

Tax Evasion in Integrated Fiscal and Electronic Payment Systems: Vulnerabilities, Detection, and Mitigation in the Greek Digital Tax Ecosystem

Panagiotis Mavridis

Hellenic Mediterranean University

Anargyros T. Baklezos

Hellenic Mediterranean University

Nikolas Kapsalis

National Technical University of Athens

Christos D. Nikolopoulos

`cnikolo@hmu.gr`

Hellenic Mediterranean University

Research Article

Keywords: Fiscal Electronic Mechanisms, EFTPOS, eSEND, myDATA, electronic invoicing, tax evasion, hash chain, cryptographic protocol, ERP, EIPS, anomaly detection, VAT

Posted Date: October 15th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11353583/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Tax Evasion in Integrated Fiscal and Electronic Payment Systems: Vulnerabilities, Detection, and Mitigation in the Greek Digital Tax Ecosystem

Panagiotis Mavridis¹, Anargyros T. Baklezos^{1,2},
Nikolas Kapsalis², Christos D. Nikolopoulos^{1,2*}

¹Department of Electronic Engineering, School of Engineering, Hellenic Mediterranean University, Chania, Greece.

²School of Electrical and Computer Engineering, National Technical University of Athens, Athens, Greece.

*Corresponding author(s). E-mail(s): cnikolo@hmu.gr;

Abstract

Greece has developed a highly digitized fiscal ecosystem combining Fiscal Electronic Mechanisms (FEMs), Electronic Funds Transfer at Point-of-Sale (EFTPOS) terminals, the central FEM information system eSEND, the myDATA reporting platform, Enterprise Resource Planning (ERP) systems, and Electronic Invoicing Provider Services (EIPS). This paper provides an integrated technical analysis of this ecosystem, extending previous work on hash-chain and blockchain-like integrity mechanisms in Greek fiscal devices. First, the hardware and cryptographic architecture of Fiscal Electronic Cash Registers, Fiscal Printers, Fiscal Signing Machines (EAFDSS), and Fiscal Electronic Mechanisms of Accumulation and Signing (FEMAS) is examined, including fiscal memory, progressive counters, SHA-1 hash chains, Z-report chaining, and encrypted transmission to eSEND. Second, the unified FEM–EFTPOS protocol defined by A.1098/2022 and amended by A.1088/2023 and A.1027/2024 is analyzed at message-flow level, including master/session keys, AMOUNT, RESULT, REGRECEIPT, RESEND-ALL, and the e.txt records 355, 356, and 358. Third, the intermediary FEM–ERP–EFTPOS and EIPS–ERP–EFTPOS models permitted by A.1155/2023 are evaluated. The analysis identifies a structural tax-evasion vector in which an intermediary may prevent successful card-payment information from reaching the FEM or central tax systems, while the lack of mandatory locked-keypad behavior and a fully specified secure ERP–EFTPOS protocol weakens end-to-end binding between payment and fiscal receipt. A layered remediation is proposed, combining regulatory unification, authenticated

encryption, cryptographically bound tokens, signed EFTPOS results, hardware-backed keys, immutable telemetry, and AI/ML-based reconciliation of acquirer and fiscal records.

Keywords: Fiscal Electronic Mechanisms, EFTPOS, eSEND, myDATA, electronic invoicing, tax evasion, hash chain, cryptographic protocol, ERP, EIPS, anomaly detection, VAT

1 Introduction

Digital tax administration increasingly relies on continuous transaction controls, electronic invoicing, fiscal devices, and near-real-time reporting. These mechanisms aim to reduce the information gap between taxable economic activity and the data available to tax authorities. Greece is a particularly relevant case because its architecture combines certified hardware fiscal mechanisms, payment terminals, centralized reporting infrastructures, and software-based electronic invoicing services.

A blockchain is a sequence of records linked by cryptographic hashes such that modification of an earlier record changes the hash relation of subsequent records [1, 2]. Blockchain and hash-chain concepts have consequently been investigated for VAT settlement, tax information exchange, invoice authentication, and prevention of missing-trader fraud [3–9]. The essential property for fiscal applications is not necessarily a public distributed ledger; rather, it is the ability to provide tamper-evident sequencing, completeness, and auditability of transaction records.

Greek Fiscal Electronic Mechanisms (FEMs) implement these principles using protected hardware, fiscal memory, sequential document counters, receipt-level hashes, daily Z-report hash chains, and encrypted transfer to the central eSEND system. The earlier conference version of this work focused on these blockchain-enabled integrity mechanisms and contrasted them with the less strongly chained myDATA/EIPS model [27]. The present paper substantially extends that analysis in four directions. First, it incorporates the detailed FEM–EFTPOS payment protocol and its key-establishment procedure. Second, it analyzes direct and ERP-mediated transaction flows for immediate receipts, deferred/preloaded receipts, and card prepayments. Third, it formalizes the tax-evasion vectors introduced when the ERP/EIPS intermediary can drop, delay, or suppress payment-result messages. Fourth, it proposes technical, regulatory, and analytics-based countermeasures.

Tax-fraud detection is also increasingly data-driven. To this end, several technological and scientific solutions have been proposed in the bibliography, ranging from big-data analysis, graph mining and neural networks, to visual analytics and synthetic-data generation. All these solutions have been proposed to identify and analyze suspicious taxpayer behaviour and to identify potential suspicious transactions [28–35]. These approaches can be seen as complementary to device-level controls: although cryptographic mechanisms either prevent or expose possible in-situ manipulations, data analytics can identify inconsistencies at scale.

Thus, the scientific contribution of this work goes beyond a mere description of the Greek regulatory framework. It accomplishes this by using the Greek ecosystem as an indicative case study to examine how a digital tax architecture can preserve the integrity and completeness of the fiscal record, even in cases when payment, receipt issuance, ERP processing, and central reporting are decentralized and spread throughout various components. The principal contributions of the present work are: (i) a system-level decomposition of the Greek fiscal-payment ecosystem; (ii) a transaction-flow analysis of the unified and intermediary protocols; (iii) a structured threat model identifying specification, trust, binding, completeness, and operational gaps; (iv) a comparative security assessment of the principal architectures; and (v) a layered mitigation framework combining regulatory, cryptographic, device-level, and data-analytics controls.

The remainder of the paper proceeds from the research methodology and technological background to the Greek fiscal infrastructure, transaction-flow analysis, threat model, economic/public-finance evaluation, quantitative sensitivity analysis, mitigation framework, implementation roadmap, policy discussion, and conclusions.

2 Research Methodology and Assessment Framework

This work adopts a qualitative technical-regulatory case-study methodology. The unit of analysis is an electronic payment transaction that should be associated with a valid fiscal document and subsequently become visible to the competent tax authority. The analysis follows that transaction across four logical layers: (1) fiscal-document generation, (2) payment authorization, (3) intermediary ERP/EIPS processing where applicable, and (4) central reporting to eSEND or myDATA. The regulatory and protocol descriptions are mapped to these layers and compared according to whether they provide an enforceable end-to-end relationship between the payment event and the fiscal record.

The assessment uses six security and compliance properties. *Endpoint trust* considers whether the security-critical endpoints are certified or otherwise controlled. *Protocol standardization* considers whether commands, fields, states, and error handling are prescribed. *Payment–receipt binding* considers whether a successful authorization is cryptographically or procedurally linked to a specific fiscal record. *Completeness* considers whether omission of a successful transaction is detectable by the central authority. *Replay and integrity protection* considers whether message alteration or reuse can be detected. Finally, *central auditability* considers whether independent records exist that permit reconciliation among fiscal, payment, and acquiring systems.

The study combines architectural analysis with a public-finance evaluation framework. The present data support identification of feasible failure paths and construction of auditable fiscal-risk measures, but they do not support a causal estimate of the prevalence of tax evasion or of the revenue effect of a particular regulation. Accordingly, the quantitative results reported below are explicitly calibrated sensitivity scenarios rather than observed treatment effects. A separate econometric design is specified for future administrative microdata so that architectural feasibility, measured incidence, and causal policy impact are not conflated.

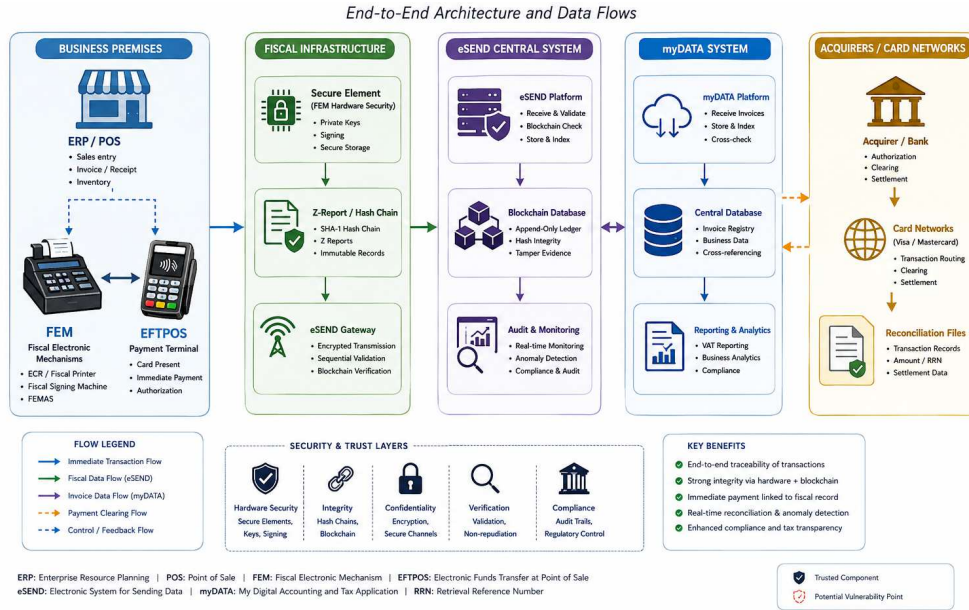


Fig. 1 System-level decomposition of the Greek fiscal–payment ecosystem used in the assessment. The upper layer shows the certified fiscal, intermediary software, and payment endpoints; the lower layer shows central reporting and independent audit evidence.

