Enhanced Fraud Data (EFD) Messaging Standard

V0.21

March 2024

Contents

1 Documentation Information

Version History

Version	Date	Description	Author
V0.1	31/03/2023	Initial messaging standard	Martin Sansone – Lead Architect
V0.1b	08/01/2024	Inclusion of Sidecar Data Pattern	Stephen Hartley – Solution Architect
V0.2	26/02/2024	Industry feedback updates	Martin Sansone – Lead Architect
V0.21	12/03/2024	Additional capabilities	Martin Sansone – Lead Architect

Copyright Statement

2 Introduction

Understanding EFD Messaging

Pioneering Trust and Transparency in the Digital Payment Era

EFD Messaging, short for Enhanced Fraud Data Messaging, introduces a groundbreaking way to make financial transactions safer and more transparent in today's digital world. Traditionally, when money is sent from one party to another, only basic information is exchanged, which can sometimes hide who's behind the transaction, their intentions, or their financial habits. As we move towards a world with fewer face-to-face interactions, establishing trust in these transactions has become more challenging, often based on scant evidence of who's actually on the other end.

Even though new technologies allow for more data to be shared during these transactions *(for example, the ISO 20022 global standard for the electronic exchange of financial transaction data)*, they often miss out on crucial details that could help reveal the true nature of these exchanges. EFD Messaging steps in to fill this gap. It's a specialised exchange of information that happens alongside the payment process, designed with the help of experts in financial crime. It aims to provide specific, crucial data that helps identify suspicious activities before they happen.

A key feature of EFD Messaging is its flexibility. It's built to evolve, allowing the system to adapt over time as financial institutions enhance their methods and fraudsters change tactics. This agility is vital for staying one step ahead in the ongoing fight against fraud, making financial transactions safer and building a foundation of trust and transparency in the digital age.

The Vision

Our vision for EFD Messaging goes beyond traditional financial transaction security. We are setting a new standard in the digital payment landscape, aiming to re-establish trust where it has been eroded. By introducing a more comprehensive data exchange through EFD Messaging, we envision a world where financial interactions are secure, transparent, and informed. This initiative seeks to restore the confidence that once stemmed from face-to-face relationships and direct knowledge of transaction parties in this new digital realm.

EFD Messaging aims to significantly reduce fraudulent activities, such as Automatic Push Payment (APP) Fraud, enhancing the reliability of digital payments. This guide lays the foundation for this vision, offering comprehensive insights into implementing EFD Messaging and making financial transactions safer for everyone, from everyday users to large financial institutions.

Benefits for All:

- **For Consumers:** Gain reassurance in the authenticity and security of their financial engagements.
- **For Banks and Payment Service Providers (PSPs):** Empowerment through advanced data to enhance fraud detection and prevention.
- **For the Financial Ecosystem:** It is a dynamic and adaptable standard that evolves with emerging use cases, threats and technologies, ensuring long-term resilience and integrity.

Navigating this Guide:

This guide aims to be accessible to everyone, regardless of their familiarity with financial technology. It is essential to understand the hierarchy of terms used to describe the standard:

1. **EFD Service**: This is the most encompassing term, referring to the entire solution operated by Pay.UK for PSPs to exchange customer personally identifiable information (PII) data in the first use case(UC-1). It implies a comprehensive system including all components and processes.
2. **EFD Message Standard**: This is a more specific term focusing on the structure and protocol for exchanging messages within the service. It includes details on the format of request and response messages and the additional statistical data message, which follows the architectural Sidecar pattern.
3. **EFD Data Standard**: The most granular level defines individual data fields within the EFD messages. It details each field's syntax, constraints, dependencies, and rules.

Background

As part of addressing the specific challenges of APP fraud, UK Finance (UKF) and Pay.UK agreed to set up a common approach with industry engagement. One facet of this was Pay.UK 's development of an Enhanced Fraud Data (EFD) Messaging Standard, capable of carrying data in a pre-agreed, structured format that could be used more quickly and easily by economic crime (EC) specialists to have better-informed detection of potential fraud for both sending and receiving firms.

The EFD Messaging Standard is specifically designed for a pre-payment initiation message exchange *(outside of the payment flow and irrespective of payment channel),* carrying data points between the sending and receiving financial institutions participating within an organised trust framework that is of maximum benefit to help identify APP fraud.

It is important to note that the development of the overall EFD Messaging Standard has had separate work streams focussing on five distinct pillars which combine to help deliver the overall EFD Service solution:

1. **Data protection workstream**
   ICO engagement and privacy assessment leading to an accepted DPIA
2. **Standards workstream (*the EFD Messaging Standard as the output*)**
   Development of technical standards for a universally accepted data-sharing pattern
3. **Architects workstream**
   Development of potential implementation solutions to support the EFD Message data sharing
4. **Governance workstream**
   Development of the liability framework and any 'scheme' constructs that are required to answer eligibility criteria, data protection, limitations, dispute process and commercial models
5. **Regulatory engagement**
   UK Finance and the Payment Systems Regulator (PSR) support for engagement with stakeholders

The outputs from the five work streams support the other workstream activities in developing the overall solution, its rulebook and operation.

This document represents the output of the Standards workstream #2 above. It uses the concepts established within the common approach. A revised draft of the starting EFD Data Model is included in the appendices of this document. It provides an initial view of the EFD Service to allow parties wishing to use this messaging standard to start their design and guidance on using the associated technical standards artefacts, collateral and sample content within this release.

All the artefacts referred to in this document and released in March 2024 enable organisations to plan for, test and implement their build to participate within an EFD Messaging Framework.

Intended Audience

This guide's primary audience is banking and payment industry professionals within the United Kingdom, encompassing roles from technical implementers to policy strategists. It is particularly relevant for those involved in various UK payment channels like Faster Payments, Open Banking, NPA and CHAPS.

The EFD Messaging Standard's alignment with international banking practices and adaptability for cross-border transactions are valuable resources for global financial institutions and regulatory bodies. This guide serves as a blueprint for regions worldwide looking to enhance their defence against the escalating challenge of payment fraud. This inclusive approach ensures that the standard's benefits extend beyond the UK, offering a scalable and adaptable solution towards global financial security.

How to use this document

This document is an essential guide for implementing the EFD Messaging Standard within the UK and potentially internationally. Its instructions must be applied to all EFD messages:

1. **Evolution and Updates**: As the EFD Messaging Standard evolves, this document will reflect new developments and expanded content. Stay informed of these changes via its version control for effective implementation.
2. **Complementary Resources**: This guide should be used alongside other Pay.UK artefacts in the EFD Service Set for a comprehensive understanding. Artefacts like message schemas for requests and responses, implementation guidelines, message sequence diagrams, the sidecar pattern for success metrics, and sample real-world examples.
3. **Continuous Engagement**: Developed through ongoing engagement and feedback from the payments ecosystem, this document represents a collective effort towards a robust standard.
4. **Accuracy and Feedback**: While every effort is made to ensure accuracy, errors or omissions may occur. Your feedback is invaluable. Please report any discrepancies to standards@wearepay.uk.
5. **Implementation Guidance**: This document and the Implementation Guidelines outline Pay.UK's technical approach for the pre-payment data-sharing exchange is integral to EFD messaging.

Your contribution and adherence to these guidelines are crucial in fostering a secure and efficient anti-fraud payment environment. To check the terminology used within this document, use the separate EFD Glossary Document.

3 Antifraud Data Sharing – Alignment

The EFD Messaging Standard is designed to be extensible, use the concepts and business logic contained within, and align where possible with ISO20022's naming convention. The standard seeks to align with existing regulatory requirements (*See also Section 7 Legal Framework*) and industry practices while effectively introducing innovative methodologies for combating fraud. The EFD messages:

- aim to share helpful data points between transacting parties to improve fraud risk assessment **before initiating any transaction**;
- emphasises interoperability across various banking and payment schemes and initiatives such as CHAPS, CBPR+, SEPA, CGI-MP, and Open Banking but with a clear intention that the EFD Messaging Standard itself is **framework agnostic** on purpose;
- attempts to integrate with international standards such as the OpenID Connect for Identity Assurance (OIDC IDA) and alignment with the UK's Digital Identity and Attributes Trust Framework (DIATF);
- facilitate a unified approach to identity verification, risk assessment, and fraud prevention, leveraging modern technology and providing robust defence against fraudulent activities.

The standard's extensible nature allows for continuous evolution, accommodating emerging threats and incorporating feedback from PSP crime specialists to refine the system's effectiveness.

Reference information for future alignment has been sourced, as shown in the table below.

Reference	Payment/Identity Initiative
CHAPS	CHAPS RTGS Renewal Programme (includes HVPS+ alignment)
CBPR+	Cross Border Payments and Reporting Plus market practice guidelines
SEPA Instant	Single European Payments Area Instant Credit Transfer Scheme Interbank Implementation Guidelines
CGI-MP	The Common Global Implementation (CGI)
Open Banking	Open Banking UK
OpenID IDA + Guide	OpenID Identity Assurance
Digital ID	UK Digital Identity & Attributes Trust Framework (DIATF)
eIDAS	electronic IDentification, Authentication and trust Services

Table 1: EFD Messaging Standard Alignment

Alignment tasks outstanding:

1. Berlin Group: Payment Data Model for Version 2.0 of the open Finance API Framework https://www.berlin-group.org/_files/ugd/c2914b_f8cab18ec71e476a9685c9a5f5260fda.pdf
2. EUDIW draft-payment-presentation-profile https://digitallabor.berlin/draft-payment-presentation-profile.html
3. JSON to Future state - supporting JSON-LD https://www.w3.org/TR/json-ld11/
4. Verifiable Credentials Data Model v1.1 Verifiable Credentials Data Model v1.1 (w3.org)

4 Stakeholders in the EFD Ecosystem: Roles and Responsibilities

The EFD Service is a collaborative ecosystem designed to enhance the security and integrity of digital payment systems. It relies on stakeholders' active participation and cooperation, each contributing to a robust framework to prevent fraud. This section outlines the key roles and responsibilities within the EFD ecosystem, ranging from Payment Service Providers (PSPs) to regulatory authorities. It highlights how each contributes to the overarching goal of secure, efficient, and transparent payment processes.

