trust Mechanism as the legal instrument for the absent-state scenario under eIDAS 2.0. Layer 4 defines three degradation levels with measurable activation parameters, converting an architectural gap into a managed operational protocol.

CMIF does not replace EES, ETIAS, or any component of the existing Smart Borders architecture. It operates as a complement to it, activating where the current architecture's upstream dependency fails. The distinction matters because CMIF is not a proposal to redesign EU border management. It is a proposal to make the existing architecture resilient to a condition that the literature has identified but that no published framework has technically addressed.

The contribution of this article is a repositioning of identity resilience within the EU security architecture. Identity verification at the eastern border is not merely an administrative function. Under conditions of Administrative Discontinuity induced by hybrid warfare, it is a national security instrument. Fabricated identities injected during a period of origin-state registry disruption represent a threat vector that exploits the same gap CMIF is designed to close. The EU's Digital Strategic Autonomy cannot be limited to data governance and platform regulation. It must extend to the identity verification infrastructure on which border security depends, and that infrastructure must be designed to function when the conditions that it was built to assume no longer hold.

References

- Akhison, G. (2025). Towards a universal digital identity: A blockchain-based framework for borderless verification. *Frontiers in Blockchain*, 8, 1688287. <https://doi.org/10.3389/fbloc.2025.1688287>
- Ambrozie, A. M., & Şorcaru, S. L. (2022). Logistics in a green era, a blockchain-based framework. *Acta Universitatis Danubius. Œconomica*, 18(6).
- Beduschi, A. (2021). International migration management in the age of artificial intelligence. *Migration Studies*, 9(3), 576–596. <https://doi.org/10.1093/migration/mnaa003>
- Chatzis, P., & Stavrou, E. (2021). *Cyber-threat landscape of border control infrastructures*. Applied Cyber Security Research Laboratory, University of Central Lancashire Cyprus.
- Coman, I. (2025). Large-scale integration of technical systems in cross-border police cooperation management. In H. Takemura & S. O. Michael (Eds.), *Public law at the crossroads of technology, jurisprudence and governance in contemporary Europe*, 198–208. *ADJURIS*. <https://doi.org/10.62768/ADJURIS/2025/4/13>
- Council of the European Union. (2022). *Council implementing decision (EU) 2022/382 of 4 March 2022 establishing the existence of a mass influx of displaced persons from Ukraine*. *Official Journal of the European Union*, L 71.
- Csatlós, E. (2025). Blending digitalization and enhanced security: Exploring the role of ETIAS in migration control and its administrative structure. *Hungarian Journal of Legal Studies*, 65(3), 323–346. <https://doi.org/10.1556/2052.2024.00508>
- European Parliament and Council of the European Union. (2019). *Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa*. *Official Journal of the European Union*, L 135. <https://eur-lex.europa.eu/eli/reg/2019/817/oj>

European Parliament and Council of the European Union. (2019). *Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard*. Official Journal of the European Union, L 295. <https://eur-lex.europa.eu/eli/reg/2019/1896/oj>

European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>

European Parliament and Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

European Union. (2024). *European Digital Identity Wallet Architecture and Reference Framework (v2.8.0)*. <https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/>

Forti, M. (2021). *Blockchain-driven identification procedures in the migration context: Regulatory challenges and fundamental rights issues*. SSRN. <https://ssrn.com/abstract=3866594>

Forti, M. (2024). Addressing algorithmic errors in data-driven border control procedures. *German Law Journal*, 25, 635–645. <https://doi.org/10.1017/glj.2023.102>

Matta, S. S., & Bolli, M. (2022). Blockchain-based decentralized identity for cross-border authentication: Enhancing cybersecurity and immigration applications. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 2(1), 63–88. <https://doi.org/10.63125/sr1rz960>

Musco Eklund, A. (2023). Rule of law challenges of “algorithmic discretion” and automation in EU border control: A case study of ETIAS through the lens of legality. *European Journal of Migration and Law*, 25(3), 249–274. <https://doi.org/10.1163/15718166-12340152>

Shafin, K. M., & Reno, S. (2025). A byzantine-resistant blockchain framework for secure and scalable immigration management. *Scientific Reports*, 15, 32338. <https://doi.org/10.1038/s41598-025-10235-3>

Șorcaru, S. L., Nuță, F. M., Topliceanu, S. C., & Ambrozie, A. M. (2023). Measuring the FDI attractiveness in the EAP countries from an institutional perspective. *Journal of business economics and management*, 24(6), 1019-1041.

Van Den Meerssche, D. (2022). Virtual borders: International law and the elusive inequalities of algorithmic association. *European Journal of International Law*, 33(1), 171–204. <https://doi.org/10.1093/ejil/chac007>

Velasco Rico, C. I., & Laukyte, M. (2024). ETIAS system and new proposals to advance the use of AI in public services. *Computer Law & Security Review*, 54, 106015. <https://doi.org/10.1016/j.clsr.2024.106015>

World Wide Web Consortium. (2022). *Decentralized identifiers (DIDs) v1.0*. W3C Recommendation. <https://www.w3.org/TR/did-1.0/>