3 Technological Background for Digital Tax-Evasion Control

3.1 Tamper-Evident Fiscal Logging

A fiscal logging system should provide at least four properties: authenticity of the reporting device, integrity of individual records, completeness of the transaction sequence, and non-repudiable association between a payment and the corresponding fiscal document. In this sense, hash chaining can be effective, since any modification of earlier records results in detectable inconsistencies in later ones.

3.2 AI/ML for Fraud and Anomaly Detection

Due to the ever-increasing amounts of fiscal and payment data, modern tax administrations can employ them to identify anomalous or potentially suspicious behavior. Network-based approaches can reveal suspicious taxpayer groups at large, while graph-based and unlabeled learning techniques can be employed to detect patterns largely unlabeled data [29, 30, 34]. Relevant features that can be employed in the Greek fiscal environment include daily totals, card-to-cash payment ratio, unmatched payment identifiers, token lifetimes, upload latency, repeated failed sessions, and discrepancies between acquirer data and eSEND/myDATA records.

3.3 Communication and POS Security

To ensure that all payments are secure requires an overall secure architecture. Such kinds of architecture must provide multiple security components, such as endpoint authentication, protected key provisioning, replay resistance, integrity of command parameters, trusted device state, and end-to-end binding between the amount authorized by the cardholder and the fiscal document reported to the tax authority. Furthermore, the potential attack surface increases in cases when general-purpose ERPs are inserted between two certified endpoints.

3.4 Centralized Clearance and Permissioned-Ledger Concepts

Centralized systems and ledgers provide an alternative model to device-local chaining, since they enable tax authorities to validate transactions shortly after completion, or even before transactions take place. Blockchain architectures are in general not necessary for sensitive tax data, since an architecture can be developed to provide controlled access, auditability, and governance without disclosing confidential taxpayer information [5, 6].

4 Greek Digital Fiscal Infrastructure: Fiscal Electronic Mechanisms

Greek FEMs are governed by technical specifications including POL 1220/2012 and subsequent amendments [13, 15]. Relevant approval procedures include a series of software and technical checks. Furthermore, fiscal devices operate inside sealed enclosures accessible only to authorized technicians. The principal FEM categories in the Greek Legislation include Fiscal Electronic Cash Registers (ECRs), Fiscal Printers, Fiscal Signing Machines (EAFDSS), and Fiscal Electronic Mechanisms of Accumulation and Signing (FEMAS).

4.1 Fiscal Memory and Working Memory

Fiscal memory, which is an essential part of all fiscal devices typically comprises of an EPROM or microprocessor-controlled nonvolatile memory, thus permitting new entries while, at the same time, preventing deletion or modification of past records. It is physically protected, commonly by encapsulation in resin. The working memory contains counters and accumulators for net values and VAT amounts by category. At the end of a fiscal day, the accumulated values are transferred to a new fiscal-memory entry through the Z report.

Each sales document is also stored on an SD card or associated storage. The original receipt text is recorded in an `a.txt` file. A SHA-1 digest is stored in a corresponding `b.txt` file, and fiscal fields are stored in an `e.txt` record. Although SHA-1 is now cryptographically obsolete for new security designs, its use here is part of the legacy regulatory specification and should be distinguished from the proposed modernization in Section XI.

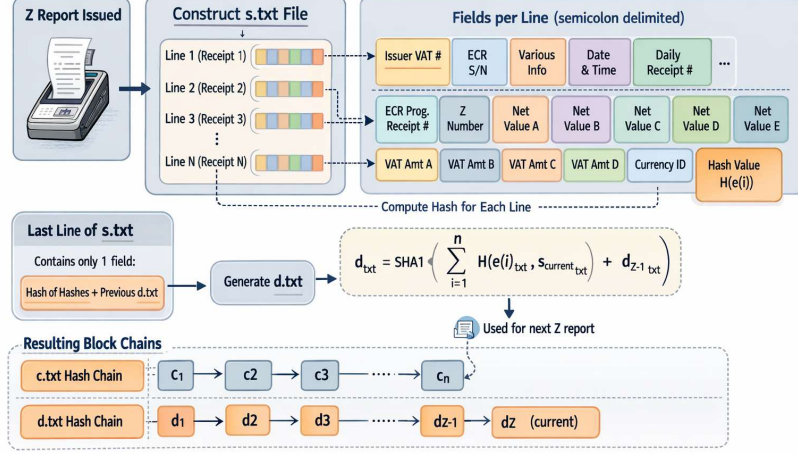


Fig. 2 Representation of the FEM receipt and Z-report hash-chain structure. Receipt digests are aggregated with the previous Z-chain value to create the current tamper-evident chain value.

4.2 Z Reports and Hash-Chain Construction

When the Z report is issued, the FEM computes a daily chain value from all receipt hashes of the current Z and the previous Z-chain value:

$$c_Z = \text{SHA1}(b_1 \| b_2 \| \dots \| b_n \| c_{Z-1}), \quad (1)$$

where b_i denotes the receipt-level digest and c_{Z-1} the previous daily chain value. Consequently, omission or modification of a previously incorporated receipt affects subsequent chain verification.

At receipt level, the stored digest can be represented as

$$b_i = \text{SHA1}(D_i), \quad (2)$$

where D_i denotes the canonicalized receipt payload. The daily chaining rule therefore acts as a second integrity layer on top of individual receipt digests.

A second chain is created for fiscal-field records in systems supporting `s.txt/d.txt`. In abstract form,

$$d_Z = \text{SHA1}(h(e_1) \| \dots \| h(e_n) \| d_{Z-1}). \quad (3)$$

Progressive net-value and VAT totals stored in fiscal memory form an additional sequential accounting chain. Depending on FEM type, these mechanisms result in double or triple integrity structures.

4.3 ECRs, Fiscal Printers, EAFDSS and FEMAS

Fiscal ECRs combine protected fiscal memory, working-memory accumulators, receipt storage, and Z-report chaining. Fiscal Printers provide similar fiscal functionality but

Table 1 Representative Fiscal and Payment Fields Reported by FEMs

Category	Representative fields
Identity	Issuer VAT number, recipient VAT number, FEM serial number
Sequence	Daily document number, progressive document number, Z number, series, document number
Fiscal values	Net amounts by VAT category, VAT amounts, grand total, currency
Card payment	Number of card payments, total card payments, session/acquirer/terminal/RRN/date-time/final amount/status identifiers
Interoperability	myDATA information and additional information fields
Integrity	Receipt hash and Z-related chaining/integrity fields

receive sales commands from an attached computer rather than a keyboard. EAFDSS devices focus on signing and fiscal data files and implement the `c.txt` and `d.txt` chains. FEMAS combines ECR-like accumulation with EAFDSS-like signing and therefore integrates protected storage, fiscal accumulators, and multiple hash-chain mechanisms in one device.

5 Central Reporting and Data Integrity: eSEND

The FEM Central Information System eSEND is the central destination for transaction data transmitted by FEMs. If connectivity is unavailable at Z-report time, the FEM retains the unsent data and transmits it when communication is restored, preventing a temporary network failure from creating an accepted gap in the fiscal sequence [21].

5.1 Encrypted Back-End Transmission

FEM sales data are encrypted for transmission. The original conference analysis describes AES-256 encryption with a device-specific key for FEM-to-eSEND packages. At the receiving side, eSEND identifies the FEM, decrypts the package, verifies sequencing, and checks the hash-chain relation before accepting the Z data.

If the last accepted report is denoted as $Z = k$, the next valid report is $Z = k + 1$. If this sequence or the prescribed hash-chain rules are violated, the next report cannot be accepted. This provides two distinct completeness checks: sequential Z numbering and cryptographic linkage.

5.2 Fiscal Record Schema

The detailed fiscal records transmitted to eSEND include the issuer and recipient VAT numbers, FEM serial number, date/time, daily and progressive document numbers, Z number, document type and series, net values, VAT amounts, grand total, currency, card-payment count and total, card-payment identification, myDATA-related information, and integrity fields. The combination of FEM serial number and progressive document number provides a strong device-local identifier for a sales document.

6 Software-Based Fiscal Reporting: EIPS and myDATA

Electronic Invoicing Provider Services (EIPS) have been permitted as an alternative channel for issuing invoices and retail receipts under A.1035/2020 and subsequent amendments, including A.1158/2023 and A.1112/2025 [23, 24, 26]. The issuer sends the document to the provider, which authenticates/processes it and transmits it to myDATA and, where applicable, to the recipient or the recipient’s provider.

Unlike a certified FEM, the issuer side may be a general-purpose computer without protected fiscal memory. Under permitted offline operation, documents may be generated locally and transmitted later. The conference study emphasized that the EIPS/myDATA path does not impose the same device-level progressive numbering and Z-report hash-chain verification as the FEM/eSEND path [27]. myDATA returns a unique MARK identifier for accepted documents, but MARK values are not a consecutive per-business sequence from which an auditor can directly infer that no intermediate sales document is missing.

This concept is key: Although transport security - such as the HTTPS protocol - can protect data in transit, it cannot be used to ensure that all transactions generated before transmission were preserved. Completeness requires a trusted sequence, protected local storage, authoritative reconciliation, or an equivalent cryptographic mechanism.