Section 11, "Adapting EFD Messaging Standards for Diverse Ecosystems," emphasises the pivotal points in enabling any EFD Service in a region to adapt to diverse ecosystem requirements, reinforcing the ecosystem's capacity for innovation and resilience.

Direct Participants (PSPs)

Entities authorised to initiate or receive payments directly engaged in EFD message exchanges.

Responsibilities:

- Initiate and receive EFD messages as part of the transaction process.
- Ensure compliance with EFD Service standards and regulations.
- Implement robust fraud detection and prevention measures.

Indirect Participants

Entities participating in EFD through Aggregators are indirectly involved in EFD message exchanges.

Responsibilities:

- Participate in the EFD Service through Aggregators.
- Adhere to the operational and security requirements set by the EFD Service.

Aggregators

Facilitate participation for Indirect Participants by providing the necessary technology and system support.

Responsibilities:

- Facilitate the participation of Indirect Participants.
- Provide technical and operational support to meet EFD Service standards.

Technology Providers

Supply equipment, systems, technology, and services to enable or facilitate the EFD Standard for Direct Participants and Aggregators.

Responsibilities:

- Supply and maintain technology solutions to support EFD messaging and compliance.
- Ensure the reliability and security of systems used for EFD transactions.

EFD Service Provider

Manages and operates an EFD Service, maintaining the infrastructure, standards, and compliance.

Responsibilities:

- Manage and operate an EFD Service infrastructure.
- Set and enforce standards for EFD message exchange and compliance.
- Monitor and support the ecosystem's integrity and security.

Regulatory Authorities

Oversee compliance with financial laws and regulations, ensuring the integrity and security of the EFD Service.

Responsibilities:

- Oversee the EFD Service's adherence to legal and regulatory frameworks.
- Ensure the protection of consumer rights and data privacy.

Customers

End-users of the PSPs' services, whose transactions are subject to EFD message exchanges for fraud prevention. End-users are not parties to viewing the data contained within EFD message exchanges.

Responsibilities:

- Engage with PSPs under the protection of the EFD Service.
- Remain informed about the security measures in place for their transactions.

EFD MI Provider

Analyses EFD MI Sidecar messages to improve fraud detection strategies and the effectiveness of the EFD Service.

Responsibilities:

- Analyse EFD MI Sidecar message data to improve fraud detection strategies.
- Provide insights back to the participants to enhance the effectiveness of the EFD Service.

Technical Support Teams

Ensure the technical reliability and security of the EFD Service.

Responsibilities:

- Ensure the continuous operational reliability and security of the EFD Service.
- Address technical issues and support system upgrades and maintenance.

BECOME INVOLVED: There can be multiple EFD Services in many regions of the world, solving specific use case issues. Show your interest for involvement and implementing EFD Messaging in any of the above capacities by emailing

efd@wearepay.uk

5 Enhanced Reliability through KYC in EFD Messaging

The foundation of trust and transparency in digital payment ecosystems lies significantly in the rigorous application of **Customer Identification Programs (CIP)** and **Know Your Customer (KYC) processes**. These programs are not just regulatory requirements but critical tools for understanding and verifying the identities of parties involved in financial transactions. In the context of Enhanced Fraud Data (EFD) Messaging, the depth and rigour of KYC processes employed by banks provide a rich layer of verified identity information and account behaviour insights.

Customer Identification and Verification

Banks implement comprehensive procedures to collect and verify identification information from all clients when opening a new account or adding any party to an existing account. This information, encompassing legal names, Tax ID numbers, dates of birth, and physical addresses, is meticulously verified against reliable documents or through advanced electronic verification systems. Such thoroughness ensures that every transaction initiated or received is backed by a profile that has undergone stringent checks against potential financial crimes.

Risk Assessment and Ongoing Diligence

Identifying a client marks the beginning of a continuous risk management process. Banks assess the risk at client and account levels, tailoring due diligence efforts to the risk profile. Enhanced Due Diligence (EDD) and Ongoing Due Diligence are mechanisms for deeper investigation, particularly for clients in industries or with behaviour patterns that suggest higher risk. This continuous monitoring is crucial for updating customer information and ensuring that EFD Messages reflect the most current and accurate risk assessment.

Implications for EFD Messaging

In the EFD Messaging framework, the richness of KYC data translates into more effective fraud detection and prevention strategies. PSPs leveraging EFD Messages benefit from:

- Access to a baseline of verified digital identity and risk information, enhancing the accuracy of fraud assessments.
- The ability to incorporate real-time changes in customer profiles and risk ratings into fraud detection algorithms.
- Enhanced transparency between PSPs, fostering mutual trust in the authenticity of transaction parties.

By integrating KYC and CIP insights into EFD Messaging, the digital payment ecosystem moves closer to its goal of pioneering trust and transparency. This integration mitigates the risk of fraud and strengthens the foundation for secure and reliable financial transactions.

6 Understanding PSP Capabilities in EFD Messaging

Understanding and accommodating PSPs' diverse capabilities becomes crucial as the Enhanced Fraud Data (EFD) Messaging Standard evolves to enhance fraud detection and prevention across payment service providers (PSPs). This section introduces a nuanced approach to PSP data attribute handling. It distinguishes between attributes PSPs can receive/process for fraud risk assessments and attributes they can access/share for operational efficiency. Facilitating gradual adoption and capability expansion

Operational Definitions

- **Receivable and Processable Attributes**: These are the data attributes that a PSP can effectively receive and utilise within their fraud risk engines to assess the potential risk of fraud in a transaction. This capability is pivotal for the PSP's active participation in identifying and mitigating fraudulent activities.
- **Accessible and Shareable Attributes**: A PSP can access and share information from its internal systems with other PSPs. This capability is essential for collaborative fraud prevention efforts, enabling PSPs to exchange relevant information seamlessly.

Operational Impact on Fraud Risk Engines

The ability of PSPs to receive and process specific data attributes directly influences the efficacy of fraud risk assessments. By tailoring fraud detection strategies to the attributes that a PSP's system can handle, PSPs can optimise their risk analysis and decision-making processes, ensuring they leverage the most impactful data for fraud prevention.

Data Sharing Capabilities

The distinction between what data attributes PSPs can share versus what they can process acknowledges the operational diversity among PSPs. This understanding facilitates more efficient data exchanges, allowing PSPs to share meaningful information that aligns with each participant's technical capabilities and fraud prevention strategies.

EFD Whitelist Requests and Responses Implementation

To streamline the process of identifying mutually compatible data attributes, we introduce the EFD Whitelist Request and EFD Whitelist Response mechanism. Through a RESTful API, PSPs can query each other's current capabilities regarding the data attributes they can process and share. This API exchange enables PSPs to:

- Determine the intersection of receivable/processable and accessible/shareable attributes.
- Customize data exchanges to fit the sender and receiver's operational capabilities.

Strategic Considerations for PSPs

PSPs are encouraged to regularly review and update their data attribute handling capabilities in alignment with technological advancements and fraud detection needs. This continuous improvement approach ensures that the EFD ecosystem remains robust, adaptable, and effective in combating fraud across all participants. By embracing the EFD Whitelist mechanism, PSPs can foster a more interconnected and cooperative environment that accelerates the adoption of the EFD Service.

7 Legal Framework and Compliance for EFD Service

Legal Considerations

This section provides an overview of the legal considerations and compliance requirements essential for participants in creating an EFD Service. It summarises the contents of four key legal documents specifically being used for Pay.UK's EFD Service:

1. **EFD Admission Agreement:** This agreement details the criteria and process for PSPs to join the EFD Service, including rights and obligations.
2. **EFD Terms & Conditions:** Describes the operational, security, and data protection standards participants must adhere to.
3. **EFD Compliance Warranty Letter:** Participants' commitment to comply with specified requirements enhances the service's integrity.
4. **EFD Operating Manual:** Provides comprehensive guidelines on the EFD Service's operational aspects, ensuring participants understand and follow established procedures.

Together, these documents form the legal backbone of the EFD Service, ensuring participants operate within a structured, secure, and compliant framework. They are designed to facilitate the smooth setup and ongoing management of the EFD Service, emphasising the importance of adherence to legal and regulatory standards.

As we explore the adaptability of EFD Messaging Standards in diverse ecosystems within section 11, it's crucial to recognise that these legal frameworks and compliance requirements underpin the operational flexibility, ensuring that adaptions remain within structured, secure, and regulatory-compliant guidelines.

Privacy Regulations

Additionally, the following UK Governmental bills/laws enacted have been referenced as part of the alignment and structuring of the standard for compliance with:

- Data Protection & Digital Information Bill;
- Economic Crime and Corporate Transparency Act 2023 - Parliamentary Bills - UK Parliament
- Digital Markets Competition & Consumers Bill

Safeguarding Customer Information

Within the evolving landscape of digital transactions, the EFD Messaging Standard remains steadfast in its commitment to the highest customer data protection standards. In recognising the critical importance of safeguarding sensitive information, this standard aligns with stringent regulatory frameworks across jurisdictions, notably the United Kingdom, Europe and the United States.

In the UK, adherence to the Data Protection Act 2018, which encompasses the EU's General Data Protection Regulation (GDPR) principles, ensures that EFD Messaging upholds robust privacy and data protection measures. This commitment to privacy is reinforced by the Economic Crime and Corporate Transparency Act 2023 and the Digital Markets Competition & Consumers Bill, which establish a comprehensive protective shield around consumer data.

The EFD Messaging Standard also complies with international standards, aligning with the US's Gramm-Leach-Bliley Act (GLBA). This Act compels financial institutions to protect the privacy of consumer financial information, mandating safeguards against unauthorised access or use of customer data.

Elevating Collaboration through the Joint Protocol

The Joint Protocol is a cornerstone of the EFD Messaging Standard's legal and operational framework. This protocol is not merely a set of guidelines but a dynamic governance model that fosters collaboration among PSP participants. It plays a pivotal role in ensuring that the exchange of Enhanced Fraud Data (EFD) between participants is secure and compliant with prevailing privacy regulations.

Quarterly Collaborative Meetings

The essence of the Joint Protocol is brought to life through quarterly meetings facilitated by the EFD Service Provider's Standards Team. These sessions serve as a platform for PSP participants to collectively review the performance of the EFD Messaging system and the insightful analytical Management Information (MI) provided by the MI Sidecar messages. This collaborative environment enables participants to share best practices, discuss challenges, and adapt to emerging fraud patterns.