7 Unified FEM–EFTPOS Protocol Architecture

The unified protocol defined by A.1098/2022 and amended by A.1088/2023 and A.1027/2024 was introduced to ensure that card payments are coupled to fiscal records [18–20]. In the direct architecture, the EFTPOS keypad is locked for amount entry and the transaction amount is supplied by the FEM. Thus, the payment terminal is not intended to operate as an independent source of arbitrary payment amounts during the coupled workflow.

Before payment, the FEM transmits data including the session number, FEM identifier, and amount. After payment, the EFTPOS returns transaction information including the session number, acquirer identifier, terminal identifier, retrieval reference number (RRN), date/time, final amount, and transaction status. The FEM incorporates card-payment totals into its accumulators and reports detailed payment information to eSEND.

7.1 Master Key and Session Key Establishment

Under A.1088/2023, both FEM and EFTPOS receive a common master key from eSEND. The FEM then constructs a session key, protects it using the master key, and sends it to the EFTPOS. After decryption, both endpoints share the session key used for protected protocol exchanges. The legacy specification uses DES in parts of the FEM–EFTPOS key/message protection process; Section XI proposes migration to modern authenticated encryption.

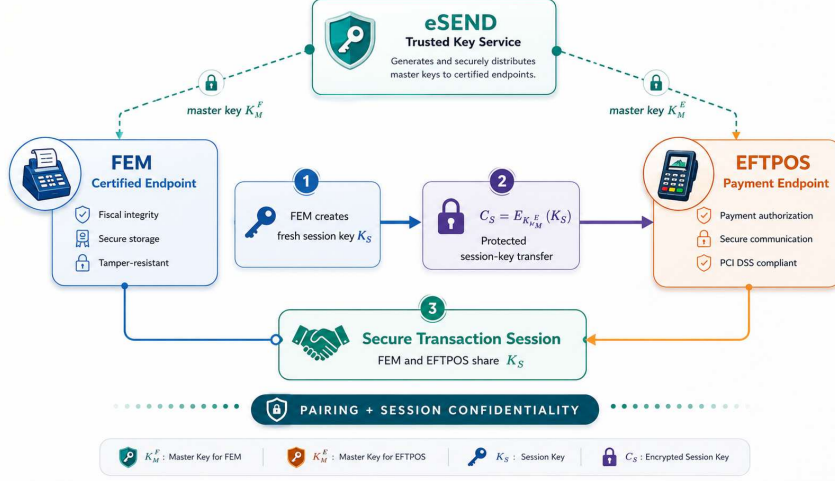


Fig. 3 FEM–EFTPOS key-establishment process under the unified protocol. eSEND distributes the master key to both endpoints and the FEM establishes a fresh protected session key for transaction communication.

The key establishment can be abstracted as

$$K_M \leftarrow \text{eSEND}(\text{FEM}, \text{EFTPOS}), \quad (4)$$

$$K_S \xleftarrow{\$} \{0, 1\}^\kappa, \quad (5)$$

$$C_S = E_{K_M}(K_S), \quad (6)$$

$$\text{FEM} \rightarrow \text{EFTPOS} : C_S, \quad (7)$$

where K_M is the centrally provisioned master key, K_S is a fresh session key, and $E_{K_M}(\cdot)$ denotes the legacy protection function defined by the protocol.

7.2 Direct and ERP-Initiated Direct Schemes

The unified protocol supports two conceptually secure arrangements:

1. **FEM–EFTPOS**: direct communication between the certified fiscal mechanism and certified payment terminal.
2. **ERP–FEM–EFTPOS**: the ERP instructs the FEM to create the fiscal transaction, but the FEM itself communicates with the EFTPOS using the unified protocol.

In both cases, the security-critical payment/fiscal coupling remains between the FEM and EFTPOS.

8 Transaction-Flow Analysis

8.1 Preloaded Fiscal Receipt for Later Payment

For a receipt issued before the actual card payment, the FEM can preload the receipt into the EFTPOS using **REGRECEIPT**. At end of day, **RESEND-ALL** is used to request the results associated with preloaded receipts. The FEM then creates record code 356 and transmits the corresponding information to eSEND.

A compact representation of the flow is

$$\text{FEM} \rightarrow \text{EFTPOS} : \text{REGRECEIPT}(S, A, C, D, R, H, T, M, Q), \quad (8)$$

$$\text{FEM} \rightarrow \text{EFTPOS} : \text{RESEND-ALL}(R, D, Q), \quad (9)$$

$$\text{EFTPOS} \rightarrow \text{FEM} : \text{RESULT}(S, R, T, M, C, D, P), \quad (10)$$

where the symbols compactly denote the session, amount/currency, date-time, ECR/FEM identifier, operator, receipt number, custom data, MAC, response code, transaction data, and printable data specified by the protocol.

8.2 Immediate Card Payment and Immediate Fiscal Receipt

For immediate payment, the FEM begins the receipt process and sends **AMOUNT** (or a defined variant such as installment/completion/mail-order). The EFTPOS performs the transaction and returns **RESULT**. Upon successful result, the FEM completes the fiscal receipt and creates an **e.txt** record with code 358 for transmission to eSEND.

$$\text{FEM} \rightarrow \text{EFTPOS} : \text{AMOUNT}(S, A, C, D, R, H, T, M, Q), \quad (11)$$

$$\text{EFTPOS} \rightarrow \text{FEM} : \text{RESULT}(S, R, T, M, C, D, P). \quad (12)$$

This creates an explicit protocol-level association between fiscal issuance and payment authorization.

8.3 Card Prepayment

A.1027/2024 introduced a secure prepayment case in which no fiscal receipt is necessarily issued at the moment of payment. The FEM sends an **AMOUNT** command with the progressive counter set to zero. If the EFTPOS returns a successful **RESULT**, the FEM creates a special **e.txt** record with code 355 and reports it to eSEND. The record contains payment identification including session number, acquirer ID, terminal ID, RRN, transaction date/time, final amount, and transaction status. Thus, even without an immediate fiscal receipt, the card payment leaves an authoritative fiscal-system trace.

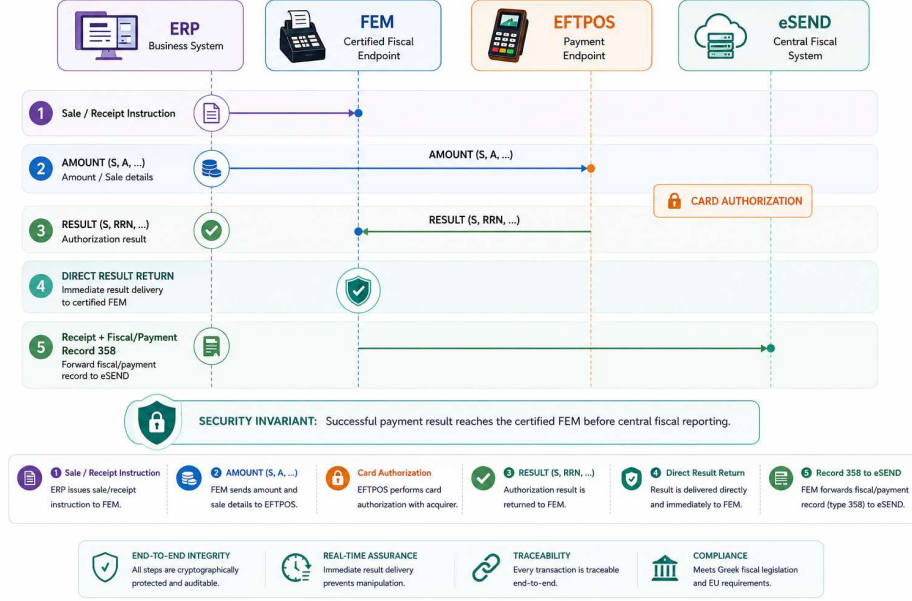


Fig. 4 Immediate-payment sequence in the unified FEM–EFTPOS architecture. The successful payment result returns directly to the certified FEM before the corresponding fiscal/payment record is reported to eSEND.

9 ERP/EIPS Intermediary Architecture under A.1155/2023

Decision A.1155/2023 permits an alternative architecture in which the ERP is interposed between FEM and EFTPOS [36]. The FEM may generate a token and send it to the ERP, which then communicates with the EFTPOS. Two implementation classes arise.

In the first, ERP and EFTPOS implement an arbitrary case-specific protocol. The decision does not prescribe a single command syntax or a mandatory encryption method for that ERP–EFTPOS link, and locked-keypad semantics are not guaranteed. In the second, the ERP relays tokenized commands compatible with the A.1088/2023 protocol. For example, a FEM can generate a token structurally equivalent to REGRECEIPT or AMOUNT; the ERP forwards it to the EFTPOS, which validates/decrypts it and treats it as the corresponding command. The EFTPOS then returns RESULT through the ERP to the FEM.

The second case preserves cryptographic protection of the token itself but changes the trust topology. The ERP now controls message delivery. It can potentially suppress a successful RESULT, prevent the FEM from completing a receipt or creating code 355/358, or fail to forward the payment information to myDATA. Cryptographic confidentiality of a token does not guarantee reliable end-to-end delivery of the transaction outcome.

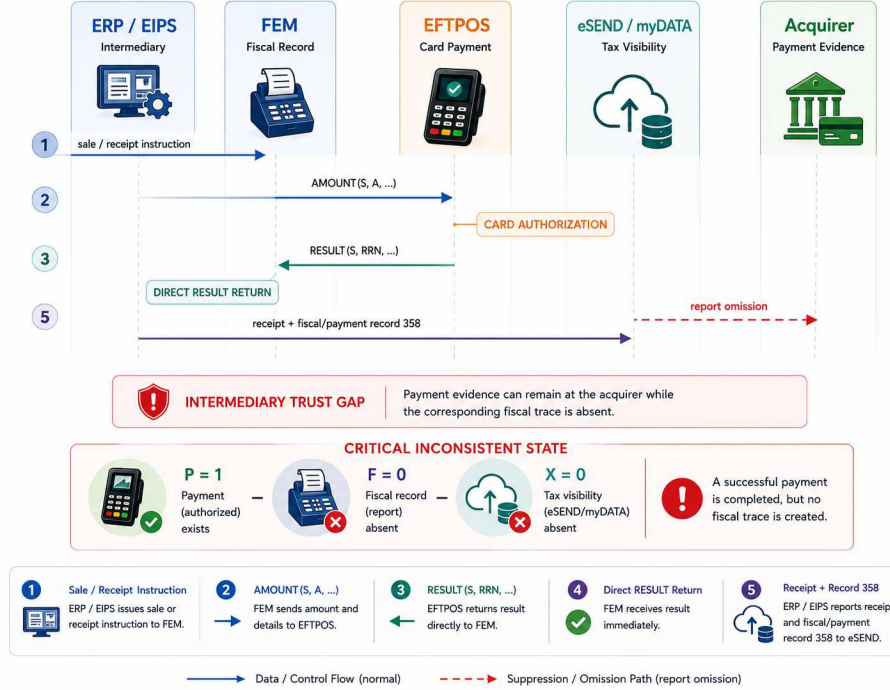


Fig. 5 Intermediary trust gap in the A.1155/2023 architecture. A successful authorization can remain visible to the acquirer while suppression at the ERP/EIPS layer prevents the corresponding fiscal trace from reaching the FEM or central tax systems.

10 Threat Model and Comparative Security Assessment

10.1 Immediate-Payment Suppression

Suppose the FEM creates an **AMOUNT**-type token and the EFTPOS successfully charges the card. If a malicious or compromised ERP does not forward the successful **RESULT** to the FEM, the FEM may retain a pending token and never complete the fiscal receipt or code-358 record. If the ERP also suppresses the corresponding myDATA transmission, the payment can exist in acquirer records without a corresponding fiscal-system record.

The ambiguity of a pending token rests in the fact that it may represent a legitimate failed payment due to many reasons, such as insufficient card balance. Thus, token lifecycle and deletion must be centrally specified and immutably logged, in order to enable pending tokens to be used as evidence of potentially deliberate suppression.

10.2 Prepayment Suppression

The aforementioned logic also applies to prepayments. A successful card transaction must lead to a code-355 **e.txt** record. In cases that the deployed ERP does not return a successful result to the FEM, subsequently the eSEND cannot not informed. This

results in payment presence at the acquirer’s side while, at the same time, being absent from the fiscal reporting chain.

10.3 EIPS and Free-Keypad Risk

The EIPS–EFTPOS interconnection described under A.1155/2023 supports multiple detailed command syntaxes equivalent to the unified FEM–EFTPOS protocol, and does not take into account the locked-keypad requirement. This enhances the attack surface, since a trader using an EIPS can potentially operate an EFTPOS with free amount entry, thus enabling them to accept card payments without the issuance and subsequent report of a corresponding retail receipt. This undermines the policy objective described as “card collection implies mandatory fiscal recording.”

The end-to-end fiscal-completeness requirement can be expressed as

$$P_j = 1 \Rightarrow (F_j = 1) \vee (X_j = 1), \quad (13)$$

where P_j denotes a successful electronic payment, F_j denotes the presence of a fiscal record connected to that payment, and X_j denotes a visible exception. A vulnerable architecture permits the undesirable state

$$P_j = 1, \quad F_j = 0, \quad X_j = 0, \quad (14)$$

which may result due to a successful card payment without corresponding fiscal records or auditable exceptions.

10.4 Security-Gap Classification

The security gaps can be grouped as follows:

- **Specification gap:** no authoritative ERP–EFTPOS command set, transport-security architecture, and device-state allocation across intermediary data flows.
- **Trust gap:** insertion of a non-certified or unchecked ERP between certified endpoints, acting as a weak link.
- **Binding gap:** central authorities may lack a verifiable cryptographic link linking fiscal receipt ID, payment authorization, and acquirer record.
- **Completeness gap:** a successful payment result can be dropped before the FEM creates the fiscal record.
- **Operational gap:** pending tokens can be difficult to distinguish from legitimate failed payments unless lifecycle telemetry is retained.

11 Economic and Public-Finance Evaluation Framework

The security analysis can be translated into a public-finance problem by treating an unmatched successful electronic payment as a transaction for which the tax authority

Table 2 Security and Fiscal-Integrity Comparison of the Unified Regulatory Architecture, the A.1155/2023 Intermediary Model, and the Proposed Architecture

Property		A.1098/2022– A.1088/2023– A.1027/2024	A.1155/2023 ERP/EIPS interme- diary	Proposed architec- ture
FEM–EFTPOS binding	direct	Yes in the unified FEM–EFTPOS transaction path	Not guaranteed when ERP/EIPS is interposed	Mandatory end-to-end binding independent of intermediary
Standardized syntax	command	Defined commands and transaction states, including AMOUNT, RESULT, REGRECEIPT, and RESEND–ALL	No single mandatory ERP–EFTPOS command syntax for all implementations	Single certified command/state model for FEM, ERP/EIPS, and EFTPOS
Trusted amount entry / locked EFTPOS keypad		FEM-controlled amount and locked-keypad semantics in the unified flow	Not uniformly mandatory for EIPS/intermediary operation	Mandatory trusted amount source and locked/equivalent protected entry
Session-key / message protection		Master/session-key mechanism; legacy cryptography remains in parts of the protocol	Protection depends on the specific path and implementation	AEAD-based protection, modern key derivation, rotation, and hardware-backed storage
Payment–receipt binding		Strong procedural/protocol association through tokenized fiscal-payment flow	Can be interrupted if the intermediary suppresses the successful payment result	Cryptographic token binds fiscal ID, amount, timestamp, nonce, RRN, and approval result
Central fiscal trace		eSEND receives fiscal/payment records such as codes 355, 356, and 358 when the prescribed flow completes	Trace may depend on the intermediary forwarding the result and/or reporting to myDATA	Successful EFTPOS result produces an independently auditable central trace
Replay/integrity protection	protec- tion	Session-based protection, but modernization is desirable	Implementation-dependent across intermediary links	Nonce, timestamp, AEAD/HMAC-SHA-256, anti-replay state, and signed result
Non-repudiation		Limited; central/fiscal records provide evidence but EFTPOS result is not universally independently signed	Limited and vulnerable to intermediary message suppression	EFTPOS/acquirer signature using device-protected keys plus immutable acknowledgement chain
Independent acquirer reconciliation	recon- ciliation	Possible operationally but not the primary end-to-end enforcement mechanism described	Incomplete if successful payment data are absent from fiscal reporting	Mandatory automated matching of acquirer RRN/authorization data with eSEND/myDATA records
Exposure to payment-without-receipt scenario		Low when the unified protocol is correctly enforced	Higher because message delivery and keypad controls can be weakened by the intermediary topology	Low by design; unmatched successful payments become centrally detectable exceptions

observes payment evidence but does not observe the corresponding fiscal liability. Let i index firms and t index days (or another audit interval). Define card turnover observed from acquiring records as C_{it} and card-linked fiscal turnover accepted by eSEND/myDATA as F_{it}^c . After accounting for legitimate timing differences, refunds, reversals, tips, and other legally defined adjustments L_{it} , the unmatched-payment gap

is

$$G_{it} = \max \{0, C_{it} - F_{it}^c - L_{it}\}. \quad (15)$$

The normalized mismatch rate is

$$g_{it} = \frac{G_{it}}{C_{it} + \varepsilon}, \quad (16)$$

where $\varepsilon > 0$ avoids division by zero. Unlike a comparison of aggregate daily sales and card payments, transaction-level matching by RRN, authorization code, amount, terminal, timestamp, and fiscal identifier can distinguish genuine unmatched authorizations from differences in payment mix.

11.1 Revenue-at-Risk Measure

Let τ_{it}^{eff} denote the effective VAT rate applicable to the unmatched taxable base. The gross VAT associated with unmatched card turnover is

$$\text{VATGap}_{it}^{\text{gross}} = \tau_{it}^{\text{eff}} G_{it}. \quad (17)$$

Because an unmatched record is an audit signal rather than proof of evasion, let $\pi_{it} = \Pr(E_{it} = 1 \mid \mathbf{x}_{it})$ denote the estimated probability that the mismatch represents non-compliance conditional on observable features $\mathbf{x}_{it}$. Expected VAT revenue at risk is then

$$\text{EVAR}_{it} = \pi_{it} \tau_{it}^{\text{eff}} G_{it}. \quad (18)$$

Aggregating Eq. (18) over firms and time provides a fiscally interpretable measure for audit prioritization without assuming that every mismatch is fraudulent.

11.2 Behavioral Model of Compliance

A stylized taxpayer chooses whether to suppress a fiscal record by comparing the expected private gain with the expected sanction. For transaction j , let A_j be the taxable amount, τ_j the effective tax rate, p_d the probability that suppression is detected, ϕ the monetary sanction conditional on detection, and c_j the operational or concealment cost. Suppression is privately attractive when

$$\tau_j A_j > p_d (\tau_j A_j + \phi) + c_j. \quad (19)$$

Solving for the minimum detection probability that eliminates the expected monetary incentive gives

$$p_d^* = \frac{\tau_j A_j - c_j}{\tau_j A_j + \phi}, \quad 0 \leq p_d^* \leq 1. \quad (20)$$

The economic function of mandatory payment–receipt binding and subsequent acquirer reconciliation extends beyond pure technical aspects. Such kind of controls increase the perceived and actual p_d , thus affecting the expected non-compliant return.