Adapting Data Attributes

One key focus of these meetings is evaluating the usage and effectiveness of data attributes within the EFD messages. Participants can propose adjustments to the attributes based on practical experiences and the evolving landscape of digital fraud. These adjustments might include introducing new data points that enhance fraud detection or revising existing ones to increase predictive value. By doing so, PSPs ensure that the EFD Messaging Standard remains relevant and effective in combating fraud.

Enhanced Responsiveness and Compliance

The Joint Protocol, underpinned by these quarterly meetings, underscores the EFD Messaging Standard's commitment to responsiveness and compliance. It allows for the EFD Service to be a living ecosystem that adapts to the needs of its participants while maintaining the highest standards of customer data protection. This adaptability is crucial for navigating the complexities of digital transactions and the regulatory environments in which PSPs operate.

Therefore, the Legal Framework and Compliance for EFD Service is not just a static set of guidelines but a living document that provides for a structured, secure, and compliant framework, adaptable to the evolving needs of its participants while maintaining the highest standards of customer data protection.

8 Provenance in Banking: Enhancing Trust through Verified Identity Attributes in EFD Messaging

In the digital age, our daily interactions, from unlocking our phones to conducting online banking, inherently rely on digital identity verification, often without our explicit recognition. In a recent public dialogue on trust in identity, a participant insightfully highlighted this ubiquitous yet unnoticed practice:

> ***"****It suddenly dawned on me how often we prove our ID without a second thought. (It happens) every day when we open our phones using face, fingerprint, or a four-digit code; open various accounts for shopping online; government apps such as HMRC; or online banking.****"***

This everyday reliance underscores the pivotal role of provenance in banking interactions, particularly within the Enhanced Fraud Data (EFD) Messaging framework.

In this context, provenance refers to the origin and historical verification of identity attributes maintained by banking institutions. Banks, as custodians of rich, verified customer data, play a crucial role in the EFD ecosystem. Their meticulous KYC processes ensure that each piece of identity data is not just a datum but a trusted attribute backed by rigorous verification. When integrated into EFD Messaging, these bank-verified identity attributes provide a robust foundation for trust, significantly enhancing fraud prevention capabilities. (for examples of how to use specific data attributes such as "Payment Value as Balance Percentage", "Average value of Credits in the last six months", and others, see the separate standards artefact within this collection called EFD Example Messages.

Incorporating provenance into EFD Messaging leverages banking systems' inherent trust and verification processes to authenticate identity attributes. Provenance fortifies the messaging standard against fraud and promotes the development of a seamless, secure digital identity ecosystem. By recognising the value of provenance, the EFD Messaging Standard addresses the technicalities of fraud prevention and embeds a deeper layer of trust in a bank's digital identities, fostering confidence in every transaction.

For further insights into the public dialogue on trust in digital identity services, refer to the UK government's findings report at https://www.gov.uk/government/publications/public-dialogue-on-trust-in-digital-identity-services/public-dialogue-on-trust-in-digital-identity-services-a-findings-report.

9 EFD Messages – What are they?

Overview

In the digital payment era, traditional messaging protocols like ISO8583 and ISO20022 fall short of addressing the nuances of fraud in today's transactions, where the anonymity of digital interactions obscures the true identity of transaction parties. This gap underscores a critical need for enhanced data exchange to foster security and trust. EFD Messages can now be pivotal in digital payment ecosystems, allowing financial institutions to exchange crucial information to detect and prevent fraud. These messages enhance transparency and trust between PSPs during transaction processes.

EFD Request Message

- **Purpose:** To assess risk, the EFD Request Message initiates the information exchange sent by a PSP seeking details on a payment's context.
- **Structure:** It includes transaction identifiers, account details, and context for the intended payment, structured in a standardised JSON format.
- **Flow:** Generated by either the sending or receiving PSP, this message is the first step in the peer-to-peer (PSP ⇔ PSP) information exchange.

EFD Response Message

- **Purpose:** In reply to a Request, the Response Message provides additional PII about the customer, aiding the requesting PSP's risk analysis.
- **Structure:** Contains detailed PII and account information, reinforcing the initial inquiry with enriched data insights, structured in a standardised JSON format.
- **Flow:** It can be issued by either PSP involved in the transaction directly responding to the Request message.

EFD MI Sidecar Message

- **Purpose:** Designed for analytics, the MI Sidecar captures data field names from EFD messages, aiding the service provider in understanding and improving the EFD Messaging Standard. They also provide granular understanding for EFD Service participants in the quarterly collaborative meetings.
- **Structure:** Focuses on metadata collection from Request and Response messages, formatted for easy analysis. *Note: Sidecar messages Do NOT contain any PII data.*
- **Flow:** Generated alongside Request and/or Response messages but sent directly to an agreed-upon EFD MI Provider endpoint for operational insights. EFD MI Sidecar messages are not exchanged between PSPs.

EFD Whitelist Request Message

- **Purpose**: This function enables a PSP to query another PSP's capability in handling specific EFD data attributes. This inquiry supports optimising the information exchange by identifying which attributes can be effectively shared and processed.
- **Structure**: Minimalistic, primarily constituting a query without needing detailed data attributes, adhering to a RESTful API GET request format.
- **Flow**: This is initiated by any PSP aiming to understand the data attribute capabilities of another PSP, facilitating a tailored approach to subsequent EFD Request and Response messages based on shared capabilities.

EFD Whitelist Response Message

- **Purpose**: This response provides a comprehensive list of data attributes the responding PSP can receive, process, access, and share. It ensures that subsequent EFD messaging exchanges are grounded in mutual data-handling capabilities.
- **Structure**: This is detailed and lists all the data attributes the PSP can engage with, including those for receiving, processing, and sharing, formatted in a standardised JSON structure for clarity and consistency.
- **Flow**: Generated in response to an EFD Whitelist Request Message, this message completes the capability discovery phase of the PSP-to-PSP (PSP ↔ PSP) communication, laying the groundwork for efficient and relevant data exchanges.

EFD Message Implementation Guides

The table below lists the names of separate implementation guideline documents for each message:

Guideline	Document Name
EFD Request	EFD_1_Request_Implementation_Guide_V0.21.pdf
EFD Response	EFD_2_Response_Implementation_Guide_V0.21.pdf
EFD MI Sidecar	EFD_3_MI_Sidecar_Implementation_Guide_V0.21.pdf
EFD Whitelist Request	EFD_4_Whitelist_Request_Implementation_Guide_V0.21.pdf
EFD Whitelist Response	EFD_5_Whitelist_Response_Implementation_Guide_V0.21.pdf

Table 2: EFD Message Implementation Guidelines - Document Names

Understanding EFD Messaging Flows

As the EFD Service evolves to meet the diverse needs of digital transactions, it is becoming clear that it should accommodate different operational frameworks that reflect the varied interactions between parties involved in a transaction. To this end, the EFD framework has been designed to support two distinct flows: the Two-Party Flow and the Three-Party Flow. Understanding these flows is crucial for stakeholders to appreciate the flexibility and applicability of EFD Messaging across different transaction scenarios.

9.1 Two-Party Flow

The Two-Party Flow is the foundational model of EFD Messaging, designed for direct transactions between a sending party (originator) and a receiving party (beneficiary), facilitated through their respective Payment Service Providers (PSPs). In this flow, when an originator initiates a payment, an EFD Request Message is generated by the originator's PSP and sent to the beneficiary's PSP. The beneficiary's PSP then responds with an EFD Response Message, providing the necessary information to validate the transaction and assess any fraud risk. This flow is streamlined and efficient, ideal for straightforward transactions where only two parties are directly involved.

Key Characteristics:

- Direct interaction between two PSPs
- Simplified message exchange for faster processing
- Optimal for straightforward, direct transactions

Remember: As described at the start of section 9, the EFD Request Message can be initiated by either the sending or receiving PSP. The originator PSP risk appetite might not trigger an EFD Request, wherein, in such a circumstance, the beneficiary's PSP could have a different risk appetite and decide to initiate an EFD Request Message back to the originating PSP. (see Use Case UC-1b)

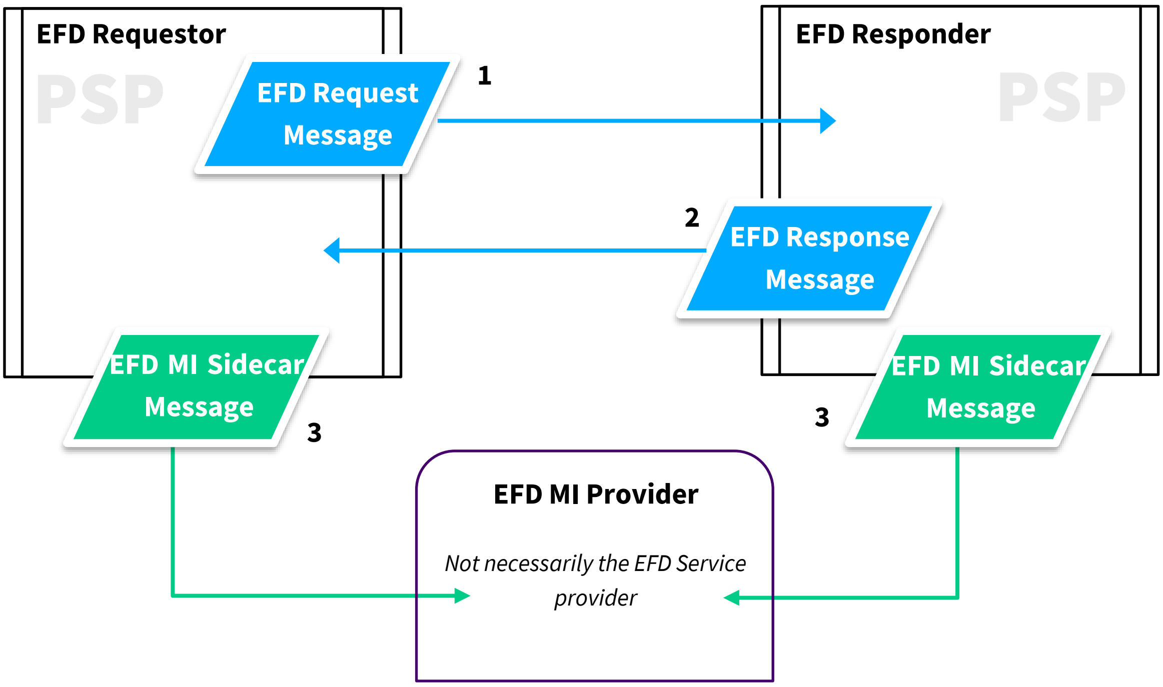


Figure 1: Two-Party Message Flow Diagram with additional Sidecar Message

#	Two-Party Message Flow Sequence Description
1	EFD Request sent directly to the Responder
2	EFD Response sent directly to the Requestor
3	EFD MI Sidecar summarising the data fields of the request or response sent to the EFD MI Provider endpoint for collection of granular management information analytics to help EFD Service participants holistically measure the success of the service

Table 3: Two-Party Message Flow Sequence

9.2 Three-Party Flow

The Three-Party Flow expands on the EFD framework to accommodate scenarios where an intermediary, such as a payment processor or an online marketplace platform, is involved in the transaction process and does not fit the direct model of the Two-Party Flow. This flow is introduced to address the complexities of transactions processed, for example, through online social marketplaces where the payment processor is critical in facilitating the transaction. In this model, an initial EFD Primer message[1] is generated by the intermediary and sent to the customer's PSP[2], starting a chain of communication that includes the intermediary as an essential participant in the fraud detection process. The EFD Request[2] and EFD Response[3] messages follow the normal flow from that point.