11.3 Econometric Identification Strategy

A policy evaluation should use administrative data rather than check policy effectiveness taking only into account aggregate VAT receipts. If implementation timing or mandate exposure creates treated and comparison groups, the baseline specification can be estimated as a difference-in-differences model:

$$Y_{it} = \alpha_i + \lambda_t + \beta (\text{Treat}_i \times \text{Post}_t) + \gamma' \mathbf{X}_{it} + \epsilon_{it}, \quad (21)$$

where Y_{it} may be the mismatch rate g_{it} , reported taxable sales, reported VAT, card-to-reported-sales ratio, or frequency of unmatched successful authorizations; α_i are firm fixed effects; λ_t are time fixed effects; and $\mathbf{X}_{it}$ controls for sector, firm size, seasonality, local economic conditions, payment mix, and other observable shocks. Standard errors should be clustered at the level at which treatment is assigned or serial correlation is expected.

For staggered adoption, Eq. (21) should be complemented by an event-study specification rather than relying only on a two-way fixed-effects coefficient:

$$Y_{it} = \alpha_i + \lambda_t + \sum_{k \neq -1} \beta_k \mathbf{1}\{t - T_i = k\} + \gamma' \mathbf{X}_{it} + \epsilon_{it}, \quad (22)$$

where T_i is the effective integration date. The pre-treatment coefficients β_k provide a diagnostic for parallel trends, while post-treatment coefficients trace persistence and dynamic adjustment. If treatment timing is endogenous, robustness analysis should use matched comparison firms, sector-by-time fixed effects, alternative windows, placebo dates, and estimators designed for heterogeneous staggered treatment effects.

The preferred administrative dataset would link, under appropriate privacy safeguards, (i) acquirer-side successful EFTPOS authorizations, (ii) FEM/eSEND records, (iii) EIPS/myDATA records, and (iv) firm characteristics. The primary transaction-level outcome is the indicator

$$U_j = \mathbf{1}\{P_j = 1, F_j = 0, X_j = 0\}, \quad (23)$$

which directly operationalizes the inconsistent state in Eq. (14). This design separates the paper’s architectural claim—that a failure state is feasible—from the empirical question of how frequently that state occurs and how regulation changes its incidence.

12 Original Observational Evidence from Anonymized Fiscal-Memory Records

12.1 Provenance, Sample, and Observation Windows

We complement the technical analysis and the separately labeled synthetic illustration with *observed* fiscal-memory receipts from 314 anonymized Fiscal Electronic Mechanisms (FEMs) provided by the company Solidus LTD (FEMs distributor). According to the data provider, devices were randomly selected from the company’s

FEM population, and authorized technicians obtained the amounts by reading fiscal memory. Device registration identifiers were replaced with pseudonyms (SAMPLE_1, SAMPLE_2, etc.). The data provide recorded monthly receipt amounts, not linked card-authorization, VAT liability, tax-return, or fraud outcomes. The interconnection month for each FEM is included as a YYYYMM field. No inference about the representativeness of all Greek firms is made.

The thirteen observation months are July 2023–2026, October 2023–2025, January 2024–2026, and April 2024–2026. These months are nonconsecutive; comparisons therefore use *the same calendar month in different years*, rather than adjacent observations. Values use decimal-comma notation in the source file. We parse missing cells as missing, not zero. For the primary matched-active comparison, a device is deemed active in both months if both recorded amounts are strictly positive. This operational definition is conservative for devices with genuine zero sales; an alternative definition based on device-registration status would require additional administrative information.

For season m and years y_0, y_1 , define the matched set $\mathcal{S}_{m,y_0,y_1} = \{i : R_{i,m,y_0} > 0, R_{i,m,y_1} > 0\}$. We estimate the aggregate same-month growth rate

$$\hat{g}_{m,y_0,y_1} = 100 \left(\frac{\sum_{i \in \mathcal{S}} R_{i,m,y_1}}{\sum_{i \in \mathcal{S}} R_{i,m,y_0}} - 1 \right), \quad (24)$$

where R is the observed FEM fiscal-memory receipt amount. We also calculate the median device-level percentage change. For the four-, or three-year season-specific charts, the balanced set contains only devices with strictly positive values in *all* available years of that season. This is a descriptive panel analysis, not a causal identification of tax compliance or the effect of EFTPOS interconnection.

12.2 Matched Active-Device Year-on-Year Comparisons

Table 3 Observed Solidus fiscal-memory receipts: same-month matched active FEMs. Euro amounts and percentages are descriptive, not VAT or causal effects.

Pair	N	Earlier (EUR)	Later (EUR)	Growth (%)	Median (%)
Jul23–Jul24	290	1,011,937	1,182,330	+16.84	+11.41
Jul24–Jul25	300	1,197,019	1,282,881	+7.17	+3.05
Jul25–Jul26	281	1,264,754	1,153,622	-8.79	-0.79
Okt23–Okt24	310	755,072	848,019	+12.31	+5.91
Okt24–Okt25	310	848,019	886,513	+4.54	-2.85
Jan24–Jan25	269	531,272	558,500	+5.12	+4.58
Jan25–Jan26	262	555,065	568,987	+2.51	-8.67
Apr24–Apr25	288	681,022	727,722	+6.86	-0.41
Apr25–Apr26	282	711,121	958,937	+34.85	-1.78

The matched-device results show positive year-on-year recorded receipts in July 2024 (16.84%) and July 2025 (7.17%), October 2024 (12.31%) and October 2025

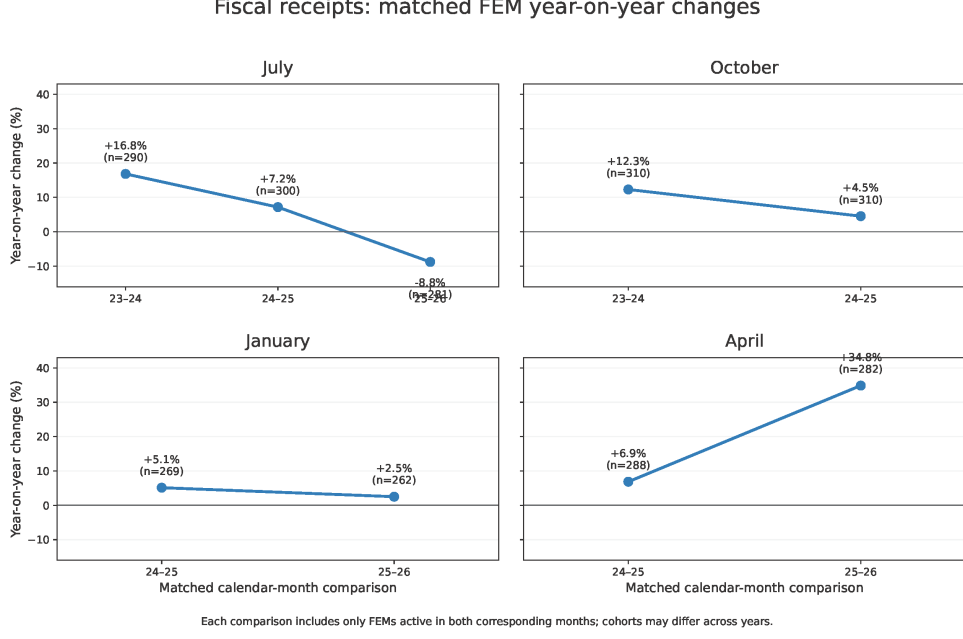


Fig. 6 Year-on-year percentage changes in observed fiscal-memory receipts for devices with positive amounts in both corresponding months. Each bar has its own matched cohort.

(4.54%), January 2025 (5.12%) and January 2026 (2.51%), and April 2025 (6.86%) and April 2026 (34.85%). July 2026 instead declines by 8.79% against July 2025 among matched active devices. The source provider attributes much of the July 2026 decrease to replacement of FEMs with Electronic Invoicing Provider Services (EIPS; Greek EIPS), which may move recorded sales outside the FEM fiscal-memory measurement channel. The dataset itself does not contain device-specific migration dates or EIPS-reported replacement turnover; hence this explanation is contextual information provided with the dataset, not independently established by the analysis.

The mean-weighted aggregate and median-device changes can diverge substantially: in April 2026, the aggregate matched-cohort increase is 34.85%, whereas the median individual-device change is -1.78% . Thus, growth is concentrated among relatively high-value devices or outliers and should not be described as a broadly shared increase across firms. Positive fiscal-memory receipts also reflect prices, business volume, mix of payment methods, firm entry/exit, and reporting-channel changes; they are not themselves evidence of recovered VAT or suppressed transactions.