Key Characteristics:

- Involvement of an intermediary (Payment Processor or Marketplace)
- Introduction of the EFD Primer message to initiate the flow
- Enhanced flexibility to support complex transaction scenarios

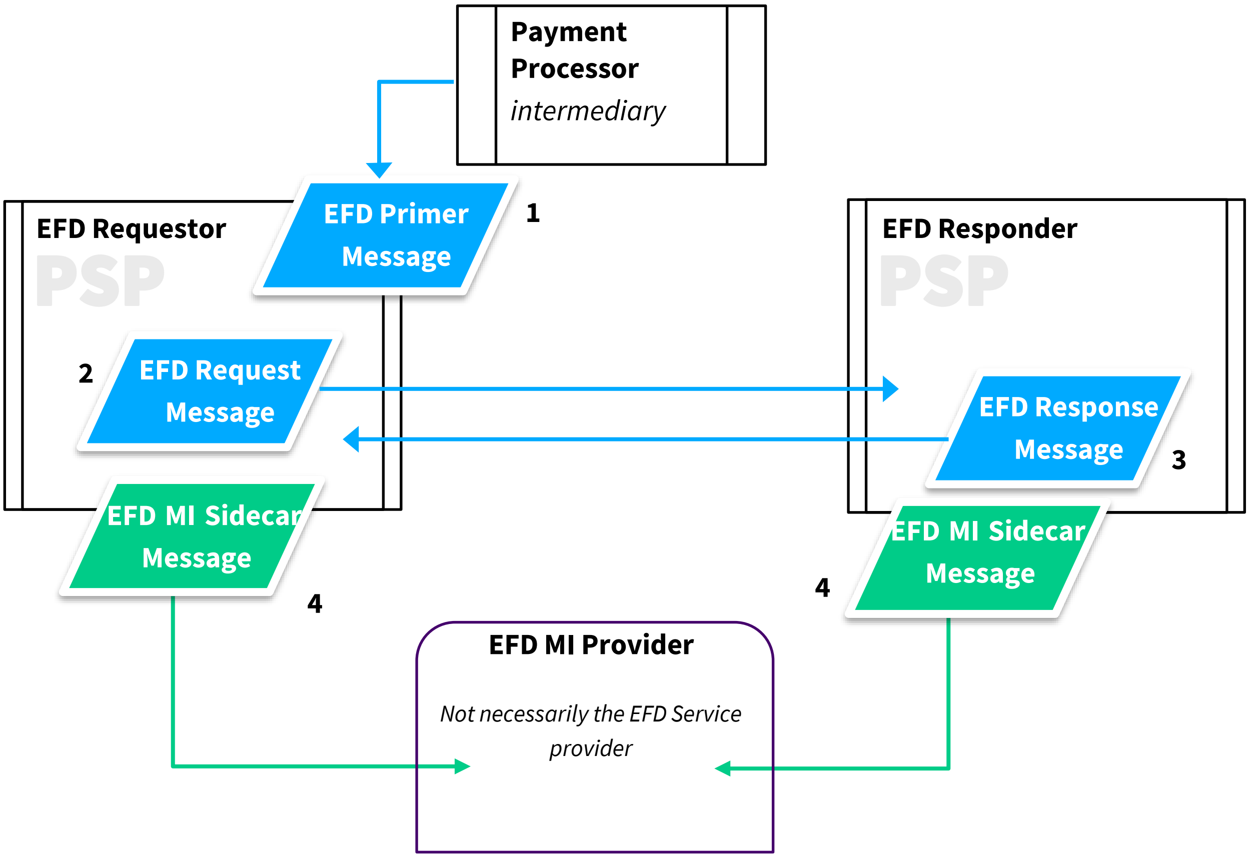


Figure 2: Three-Party Message Flow Diagram with additional Sidecar Message

#	Three-Party Message Flow Sequence Description
1	EFD Primer sent directly to the Requestor
2	EFD Request sent directly to the Responder
3	EFD Response sent directly to the Requestor
4	EFD MI Sidecar summarises the data fields of the request or response sent to the EFD MI Provider endpoint for collecting granular management information analytics to help EFD Service participants holistically measure the service's success. --- ***Note****: It is the decision of the EFD Service participants via the Joint Protocol to determine whether to enable the Payment Processor also to submit EFD MI Sidecar messages.*

Table 4: Three-Party Message Flow Sequence

Comparing the Flows

While both flows serve the critical purpose of enhancing fraud detection in digital transactions, their application depends on the nature of the transaction and the parties involved. The Two-Party Flow is straightforward and efficient, best suited for transactions with a clear, direct relationship between buyer and seller. The Three-Party Flow, on the other hand, offers the necessary complexity and flexibility for transactions that involve intermediaries, ensuring that the EFD Messaging framework can accommodate a broader range of transaction types without compromising on security or efficiency.

10 List of EFD Messaging Standard Artefacts

A suite of artefacts has been developed and made available through the Pay.UK Standards Source web portal to support the effective adoption and implementation of the Enhanced Fraud Data (EFD) Messaging Standard. These artefacts encompass various documents and tools to provide stakeholders with detailed guidance, implementation support, and reference materials necessary to successfully integrate and use the EFD Messaging Standard within their systems and processes.

The table below outlines the artefacts included in the EFD Messaging Standard release package:

#	Artefact Type	Description
0	EFD Messaging Standard Guide *(This guide)*	This comprehensive guide detailing the EFD Messaging Standard includes a conceptual overview, messages, data models, and use cases.
1	EFD Request Implementation Guide	Detailed guidelines for implementing and testing EFD Request messages.
2	EFD Response Implementation Guide	Detailed guidelines for implementing and testing EFD Response messages.
3	EFD MI Sidecar Implementation Guide	Guidelines for implementing and testing EFD MI Sidecar messages for management information.
4	EFD Whitelist Request Implementation Guide	Describes the simple sending of EFD Whitelist Request messages to query a PSP's data handling capabilities.
5	EFD Whitelist Response Implementation Guide	Describes how to create and send EFD Whitelist Response messages, detailing a PSP's data handling capabilities.
6	EFD OpenAPI Specifications	OpenAPI (Swagger) specifications to aid in API implementation for EFD message exchanges.
7	EFD Example Messages	Sample messages for each EFD message type to provide practical examples of message structures.
8	EFD Code Sets and Value Lists	Enumerations and value lists are used within EFD messages detailing permissible values for specific data attributes.
9	EFD Implementation Checklist	A checklist to assist organisations in ensuring all necessary steps are taken for implementation.
10	EFD Glossary	Provides a comprehensive list of terms and definitions used throughout the EFD Messaging Standard documentation, aiding in understanding key concepts and terminology.

Table 5: List of EFD Message Standard Artefacts In The Release Package

These artefacts facilitate a comprehensive understanding and efficient implementation of the EFD Messaging Standard. Stakeholders are encouraged to review each artefact in detail to ensure a thorough grasp of the standards, protocols, and procedures necessary for successful EFD message exchanges.

11 Adapting EFD Messaging Standards for Diverse Ecosystems

Overview

In the evolving landscape of digital payments, the necessity for a robust framework to combat fraud cannot be overstated. The EFD Messaging Standards emerge as a beacon of innovation, designed to bridge the gap left by traditional payment protocols. However, the true strength of EFD Messaging lies in its comprehensive data-sharing capabilities and inherent adaptability to diverse ecosystems. This section delves into the philosophical underpinnings and strategic design choices that render the EFD Messaging Standards a versatile tool capable of being tailored to meet the unique requirements of various payment ecosystems in any region of the world while upholding the highest levels of security and compliance.

Design Philosophy

At the core of the EFD Messaging Standards is a design philosophy that champions flexibility, interoperability, and the foresight to anticipate and adapt to emerging threats. Recognising that the battle against fraud is dynamic, the standards are crafted to be a solution and a sustainable framework that evolves in tandem with fraudsters' changing tactics and the financial sector's technological advancements.

Key to this adaptability is the separation of the messaging standards from their operational application. This strategic distinction allows the EFD Messaging Standards to serve as a foundational protocol - a lingua franca for secure data exchange - while granting ecosystems the latitude to customise their implementation. Whether adjusting to regulatory nuances, integrating with existing systems, or innovating to address new forms of fraud, the standards provide a stable base from which diverse operational models can flourish.

Furthermore, this design philosophy embeds the principle of extensibility at its heart and anticipates the future needs of payment ecosystems. The standards are structured to allow for the seamless introduction of new data elements, message types, and security protocols without disrupting existing operations. This forward-looking approach ensures that the EFD Messaging Standards remain a relevant and powerful tool against fraud, adaptable to the ever-evolving digital payment landscape.

Operational Flexibility

The EFD Messaging Standards are designed with a profound understanding that the digital payments landscape is diverse and constantly evolving. The standards champion operational flexibility by recognising different ecosystems' unique challenges and requirements. This flexibility ensures that entities across the financial spectrum, from global banks to local payment service providers, can tailor the standards to fit their operational needs and fraud prevention strategies. By accommodating varying levels of technology adoption, regulatory environments, and market demands, the EFD Messaging Standards provide a versatile foundation for secure and efficient data exchange.

Multiplicity of EFD Services

It is important to recognise that multiple providers of EFD Services can exist within the same or different regions. These providers may cater to specific scenarios and use cases, allowing banks and other financial institutions to subscribe to the services that best meet their needs. For example, one EFD Service may set its rules to fulfil only use case UC-1a, focusing on a particular aspect of fraud prevention. At the same time, another might encompass both UC-1a and UC-1b, offering greater flexibility in fraud detection and response.

This differentiation means a bank could subscribe to both services to maximise its fraud prevention capabilities. In contrast, another bank might prefer to engage with only one service that aligns with its internal systems' capacities and strategic objectives. For instance, Bank A might find value in subscribing to a service that includes UC-1b due to its ability to adapt to this broader use case. In contrast, Bank B may opt for a service that focuses solely on UC-1a if its systems are not readily conducive to handling the complexities of UC-1b.

This realisation highlights the EFD Messaging Standards' inherent adaptability, designed for today's requirements and the anticipated diversity of future digital ecosystems. It underscores our commitment to offering choices that respect the individual operational strategies of our subscribers and their ongoing battle against fraud in all its forms.

Future-proofing the Standards

In the fast-paced world of digital payments, staying ahead of fraudsters requires not just vigilance but innovation. The EFD Messaging Standards are inherently designed to be future-proof, with built-in mechanisms for updates and enhancements that respond to new threats, technological advancements, and shifts in regulatory landscapes. The standards are positioned to adapt and grow through an ongoing dialogue with stakeholders and an agile approach to standard evolution. As the digital payments ecosystem evolves, so will the standards, maintaining their relevance and effectiveness in safeguarding the integrity of financial transactions.

12 EFD Service Use Cases

Foundational Use Case

In the evolving landscape of digital payments, the Enhanced Fraud Data (EFD) Service represents a significant step forward in securing transactions and fostering trust across the financial ecosystem. It was developed under the stewardship of Pay.UK, the EFD Service is designed to address the pressing challenge of real-time payment fraud through innovative messaging patterns, collaboration between financial institutions, and rigorous adherence to privacy and security standards.

The cornerstone of this initiative is **Use Case 1: Fraud Detection in Real-time Payments, which is** below. This use case is a testament to the collaborative efforts of UK Finance, UK Banking associations, and Pay.UK. This use case is not just a blueprint but a live, operational example of how EFD Messaging can be effectively deployed to safeguard financial transactions against fraud, offering an immediate and tangible benefit to the financial industry.

Aspirational Use Cases

Beyond this foundational use case, we recognise the potential for EFD Messaging to transform other areas of the financial landscape. The subsequent use cases outlined in this section are aspirational, designed to inspire and encourage exploration into the broader applications of EFD Messaging. These scenarios envision a future where EFD's capabilities extend into mitigating online advertising fraud, enhancing bulk transaction processing (incl. BACS and OB Bulk for SME's), leveraging digital identities, and more.

Notably, these aspirational use cases are proposed not as immediate action items but as potential pathways for innovation. They serve as a call to action for financial institutions, banking associations, regulators, and online marketplaces to consider what could be possible when we harness the full potential of EFD Messaging. We aim to foster an environment of collaboration and co-working, where stakeholders across the financial industry can come together to explore, develop, and realise the benefits of EFD in addressing the complex challenges of fraud in an interconnected digital world.

As we present these use cases, we invite all stakeholders to approach them with an open mind and a collaborative spirit. The journey ahead offers numerous opportunities for innovation, enhanced security, and improved customer trust. Together, we can work towards realising the full potential of EFD Messaging, setting new standards for fraud prevention in the digital age.

Use Case 1: Fraud Detection in Real-time Payments

NOTE: This use case is the approved UK Finance and UK Banking use case for EFD Messaging (AKA. Day 1) and is being developed by Pay.UK for their EFD Service.

Objective:

To enhance PSPs' capabilities in detecting and preventing fraudulent transactions at the start of customers' real-time payment processing requests (i.e., a customer's intent to pay).

Scenario Descriptions:

Use EFD Messaging for immediate transaction analysis and decision-making, improving real-time fraud detection, purely for PSP use.

a. **Sending PSP sends EFD Request Message**

Use Case 1a (UC-1a): For example, a sending PSP is a financial institution(FI) whose customer instructs them to transfer funds to a receiving party, which the sending PSP perceives as a risk. As a result, the sending PSP generates an EFD Request Message [1] and sends it to the receiving party FI [2] (receiving PSP) to enquire about the receiving party's account enhanced data details.

Upon the EFD Request Message arriving at the receiving party FI, they, in turn, match the request to their customer account[3], generate the EFD Response Message with enhanced data [4] and send that message back to the sending PSP [5].

At this point the Sending PSP combines the additional EFD data from Receiving PSP, and assesses[6] low risk of this payment being fraudulent and goes ahead with disbursement [7].

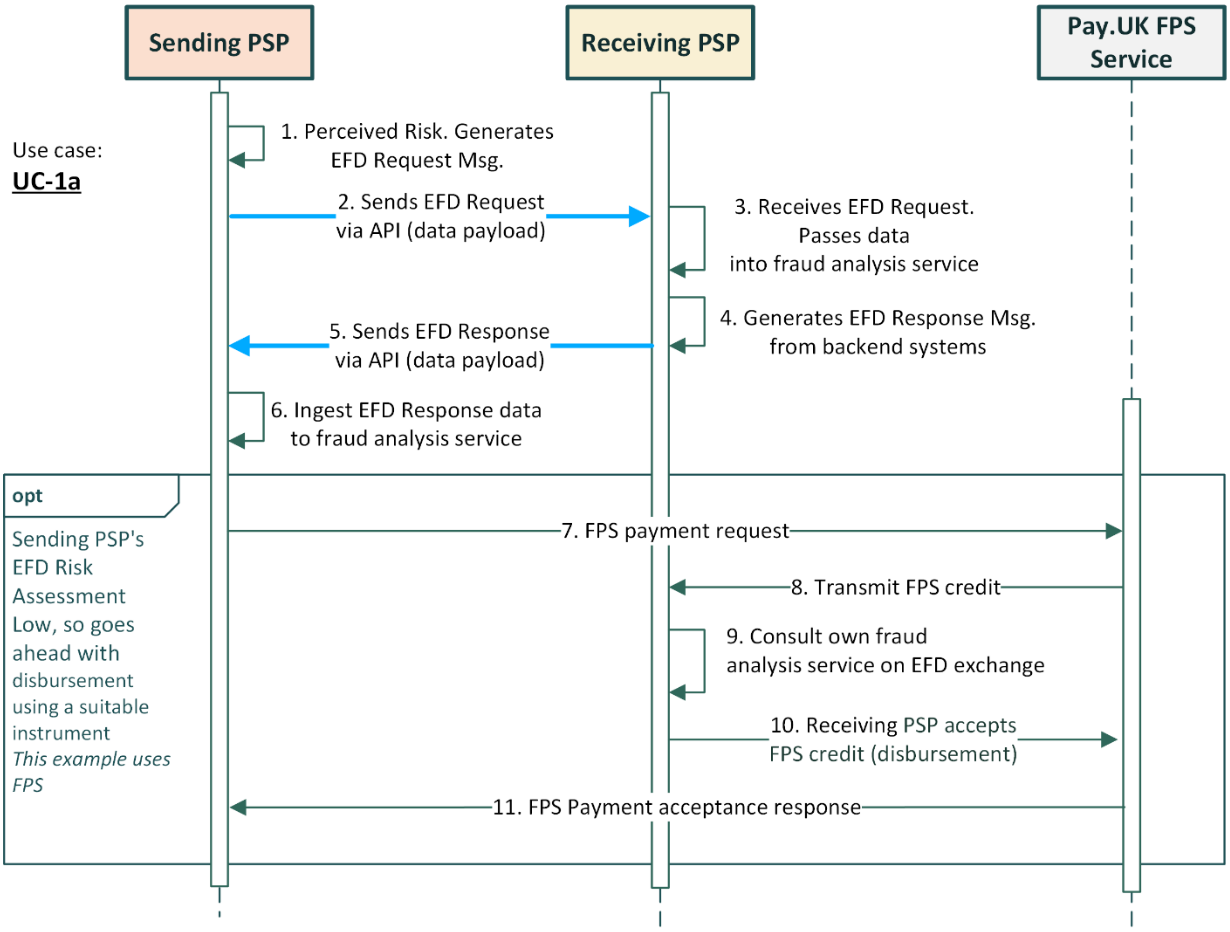

Sending PSP
Receiving PSP
Pay.UK FPS Service
Use case:
UC-1a
1. Perceived Risk. Generates EFD Request Msg.
2. Sends EFD Request via API (data payload)
3. Receives EFD Request. Passes data into fraud analysis service
4. Generates EFD Response Msg. from backend systems
5. Sends EFD Response via API (data payload)
6. Ingest EFD Response data to fraud analysis service
opt
Sending PSP's EFD Risk Assessment Low, so goes ahead with disbursement using a suitable instrument
This example uses FPS
7. FPS payment request
8. Transmit FPS credit
9. Consult own fraud analysis service on EFD exchange
10. Receiving PSP accepts FPS credit (disbursement)
11. FPS Payment acceptance response

Figure 3: UC-1a Sequence Diagram

b. **Receiving PSP sends EFD Request Message**

Use Case 1b (UC-1b), Where, for example, a sending PSP transfers funds without conducting an EFD check[1]. In this example, the receiving PSP receives the payment credit notification[2] but wants more information before posting the funds to their customer's account,[3] so generates an EFD Request Message including enhanced account data of their customer (client) and sends the request message[4] to the sending PSP whilst also accepting the payment credit[5]

Upon the sending PSP receiving the EFD Request Message[6], the Sending PSP generates an EFD Response Message[7] and, although they also receive the PSO's Payment Acceptance Response notification[8], sends the EFD Response Message[9] back to the Receiving PSP under the obligations of the EFD Service, at which point the Receiving PSP ingests the enhanced data insights[10] of the message and decides[11] whether to post the funds to their customer account, or return the funds to the sender using whatever means are available to the PSP based upon the payment instrument being used.