12.3 Interconnection Timing and Identification Limits

All 314 pseudonymized records contain an interconnection month, with most connections occurring during 2024. For each matched annual pair, we classify devices as newly connected if their connection month is after the earlier observation month and no later than the later observation month, and as already connected if the connection

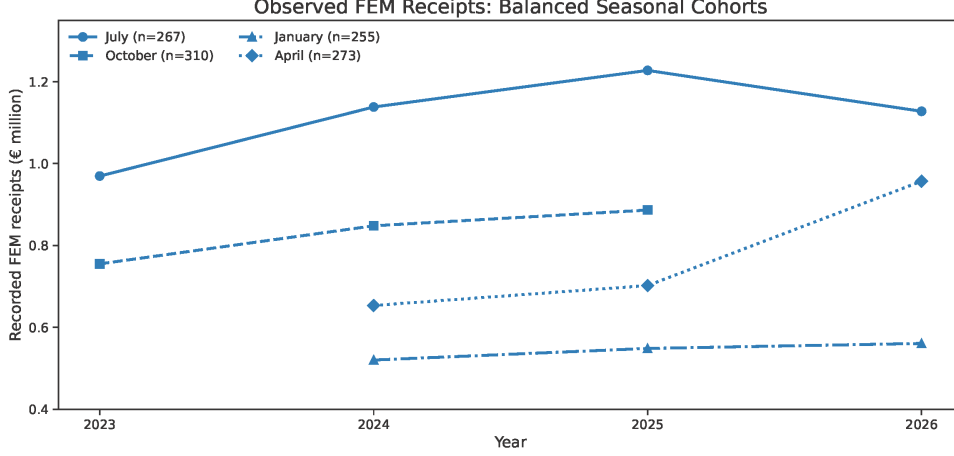


Fig. 7 Observed aggregate FEM receipts for strictly balanced cohorts within each calendar-month series: July ($N = 267$), October ($N = 310$), January ($N = 255$), and April ($N = 273$). The cohorts differ between panels and must not be pooled as a single continuous monthly series.

month is no later than the earlier observation. However, the data contain no substantial untreated contemporaneous comparison cohort for the key 2023–2024 rollout comparisons, and no monthly data around each individual adoption date. Accordingly, a parallel-trends test, reliable staggered-adoption difference-in-differences estimate, or causal event study is not identified from these observations. We do not apply the synthetic experiment’s estimated treatment effect to the observed Solidus devices.

Additional limitations are the absence of acquirer transactions, direct payment-to-receipt matches, sector and firm covariates, price adjustments, and independent verification of the asserted random selection. The available fiscal-memory receipts cannot measure the central security failure $P = 1, F = 0, X = 0$ because P is not observed. A defensible causal evaluation would require linked acquirer–FEM–EIPS administrative records, a contemporaneous untreated or not-yet-treated comparison, and verified migration histories.

13 Synthetic Empirical Results and Quantitative Evaluation

To demonstrate how the proposed identification strategy operates when transaction-level administrative microdata are available, we construct a reproducible synthetic panel. The exercise is explicitly a methodological validation and *not* evidence on the realized incidence of tax evasion in Greece. This distinction is necessary because the present study does not have access to linked acquirer–eSEND–myDATA microdata.

13.1 Synthetic Data-Generating Process

The synthetic sample contains $N = 400$ firms observed monthly for 25 event-time periods ($k = -12, \dots, 12$), yielding 10,000 firm-month observations. Half of the firms are

Table 4 Synthetic Difference-in-Differences Results

Group	Pre mismatch (%)	Post mismatch (%)	Change (pp)
Secure-integration group	1.59	0.81	-0.779
Comparison group	1.59	1.62	0.029
Difference-in-differences			-0.808
Standard error			0.012
<i>t</i> statistic			-69.2

assigned to a secure-integration group and half to a comparison group. Card turnover is generated from a log-normal firm-size distribution with common seasonality and idiosyncratic shocks. The payment–receipt mismatch rate follows

$$g_{it} = \mu + \alpha_i + \lambda_t + \delta t + \beta D_i Post_t + u_{it}, \quad (25)$$

where D_i identifies the synthetic treated firms. The calibration sets the baseline mismatch rate near 1.6% and imposes a treatment effect of approximately -0.8 percentage points after secure integration. Random firm heterogeneity and monthly shocks are added before bounding the mismatch rate to economically admissible values. An effective VAT rate of 18% is used only to translate unmatched turnover into a fiscal-risk quantity.

The synthetic design intentionally embeds parallel pre-treatment dynamics. Consequently, successful recovery of the imposed treatment effect tests whether the empirical specification in Eq. (21) can recover a known causal parameter under favorable identifying conditions. It does not validate those identifying conditions for actual Greek administrative data.

13.2 Difference-in-Differences Results

Table 4 reports the synthetic pre/post comparison. Prior to integration, treated and comparison firms exhibit similar mismatch rates. Following integration, the treated-group mismatch rate falls sharply while the comparison-group rate remains approximately stable. The difference-in-differences estimate is -0.808 percentage points. A firm-level pre/post change estimator gives a standard error of 0.012 percentage points ($t = -69.2$). The unusually high precision is a mechanical consequence of the deliberately strong signal and controlled synthetic data-generating process and should not be interpreted as a forecast of precision obtainable from real administrative data.

The magnitude has a direct fiscal interpretation. Conditional on the synthetic calibration, a reduction of 0.808 percentage points in unmatched card turnover corresponds to EUR 808,000 less unmatched turnover per EUR 100 million of card sales. Taking into account an 18% VAT rate, the gross VAT associated with this change can be approximated to EUR 145,440 per EUR 100 million of card turnover. This is merely a model-implied quantity, and not actual recovered Greek tax revenue. This

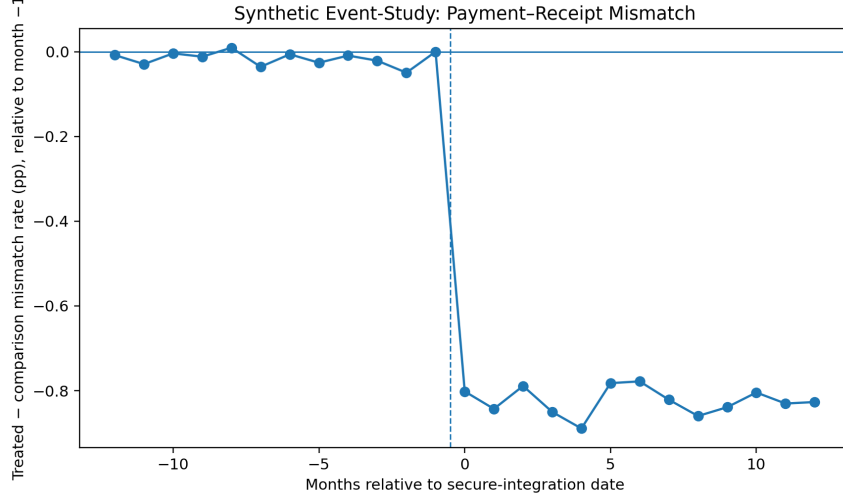


Fig. 8 Synthetic event-study of the payment–receipt mismatch rate. Values show the treated-minus-comparison difference relative to event month -1 . The data are simulated solely to demonstrate the proposed estimator.

may be attributed to mismatches reflecting legitimate timing, reversals, refunds, or measurement error, rather than potential tax evasion.

13.3 Synthetic Event-Study Evidence

Figure 8 implements Eq. (22) in actual event time and compares the gap associated with treated-minus-comparison in month -1 . The synthetic pre-treatment coefficients fluctuate around zero, as intended by the data-generating process. At the integration date a discrete negative shift appears and persists throughout the post-treatment window. In an application to real data, this figure would be central to the credibility of the causal design: systematic non-zero leads would warn against a simple parallel-trends interpretation, while gradual anticipation effects would motivate alternative treatment windows.

13.4 Fiscal-Risk Sensitivity

The empirical exercise can be connected to the architecture-level detection parameter. Let V denote card turnover subject to fiscalization, s the attempted suppression share, q the probability that the architecture detects or independently exposes suppression, and τ^{eff} the effective VAT rate. Expected undetected turnover and associated VAT revenue at risk are

$$U = Vs(1 - q), \quad R_{\text{VAT}} = Vs(1 - q)\tau^{\text{eff}}. \quad (26)$$

For EUR 100 million of card turnover, and by setting $s = 1\%$, and $\tau^{\text{eff}} = 18\%$, Table 5 shows how stronger detection mechanisms affect residual fiscal exposure.

Table 5 Fiscal-Risk Sensitivity per EUR 100 Million of Card Turnover

Scenario	q	Undetected turnover (EUR)	VAT at risk (EUR)
Weak reconciliation	0.60	400,000	72,000
Intermediate control	0.90	100,000	18,000
Strong end-to-end control	0.99	10,000	1,800
High-assurance target	0.995	5,000	900

The marginal fiscal benefit associated with the increase of detection from q_0 to q_1 is

$$\Delta R_{\text{VAT}} = V s \tau^{\text{eff}}(q_1 - q_0). \quad (27)$$

Thus, taking into account the above calculations, a change from $q = 0.60$ to $q = 0.99$ results in lower modeled VAT revenue at risk by EUR 70,200 per EUR 100 million of card turnover. As already mentioned above, this is a comparative simulation, and not an effect associated with policy change.

13.5 Public-Finance Cost–Benefit Criterion

C_0 denotes the fixed implementation cost, C_t^{op} annual operating costs, and ΔR_t additional tax revenue compared to the baseline. Then, the discounted net fiscal benefit can be calculated as follows:

$$\text{NPV} = -C_0 + \sum_{t=1}^T \frac{\Delta R_t - C_t^{\text{op}}}{(1+r)^t}. \quad (28)$$

This criterion enables the evaluation of the protocol intervention seen as a tax-administration investment, instead of merely a sole cybersecurity upgrade. If real cost and administrative data are taken into account, the break-even detection improvement can be evaluated from Eq. (28).

13.6 Interpretation and External Validity

The synthetic results highlight three narrower points. First, the mismatch indicator can be translated into an economical outcome. Second, a panel design can alleviated known reductions and mismatches in cases when parallel trends and treatment timing are controlled by construction. Third, the estimated aforementioned effect can be translated into economical metrics without translating every unmatched payment as potential fraud. They do *not* establish the prevalence of payment-without-receipt, the causal effect of A.1098/2022–A.1088/2023–A.1027/2024, or the fiscal cost of the A.1155/2023 architecture implementation. To address these issues, secure access to actual acquirer, eSEND, myDATA, and taxpayer records are needed.

14 Proposed Layered Mitigation Framework

A robust remediation framework must ensure interoperability while, at the same time, guaranteeing stronger security with the direct unified protocol.