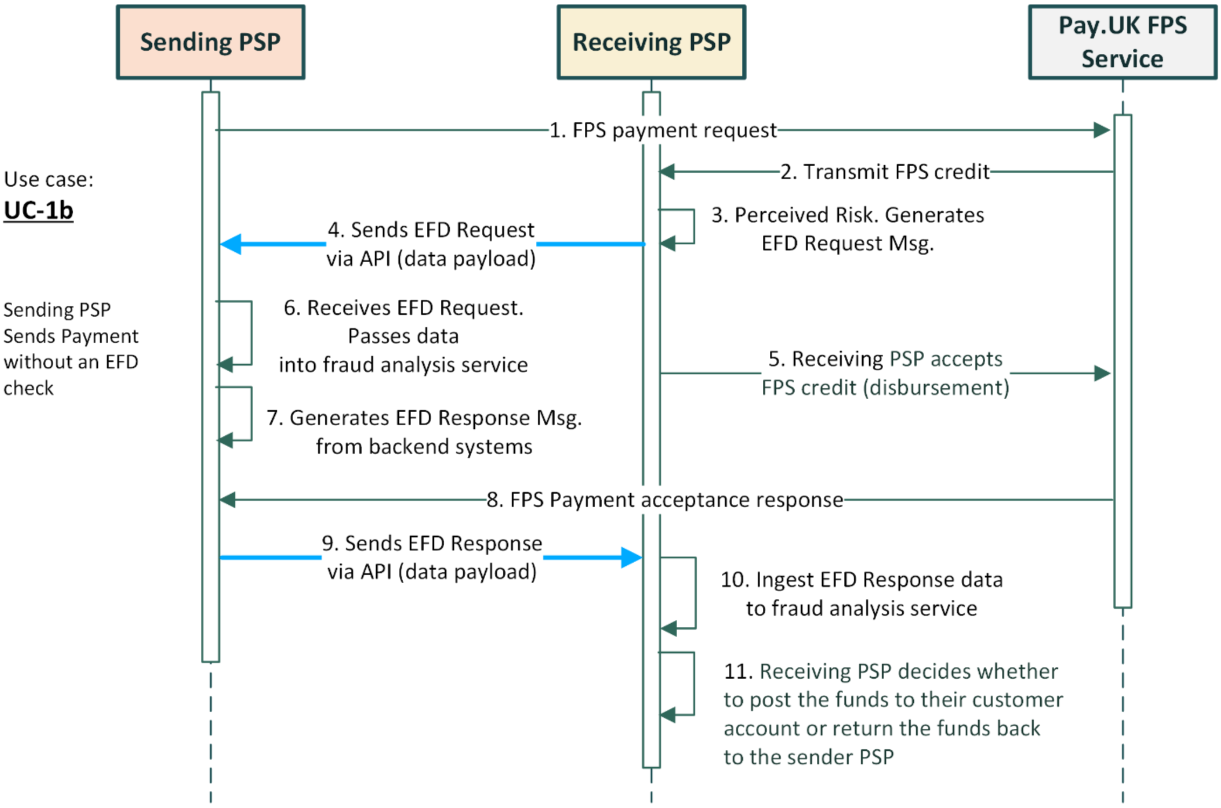

Sending PSP
Receiving PSP
Pay.UK FPS Service
Use case:
UC-1b
Sending PSP Sends Payment without an EFD check
1. FPS payment request
2. Transmit FPS credit
3. Perceived Risk. Generates EFD Request Msg.
4. Sends EFD Request via API (data payload)
5. Receiving PSP accepts FPS credit (disbursement)
6. Receives EFD Request. Passes data into fraud analysis service
7. Generates EFD Response Msg. from backend systems
8. FPS Payment acceptance response
9. Sends EFD Response via API (data payload)
10. Ingest EFD Response data to fraud analysis service
11. Receiving PSP decides whether to post the funds to their customer account or return the funds back to the sender PSP

Figure 4: UC-1b Sequence Diagram

Benefits:

These use case scenarios 1a and 1b focus on a customer's intent to pay a payee, enabling PSPs at both ends of the payment chain to derive context surrounding the intent and reason for payment from the supplementary data included in the request and response messages. The context will either increase or decrease the PSP's trust in the validity of the payment intention, resulting in a decision as to whether the sending PSP continues with the disbursement and whether the receiving PSP posts the received funds to their customer's account or not.

***NOTE**: Use Case 1 is the first solution implemented as an EFD Service by Pay.UK and UK PSPs. This use case is fully controlled by PSPs using peer-to-peer (P2P) infrastructure with zero interaction or awareness of a PSP's customer.*

Use Case 2: Enhancing Bulk Transaction Processing with EFD

Objective:

Integrating EFD Messaging within the UK BACS bulk transaction processing system enables corporate entities and banks to gain enhanced insights for fraud detection and transaction validation without altering the traditional BACS file submission process.

Scenario Descriptions:

a. **Utilisation of BACS Bureaus for EFD Message Submission**

   Use Case 2a (UC-2a) Engages BACS Bureaus to manage the submission of traditional BACS files and parallel EFD messages. This ensures that the enhanced fraud data capabilities are accessible to corporates without direct BACS access or those preferring to use bureau services for transaction processing.

b. **Corporate-PSP Collaboration for Fraud Detection**

   Use Case 2b (UC-2b) Enables corporates to submit EFD Messages to their Receiving PSPs **via** their Sending PSPs. This approach facilitates a feedback loop where PSPs can analyse the additional data provided by corporates to validate the payment intention more accurately.

c. **Utilisation of BACS Bureaus for EFD Message Submission**

   Use Case 2c (UC-2c) Engages BACS Bureaus to manage the submission of traditional BACS files and parallel EFD messages. This ensures that the enhanced fraud data capabilities are accessible to corporates without direct BACS access or those preferring to use bureau services for transaction processing.

Note:

[Use case 2 is an aspirational implementation for EFD. Sequence diagrams not undertaken at this time]

Benefits:

This use case significantly augments the fraud detection capabilities during bulk transaction processing by introducing a parallel data exchange channel via EFD Messaging. By providing PSPs and banks with additional context and insights into each transaction, the validity of payment intentions can be assessed more accurately, enhancing trust in the payment process. Integrating EFD messages with traditional BACS submissions, facilitated using the Sidecar** pattern, ensures minimal operational impact on the existing transaction submission process. This innovative approach not only strengthens the security and integrity of bulk payments but also supports the sustainable growth of the digital payments ecosystem by fostering a proactive stance against fraud.

** Sidecar pattern explainers

Microsoft description https://learn.microsoft.com/en-us/azure/architecture/patterns/sidecar

Istio https://istio.io/latest/docs/reference/config/networking/sidecar/

Kubernetes https://kubernetes.io/docs/concepts/workloads/pods/

Use Case 3: Empowering Fraud Prevention through Digital Identity Verification in EFD Messaging

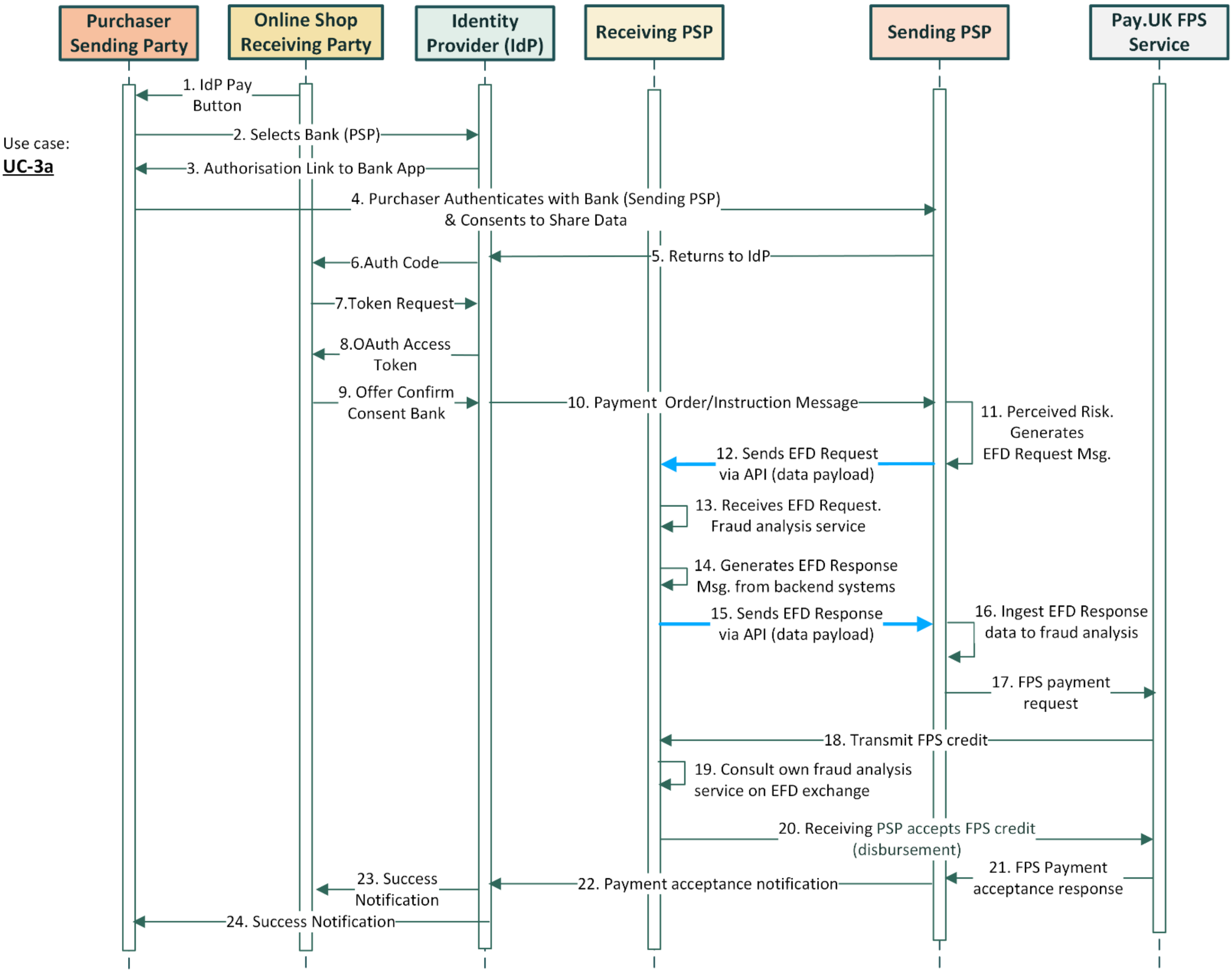
Objective:

To enhance the accuracy and reliability of fraud detection mechanisms within an EFD Service by incorporating (advanced) verified digital identity information, ensuring that payment transactions are initiated and received by verified entities.