14.1 Regulatory Unification

A.1155/2023 should be revoked or amended so that all ERP/EIPS-mediated payment flows are incorporated into the same protocol family and security semantics described in A.1098/2022, A.1088/2023, and A.1027/2024. The original European notification 2022/183/GR contemplated a single communication protocol. At minimum, all modes should require a standardized command syntax, locked-keypad or equivalent trusted amount-entry semantics, certified connectors, and mandatory reporting of successful payment outcomes.

14.2 Modern Authenticated Encryption

Legacy DES-based protection should not be used in new designs. New protocol revisions should use authenticated encryption with associated data (AEAD), such as AES-GCM or AES-GCM-SIV, together with mutually authenticated TLS where IP connectivity exists. Master/session keys should be generated, stored, and rotated using HSM-backed infrastructure.

14.3 Cryptographically Bound Fiscal-Payment Token

A proposed token is

$$T = \text{FEMID} \parallel \text{RID} \parallel A \parallel t \parallel N \parallel \text{MAC}_{K_s}(\cdot), \quad (29)$$

where RID is the fiscal receipt or prepayment identifier, A is the amount, t is the timestamp, N is a nonce, and K_s is the session key. HMAC-SHA-256 or an AEAD authentication tag can protect the fields.

The EFTPOS should return

$$R = T \parallel \text{RRN} \parallel \text{APPROVAL} \parallel \text{SIG}_{\text{POS}}, \quad (30)$$

where SIG_{POS} is produced by either a device-protected key or by the acquirer themselves. This makes the payment result independently verifiable even when an ERP relays the message.

For central verification, a deterministic binding identifier can be derived as

$$B = H(\text{FEMID} \parallel \text{RID} \parallel A \parallel \text{RRN} \parallel t \parallel N), \quad (31)$$

and included in both the fiscal-side and acquirer-side records. Reconciliation then reduces to checking equality of binding identifiers and consistency of the associated amount and status fields.

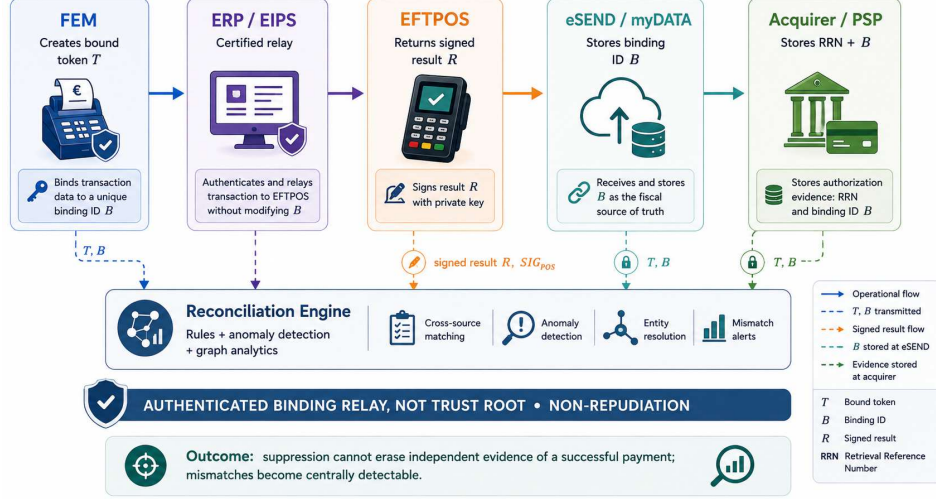


Fig. 9 Proposed secure end-to-end architecture. Transaction identifiers, signed EFTPOS results, fiscal and acquirer evidence, and central reconciliation reduce the intermediary to a relay.

14.4 Non-Repudiation and Immutable Telemetry

Certified EFTPOS devices should use HSM/TPM-backed keys for signing or authenticating successful results. ERP/EIPS systems should retain signed, append-only logs for token creation, forwarding, EFTPOS response, FEM acknowledgement, myDATA/eSEND upload, retry, expiration, and deletion. Token deletion without a terminal failure/decline result should itself be an auditable event.

14.5 Central Reconciliation and AI/ML Analytics

The tax authority should reconcile acquirer-side payment data with eSEND/myDATA fiscal records. A mismatch-detection pipeline can combine deterministic rules and ML. Candidate features include daily terminal totals, number of successful authorizations, code-355/358 counts, unmatched RRNs, ratios between pending and successfully calculated tokens, token lifetime, upload latency, repeated failures, geographic anomalies, and sudden shifts in cash/card ratio.

Graph-based models can provide an attractive alternative since taxpayers, FEMs, fiscal terminals, ERPs installations and providers, receipts, and payment identifiers form a graph with significant heterogeneity. Unsupervised learning can be useful in cases when confirmed fraud labels are sparse [30]. ML should be used for risk prioritization rather than acting as an alternative for cryptographic evidence or due-process requirements.

At an aggregation interval τ , a deterministic reconciliation residual can be calculated as follows:

$$\Delta_\tau = \sum_{j \in \mathcal{P}_\tau} A_j - \sum_{k \in \mathcal{F}_\tau} A_k, \quad (32)$$

where $\mathcal{P}_\tau$ denotes the set of successful card payments and $\mathcal{F}_\tau$ is the set of matched fiscal-payment records. During normal operation hours, Δ_τ should approach zero after refunds, reversals and potential delays are taken into account. A risk score can enhance the aforementioned residual with behavioral features as follows:

$$\mathcal{R} = \sigma \left(w_0 + \sum_{m=1}^M w_m x_m \right), \quad (33)$$

where x_m may include several features, such as unmatched-RRN ratio, token lifetime, suppression frequency, latency, and abnormal cash/card ratios; $\sigma(\cdot)$ denotes a calibrated scoring function.

14.6 Certification and Operational Controls

Certification should extend beyond just checking FEM firmware to the complete integration. ERP/EIPS connectors participating in payment routing should undergo conformance tests including successful message delivery, replay resistance, key handling, error recovery, locked-keypad behavior, and existence of mandatory reporting capabilities. Repeated mismatches should trigger targeted audits and incident reporting.

15 Implementation Roadmap

An implementation roadmap may result in potential disruptions minimization, as described below:

1. **Immediate regulatory action:** implement requirements for amount binding, token lifecycle logging, and a common ERP/EIPS protocol profile, thus suspending insecure paths.
2. **Short term (3–6 months):** implement the standardized token and signed-RESULT specification policy; integration with AEAD; update EFTPOS firmware and ERP/EIPS connectors; pilot implementation with selected acquirers.
3. **Medium term (6–18 months):** deployment of automated acquirer–eSEND/myDATA reconciliation and risk scoring; mandatory requirement of certification for production ERP/EIPS integrations.
4. **Long term:** migrate legacy SHA-1/DES mechanisms to modern cryptographic schemas while preserving audit continuity; evaluate centralized extensions for high-risk sectors and government procurement.

16 Discussion, Policy Implications, and Limitations

The comparison between eSEND/FEM and myDATA/EIPS architectures clearly demonstrates that secure data transport comprises only one layer of fiscal integrity. The FEM architecture combines protected hardware, non-modifiable fiscal memory, progressive numbering, daily closure, hash chaining, and server-side sequence validation. The aforementioned controls enable omission detection even when data

communication is delayed. On the contrary, a software-centric path can be protected in transit yet it still permits pre-transmission deletion or modification unless sequencing is enforced by another actor.

The same difference appears in the payment protocol. A token encrypted between FEM and EFTPOS can retain its authenticity while an intermediary may suppress its successful response. Therefore, the security objective must be incorporated on an end-to-end basis: every successful card authorization must become either (i) a fiscal receipt/payment record accepted or (ii) a visible exception that can be reconciled against acquirer records.

The source study reports an estimated VAT-collection increase of approximately 25% following FEM–EFTPOS interconnection. This figure illustrates the fiscal importance attributed to this interconnection. However, a causal econometric evaluation would require a separate dataset and distinct methodology. The architectural analysis presented in this work does not claim to establish causality for that estimate.

16.1 International Applicability

Although the detailed protocol and regulatory references take the case of Greece as a case study, the control problem can be generalized. Any country that wishes to couple fiscalization purposes with electronic payment acceptance must determine where the authoritative payment–receipt binding is created, identify trusted components, and detect successful payments absent from fiscal reporting. The framework presented in the present work addresses horizontal technological aspects: endpoint behavior, transaction completeness, cryptographic binding, reconciliation, and auditable exception handling. Country-specific implementations would nevertheless have to reflect local fiscal-device law, payment-services regulation, privacy requirements, and acquiring infrastructure.

16.2 Limitations and Future Validation

The present work is based on technical and regulatory analysis rather than controlled penetration testing or access to population-scale acquirer and tax-authority datasets. Consequently, the threat scenarios demonstrate architectural feasibility and control gaps; they do not establish observed fraud frequency. Likewise, the proposed cryptographic extensions have not yet been benchmarked on certified production FEM/EFTPOS hardware. Future work should implement a reference prototype, test normal and adversarial message sequences, quantify latency and availability impacts, define formal security properties, and evaluate reconciliation algorithms on appropriately anonymized transaction data. These steps would convert the present design analysis into an experimentally validated fiscal-payment security framework.

17 Conclusion

This paper presented an integrated extension of the Greek fiscal-security analysis from device-level blockchain/hash-chain logging to the complete payment-reporting path. Certified FEMs and the eSEND back end provide strong integrity properties through

protected fiscal memory, progressive counters, Z-report sequencing, hash chaining, encrypted transmission, and server-side validation. The direct unified FEM–EFTPOS protocol further couples card payments to fiscal records through locked amount entry, shared keys, structured commands, and explicit payment-result reporting.