Scenario Descriptions:

a. **Integration of Verified Claims**

Use Case 3a (UC-3a) Leverages OpenID Connect for Identity Assurance 1.0 to integrate verified claims about end-users into EFD Messaging, enabling PSPs to ascertain the identity of parties involved in a transaction with high assurance.



Purchaser Sending Party
Online Shop Receiving Party
Identity Provider (IdP)
Receiving PSP
Sending PSP
Pay.UK FPS Service
Use case: UC-3a
1. IdP Pay Button
2. Selects Bank (PSP)
3. Authorisation Link to Bank App
4. Purchaser Authenticates with Bank (Sending PSP) & Consents to Share Data
5. Returns to IdP
6.Auth Code
7.Token Request
8.OAuth Access Token
9. Offer Confirm Consent Bank
10. Payment Order/Instruction Message
11. Perceived Risk. Generates EFD Request Msg.
12. Sends EFD Request via API (data payload)
13. Receives EFD Request. Fraud analysis service
14. Generates EFD Response Msg. from backend systems
15. Sends EFD Response via API (data payload)
16. Ingest EFD Response data to fraud analysis
17. FPS payment request
18. Transmit FPS credit
19. Consult own fraud analysis service on EFD exchange
20. Receiving PSP accepts FPS credit (disbursement)
21. FPS Payment acceptance response
22. Payment acceptance notification
23. Success Notification
24. Success Notification

Figure 5: UC-3a Sequence Diagram

b. **Dynamic Request of Verification Data**

Use Case 3b (UC-3b) Utilises the technical mechanisms outlined in the OpenID specification to request specific verification data relevant to the transaction context. This includes any number of trust frameworks compliance, verification processes, and evidence types supported by OpenID Providers (OPs).

c. **Cross-Border Transaction Authentication**

Use Case 3c (UC-3c) For transactions involving parties from different EU member states, PSPs rely on the interoperability provided by eIDAS to recognise and validate electronic identifications across borders, enhancing trust and security in cross-border transactions.

d. **Operational Flexibility with Aggregated and Distributed Claims**

Use Case 3d (UC-3d) For transactions involving parties from different EU member states, PSPs rely on the interoperability provided by eIDAS to recognise and validate electronic identifications across borders, enhancing trust and security in cross-border transactions.

Note:

[Use cases 3a, 3b, 3c, and 3d are aspirational implementations for EFD. Sequence diagrams for 3b, 3c, and 3d have not been undertaken at this time]

Benefits:

Incorporating digital identity verification into EFD Messaging offers a multifaceted enhancement to fraud prevention efforts. By integrating verified claims, EFD Messaging can significantly reduce the risk of fraudulent transactions by ensuring that all parties involved in a transaction are accurately identified and verified. This integration not only bolsters the security of digital payments but also aligns with regulatory compliance requirements, such as AML and KYC, by providing a robust mechanism for identity verification. Furthermore, adopting privacy and security standards protects end-user data, fostering trust in the digital payment ecosystem. Operational flexibility, achieved through handling aggregated and distributed claims, ensures that EFD Messaging can be tailored to specific needs and regulatory environments, enhancing interoperability and effectiveness across the financial sector.

UC-3b's integration into EFD specifically for eIDAS-compliant digital identity verification significantly improves the PSPs' capabilities to authenticate the identities of parties involved in electronic transactions securely and reliably. This approach aligns with regulatory requirements, enhances trust in digital transactions, reduces the risk of fraud, and supports a seamless user experience across the European Digital Single Market.

Generally, use case 3 underscores the critical role of digital identity verification in modernising and securing digital payment systems, positioning EFD Messaging as a pivotal tool in the ongoing fight against payment fraud.

Use Case 4: EFD's Strategic Approach to Mitigating Online Marketplace Fraud (Zero Trust Multi-party Ecosystems)

Objective:

To ensure secure and fraud-resistant transactions within an online marketplace environment, leverage Enhanced Fraud Data (EFD) messaging in conjunction with a Payment Processor (PP) in scenarios excluding direct trust relationships within platforms.

Example Problem Statement:

A social media marketplace advertising platform brings buyers and sellers together to facilitate sales of goods. In this example, bad actors posing as vendors fraudulently advertise products for sale with no intent to supply. There are multiple parties:

I. **Marketplace provider (MktPl):** Provides the advertising platform, shopping basket, and universal payment UI. The T&Cs absolve MktPl of any liability between parties. MktPl receives the sales revenue and passes it to sellers minus marketplace fees.

II. **Payment Processor (PP):** Has an agreement with MktPl to process the sales via card payments, Pay-by-Bank, etc. Passes sales revenue to MktPl less processing fees.

III. **Seller (Vendor):** Lists their products on the advertising platform for sale. Receives sales revenue from MktPl minus platform fees. Sends products to customers.

IV. **Buyer (Purchaser):** A member of the MktPl who buys products from vendor advertisements on the MktPl. Pays MkPl via PP and waits for products to arrive.

V. **PSPs:** three different PSPs, each having an account relationship with one of the parties, the MktPl PSP, Vendor PSP and Purchaser PSP

Scenario Description:

This scenario underscores the significance of the EFD framework in scenarios where direct trust relationships between buyers, sellers, and their respective PSPs may not exist, highlighting its potential to safeguard transactions in a digitally interconnected marketplace.

a. <u>EFD Primer Message by Payment Provider enabling EFD Service Benefits</u>

Use Case 4a (UC-4a) enables online marketplace customers to progress with the payment flow at the checkout, knowing that their PSP is actively checking on the status of the vendor the purchaser is buying from in the marketplace.

- When the purchaser submits their payment details [1] to the PP, the PP [2] also receives from MktPl [3] their merchant account details, vendor bank details, transaction reference, price, etc. The PP generates [4] the initial EFD Primer message, sets the stage for the EFD three-party flow, and forwards [5] this to the Sending PSP via API.
- The Purchaser’s Sending PSP receives the EFD Primer message *(see 9.1.1 EFD Primer message)* from the PP, perceives a risk [6] and generates an EFD Request message directed [7] at the Vendor's Receiving PSP to verify the vendor's account status and assess fraud risk.
- The Vendor's receiving PSP checks [8] the message [9] and responds with an EFD Response [10] message, providing the required verification details for risk assessment to the Customer's PSP [11].

- Based on the EFD Response, the Sending PSP decides whether to authorise or reject the payment, informing the PP of the decision [12]. The PP processes the payment and then updates the customer (via MktPl UI [13]) and MktPl [14] systems about the payment status.
- Upon payment authorisation, the PP forwards the net payment to the MktPl PSP account. MktPl subsequently pays the vendor for the sales, deducting its sales commission. The vendor ships the sold products directly to the customer's address.