The principal weakness arises when an ERP/EIPS intermediary becomes capable of controlling whether a successful payment result reaches the FEM or central reporting infrastructure. Under A.1155/2023, underspecified ERP–EFTPOS communication and the absence of uniformly mandatory locked-keypad semantics create a practical route for payment/fiscal decoupling. The proposed remediation combines protocol unification, modern AEAD, cryptographically bound tokens, signed EFTPOS results, hardware-backed keys, immutable token telemetry, and central acquirer reconciliation supported by AI/ML anomaly detection.

The key architectural design principle lies in the fact that all successful electronic payments must leave a verifiable fiscal trace regardless of the software path used. Extending this principle consistently to FEM, ERP, EIPS, EFTPOS, eSEND, and myDATA preserves interoperability while also reducing tax-evasion surface.

Data Availability

A synthetic firm-month panel was generated to demonstrate the proposed econometric and fiscal risk framework. The synthetic data contain no taxpayer, acquirer, eSEND, myDATA, or administrative data. They must not be interpreted as evidence of observed tax evasion, VAT losses, or the actual effect of Greek regulation. Observed anonymized Solidus LTD fiscal-memory records were analyzed descriptively, and a separate synthetic panel was used to illustrate econometric methods. The underlying source data may be made available subject to permission from the data provider.

Abbreviations

FEM	Fiscal Electronic Mechanism
EFTPOS	Electronic Funds Transfer at Point of Sale
ECR	Electronic Cash Register
EAFDSS	Fiscal Signing Machine
FEMAS	Fiscal Electronic Mechanism of Accumulation and Signing
EIPS	Electronic Invoicing Provider Service
ERP	Enterprise Resource Planning
eSEND	FEM Central Information System
myDATA	IAPR/AADE digital reporting platform
IAPR/AADE	Independent Authority for Public Revenue
RRN	Retrieval Reference Number
AEAD	Authenticated Encryption with Associated Data
HSM	Hardware Security Module

Acknowledgements. The authors thank Mr. Giorgos Voulgarelis, Chief Executive Officer of Solidus LTD, for facilitating access to anonymized FEM fiscal-memory

receipt data and supporting the collaboration with authorized technicians. The authors remain responsible for the analysis and interpretation.

Declarations

Author contributions. All authors contributed equally to the conceptualization, technical analysis, and preparation of the manuscript. All authors read and approved the final manuscript.

Funding. The authors received no funding for this work.

Data availability. No datasets were generated or analyzed during the current study.

Competing interests. The authors declare no competing interests.

References

- [1] M. Iansiti and K. R. Lakhani, “The truth about blockchain,” *Harvard Business Review*, vol. 95, no. 1, pp. 118–127, 2017.
- [2] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [3] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O’Reilly Media, 2015.
- [4] J. S. Sogaard, “A blockchain-enabled platform for VAT settlement,” *International Journal of Accounting Information Systems*, p. 100502.
- [5] K. Yent, “Applying blockchain technology to cross-border tax reporting,” UCL Centre for Blockchain Technologies, Discussion Paper no. 4, 2020.
- [6] G. Bossa and E. de Paiva Gomes, “Blockchain: Technology as a tool for tax information exchange or an instrument threatening the taxpayer’s privacy?,” *SSRN Electronic Journal*, 2019.
- [7] E. Mik and N. Noked, “Blockchain and tax administration: A critical assessment.”
- [8] C. J. Delmotte, “Toward a blockchain-driven tax system,” SSRN, 2022.
- [9] R. T. Ainsworth and M. Alwohaibi, “Blockchain, Bitcoin and VAT in the GCC: The missing trader example.”
- [10] Council Directive 2006/112/EC, *Official Journal of the European Union*, L347, Dec. 11, 2006.
- [11] Law 4308/2014, “Greek Accounting Standards, related regulations, and other provisions,” *Official Journal of the Greek Government*, no. 251A, Nov. 24, 2014.

- [12] POL 1135/2005, “Completion of technical specifications of Fiscal Electronic Machines and Systems,” *Greek Government Gazette*, no. 1592B, Nov. 17, 2005.
- [13] POL 1220/2012, “Codification and completion of technical specifications of Fiscal Electronic Mechanisms,” *Greek Government Gazette*, no. 351B, Dec. 31, 2012.
- [14] A.1024/2020, “Supplementary technical specifications of communication and encryption protocol for transmission to the FEM Information System,” *Greek Government Gazette*, no. 317B, Feb. 6, 2020.
- [15] A.1173/2022, “Amendment of the technical specifications of Fiscal Electronic Mechanisms,” *Greek Government Gazette*, no. 6593B, Dec. 30, 2022.
- [16] POL 1068/2015, “Procedures for the approval and revocation of Fiscal Electronic Mechanisms,” *Greek Government Gazette*, no. 497B, Apr. 1, 2015.
- [17] National Institute of Standards and Technology, “Secure Hash Standard (SHS),” FIPS PUB 180 series.
- [18] A.1098/2022, “Determination of technical specifications for the interconnection between Fiscal Electronic Mechanisms and EFT/POS terminals,” *Greek Government Gazette*, no. 3940B, Jul. 25, 2022.
- [19] A.1088/2023, “Amendment of A.1098/2022 on the interconnection between Fiscal Electronic Mechanisms and EFT/POS terminals,” *Greek Government Gazette*, no. 3875B, Jun. 15, 2023.
- [20] A.1027/2024, “Amendment of A.1098/2022: technical specifications and functions for the interface between FEM and EFT/POS terminals,” *Greek Government Gazette*, B’ 1134, Feb. 16, 2024.
- [21] POL 1166/2018, “Technical specifications of communication and encryption protocol for the transmission of data to the FEM Information System,” *Greek Government Gazette*, B’ 3603, Aug. 24, 2018.
- [22] P. Mavridis, A. T. Baklezos, and C. D. Nikolopoulos, “e-Invoicing Provider Services in Greece: New perspectives and weaknesses,” in *Proc. 5th Int. Conf. Electronic Engineering, Information Technology and Education (EEITE)*, Athens, Greece, 2024, pp. 1–4, doi: 10.1109/EEITE61750.2024.10654410.
- [23] A.1035/2020, “Obligations of Electronic Invoicing Providers and control procedures for the provision of Electronic Invoicing Provider Services,” *Greek Government Gazette*, no. 551B, Feb. 20, 2020.
- [24] A.1158/2023, “Amendment of Decision A.1035/2020 on Electronic Invoicing Provider Services,” *Greek Government Gazette*, no. 5996B, Oct. 13, 2023.

- [25] A.1126/2024, “Amendment of A.1035/2020 on electronic data issuance services,” *Greek Government Gazette*, no. 4557B, Aug. 6, 2024.
- [26] A.1112/2025, “Amendment of Electronic Invoicing Provider Services,” *Greek Government Gazette*, no. 4206B, Aug. 1, 2025.
- [27] P. Mavridis, A. T. Baklezos, and C. D. Nikolopoulos, “Blockchain-enabled secure logging for Fiscal Electronic Mechanisms: Evaluation of the Greek eSEND and myDATA tax systems,” conference paper, 2026.
- [28] P. C. Abrantes and F. Ferraz, “Big data applied to tax evasion detection: A systematic review,” in *Proc. Int. Conf. Computational Science and Computational Intelligence*, 2016, doi: 10.1109/CSCI.2016.0089.
- [29] W. Didimo *et al.*, “Combining network visualization and data mining for tax risk assessment,” *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2967974.
- [30] Y. Gao *et al.*, “Tax evasion detection with FBNE-PU algorithm based on PnCGCN and PU learning,” *IEEE Trans. Knowl. Data Eng.*, 2023, doi: 10.1109/TKDE.2021.3090075.
- [31] Y. Lin *et al.*, “TaxThemis: Interactive mining and exploration of suspicious tax evasion groups,” *IEEE Trans. Vis. Comput. Graph.*, 2021, doi: 10.1109/TVCG.2020.3030370.
- [32] F. Tian *et al.*, “Mining suspicious tax evasion groups in big data,” *IEEE Trans. Knowl. Data Eng.*, 2016, doi: 10.1109/TKDE.2016.2571686.
- [33] N. Visitpanya and T. Samanchuen, “A machine learning approach to identifying suspicious tax evasion behavior in public financial data,” in *Proc. ICBIR*, 2023, doi: 10.1109/ICBIR57571.2023.10147479.
- [34] Y. Wang *et al.*, “T-EGAT: A temporal edge enhanced graph attention network for tax evasion detection,” in *Proc. IEEE Big Data*, 2020, doi: 10.1109/Big-Data50022.2020.9378157.
- [35] N. Visitpanya and T. Samanchuen, “Synthesis of tax return datasets for development of tax evasion detection,” *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.3276761.
- [36] A.1155/2023, “Determination of the scope, time, manner and procedure of the interconnection of EFT/POS with cashier systems and payment-service-provider infrastructure,” *Greek Government Gazette*, 2023.
- [37] L. Nascimento, P. Da Silva, and C. Peres, “Blockchain’s potential and opportunities for tax administrations: A systematic review,” in *Proc. BCCA*, 2021, doi: 10.1109/BCCA53669.2021.9657036.

- [38] J. Mathews *et al.*, “Regression analysis towards estimating tax evasion in Goods and Services Tax,” in *Proc. IEEE/WIC/ACM Web Intelligence*, 2018, doi: 10.1109/WI.2018.00011.
- [39] P. Mehta *et al.*, “Identifying malicious dealers in Goods and Services Tax,” in *Proc. IEEE ICBDA*, 2019, doi: 10.1109/ICBDA.2019.8713211.
- [40] X. Xiangyu, Y. Youlin, and X. Qicheng, “Intelligent identification of corporate tax evasion based on LM neural network,” in *Chinese Control Conference*, 2018, doi: 10.23919/ChiCC.2018.8483951.

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- [deigmafhm.csv](#)