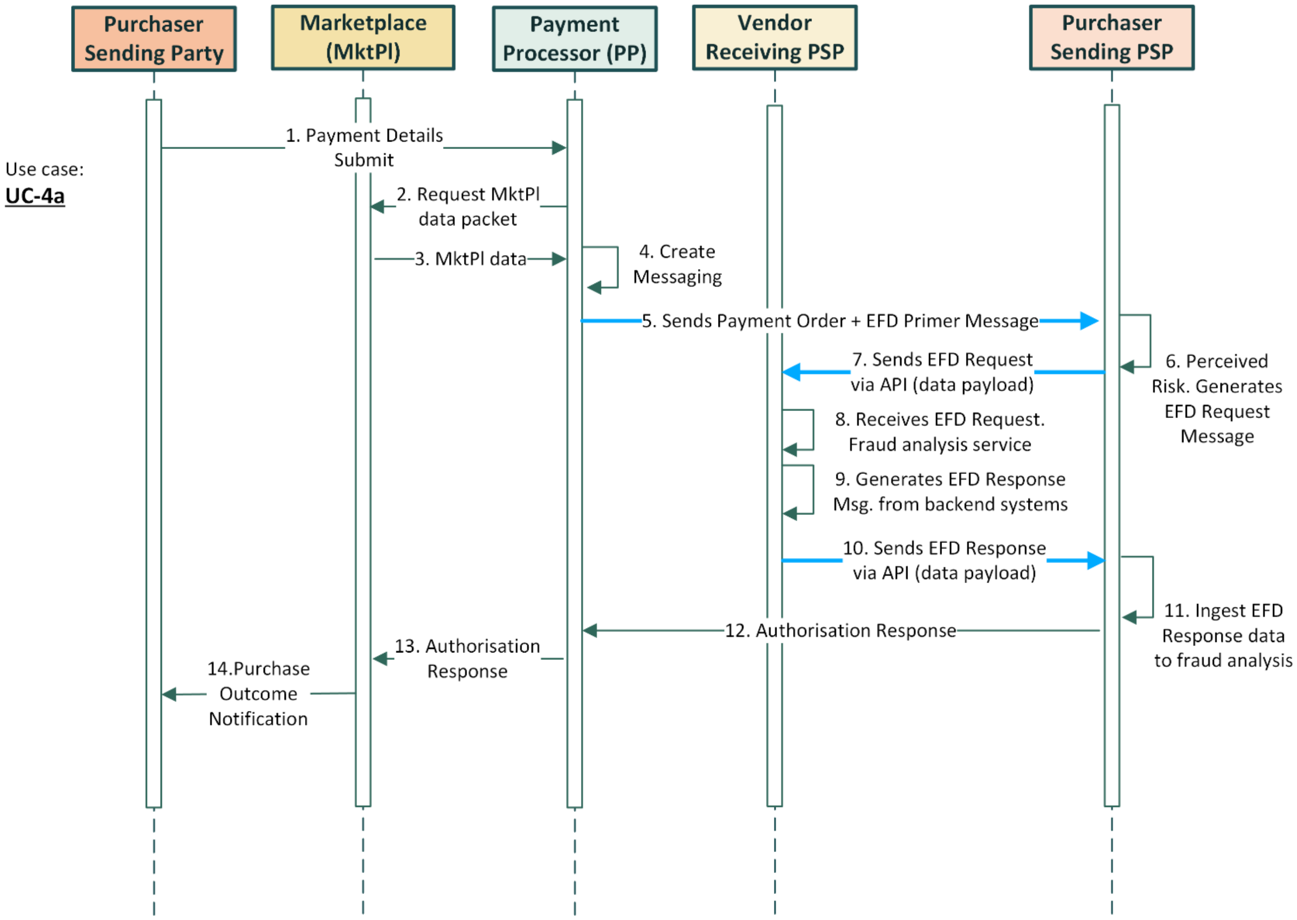

Purchaser Sending Party
Marketplace (MktPl)
Payment Processor (PP)
Vendor Receiving PSP
Purchaser Sending PSP
Use case:
UC-4a
1. Payment Details Submit
2. Request MktPl data packet
3. MktPl data
4. Create Messaging
5. Sends Payment Order + EFD Primer Message
6. Perceived Risk. Generates EFD Request Message
7. Sends EFD Request via API (data payload)
8. Receives EFD Request. Fraud analysis service
9. Generates EFD Response Msg. from backend systems
10. Sends EFD Response via API (data payload)
11. Ingest EFD Response data to fraud analysis
12. Authorisation Response
13. Authorisation Response
14.Purchase Outcome Notification

Figure 6: UC-4a Sequence Diagram

Note:

[Use case 4 is an aspirational implementation for EFD. The sequence diagram assumes the payment processor (PP) enhances its data packet submission requirement to support a three-party EFD messaging flow]

Benefits:

The sequence described above demonstrates the understanding of the necessary steps to implement EFD messaging in a three-party flow. This includes the critical role of the PP in generating the initial EFD Primer message and the subsequent interactions between customer and vendor PSPs to assess and authorise the transaction.

Overall, this scenario provides a clear and coherent framework for integrating EFD messaging within the existing operational flows of online marketplaces, addressing the challenges of online advertising fraud and enhancing transaction security. This approach not only aligns with the objectives of the EFD system but also adapts it to the complexities of modern digital commerce, showcasing a strategic application of the EFD messaging pattern to bolster trust and mitigate fraud in online transactions.

- **Enhanced Trust and Transparency**: By making the payment process transparent and secure, the confidence of both buyers and sellers in the marketplace is bolstered, encouraging more transactions and participation.
- **Operational Efficiency**: The streamlined process for payment authorisation and fund distribution ensures that transactions are processed efficiently, enhancing buyers' and sellers' overall user experience.
- **Regulatory Compliance**: The use of EFD mechanisms helps in meeting regulatory requirements related to fraud detection and prevention, thereby maintaining the marketplace's reputation and operational integrity.
- **Expand Payment Instrument Options:** This scenario allows payment processors to expand beyond card-based payments and include secure account-to-account (A2A) payments and what is termed **Pay-By-Bank**.

Implementation Considerations:

- **Privacy and Data Protection:** Utilising the new privacy regulations relating to fraud in acts such as the Economic Crime and Corporate Transparency Act 2023 helps ensure compatibility and compliance with GDPR, especially in handling and sharing sensitive financial and personal information. Limiting access and decision-making purely to regulated PSPs, etc.
- **Technical Integration:** The seamless integration of EFD messaging patterns with PPs and PSPs ensures minimal disruption to the existing payment processing workflow.
- **Stakeholder Collaboration:** Effective communication and cooperation between marketplace platforms, payment processors, PSPs, and vendors to ensure alignment with the EFD implementation strategy and objectives.

12.1 EFD Primer message:

The EFD Primer message is a strategic addition to the EFD Messaging framework, specifically tailored to address the unique challenges and requirements of processing transactions in online marketplaces.

The EFD Primer message is an initial step in the three-party flow involving the Payment Processor (PP), purchaser’s PSP, and vendor's PSP. It ensures that all relevant payment details, including vendor account information, are captured and communicated effectively to initiate the EFD messaging sequence with the Sending PSP. It represents an innovative approach to enhancing transaction security, fraud prevention, and regulatory compliance in a digital commerce environment.

13 ISO20022 Naming Convention and Abbreviations

Why Align with ISO20022?

Adopting the ISO20022 Naming Convention within the EFD Messaging Standard provides a foundation for global interoperability and consistency in financial communications. It aligns our data attributes in an internationally recognised and widely understood manner within the financial industry.

Benefits of ISO20022 Abbreviations

- **Standardization**: This ensures that our EFD messages are structured in accordance with a globally recognised framework, facilitating cross-border and cross-system communication.
- **Clarity:** With the ISO20022 Naming Convention, we balance comprehensive understanding and streamlined processing. While its comprehensive names provide detailed understanding, its abbreviations allow easy implementation and streamlined data processing without sacrificing meaning.
- **Efficiency**: The use of abbreviations in the ISO20022 Naming Convention significantly reduces message size and complexity, leading to faster processing and reduced storage requirements. This excitingly enhances your work processes without compromising data integrity or richness.

Usage of ISO XML Tag Abbreviations

By compressing the long-hand ISO data attribute names using the ISO XML Tag Abbreviation list (as found on the ISO20022 website), we maintain the robustness of ISO20022 while enhancing the agility and efficiency of our EFD Messaging Standard.

Registration with ISO

The Pay.UK Standards Authority is proactively engaging with the ISO framework by submitting a Business Justification for the EFD Messaging Standard to be registered within the International catalogue. This step signifies our commitment to maintaining best practices and ensuring our standards are relevant and sustainable within the evolving global payments landscape.

14 Data Model

Introduction to the Data Model

The cornerstone of any robust digital transaction system lies in its ability to process and manage data accurately, securely, and efficiently. Within Enhanced Fraud Data (EFD) Messaging, the data model is the architectural blueprint underpinning this capability. It is designed to ensure that every piece of information exchanged between Payment Service Providers (PSPs) adheres to the highest standards of accuracy and integrity and aligns with the overarching goal of mitigating fraud in digital payments.

The EFD data model encompasses a comprehensive structure that details the types of data exchanged, the relationships between different data elements, and the rules governing these interactions. By meticulously defining how data is organised, stored, and accessed, the model provides a clear framework for PSPs to implement EFD Messaging effectively and cohesively.

This section aims to demystify the EFD data model, offering insights into its components, functionalities, and how they collectively facilitate a secure, transparent, and efficient fraud detection mechanism. Through this exploration, stakeholders across the digital payment ecosystem will gain a deeper understanding of the data model's pivotal role in enhancing the reliability and efficacy of EFD Messaging services.

Mandatory and Optional Data Attributes

In Enhanced Fraud Data (EFD) Messaging, data attributes play a critical role in the secure and accurate processing of transactions. To ensure the effectiveness of this process, the EFD Messaging Standard categorises data attributes into two distinct groups: Mandatory (M) and Optional (O).

- **Mandatory Data Attributes (M):** These essential data fields must be provided in every EFD message. They form the core information required to validate and process a transaction securely. These attributes are non-negotiable and serve as the foundation upon which the integrity of the transaction is built.
- **Optional Data Attributes (O):** These attributes provide supplementary information that can enhance the understanding of a transaction but are not required for its execution. Including these fields is at the discretion of the sending party and depends on the transaction's specific use case, context, or additional security needs.

You will find the M/O Condition set to 'M' in our entity definitions for mandatory data attributes. These fields must be consistently present and accurately populated in each message. On the other hand, optional data attributes, indicated by an 'O,' offer PSPs the ability to provide additional context where beneficial. By adhering to this structured approach, the EFD Messaging Standard ensures the right balance between the minimal data requirement for transaction security and the flexibility to include additional details where they add value.

The EFD Implementation Guides feature a Mandatory and Optional condition

EFD Message guides contain a column "**Mult**" within the schema data information identifying the condition of each data attribute for Mandatory or Optional using the following pattern:

[1..1] = Mandatory data element needing to appear within the EFD Message

[0..1] = Optional data element if it isn't available, then the EFD Message can be sent without it.

Key Entities and Primary Data Structure

14.1 Party

- **Description**: The party represents individuals or entities involved in financial transactions. It is central to the EFD system, serving as the primary subject for KYC processes and risk assessments.
- **Attributes**: Includes identifiers (e.g., customer ID), personal details (name and date of birth for individuals; legal name and registration details for entities), and contact information.
- **Relationships**: These are connected to Accounts (ownership or signatory authority), Transactions (as originators or beneficiaries), and Identity (digital identity verification records).

14.2 Identity

- **Description**: Organizes information related to Parties' digital and physical identity verification, aligning with contemporary KYC and digital identity frameworks.
- **Attributes**: Biometric data, document scans (passport, driver's license, etc.), electronic verification records, verification measures and compliance status.
- **Relationships**: Directly linked to the Party, reinforcing the authenticity of the Party's identity.

14.3 Account

- **Description**: Details the formal banking relationships established by Parties to access financial products and services.
- **Attributes**: Account number, account type (checking, savings, loan, etc.), opening date, and status.
- **Relationships**: Associated with one or more Parties holding the account and linked to Transactions facilitated through the account.

14.4 Transaction

- **Description**: Captures the intention and details of financial transactions initiated by Parties, serving as the basis for fraud analysis and EFD message initiation.
- **Attributes**: Transaction ID, amount, currency, beneficiary details, payment method, and initiation date/time.
- **Relationships**: Originates from a Party and involves the movement of funds from or to an Account, triggering risk determination and EFD messaging processes.

Primary Data Structure Overview

The EFD Data Model is structured around these four key entities, interconnected to provide a comprehensive view of transactional activities and participant identities within the digital payment ecosystem. This structure supports PSPs in exchanging critical fraud-related indicators/information, enhancing financial transactions' overall security and integrity. The EFD system facilitates seamless interoperability and efficient fraud detection across different PSPs' platforms by standardising data elements and relationships.

Entity Relationship Diagram (ERD)

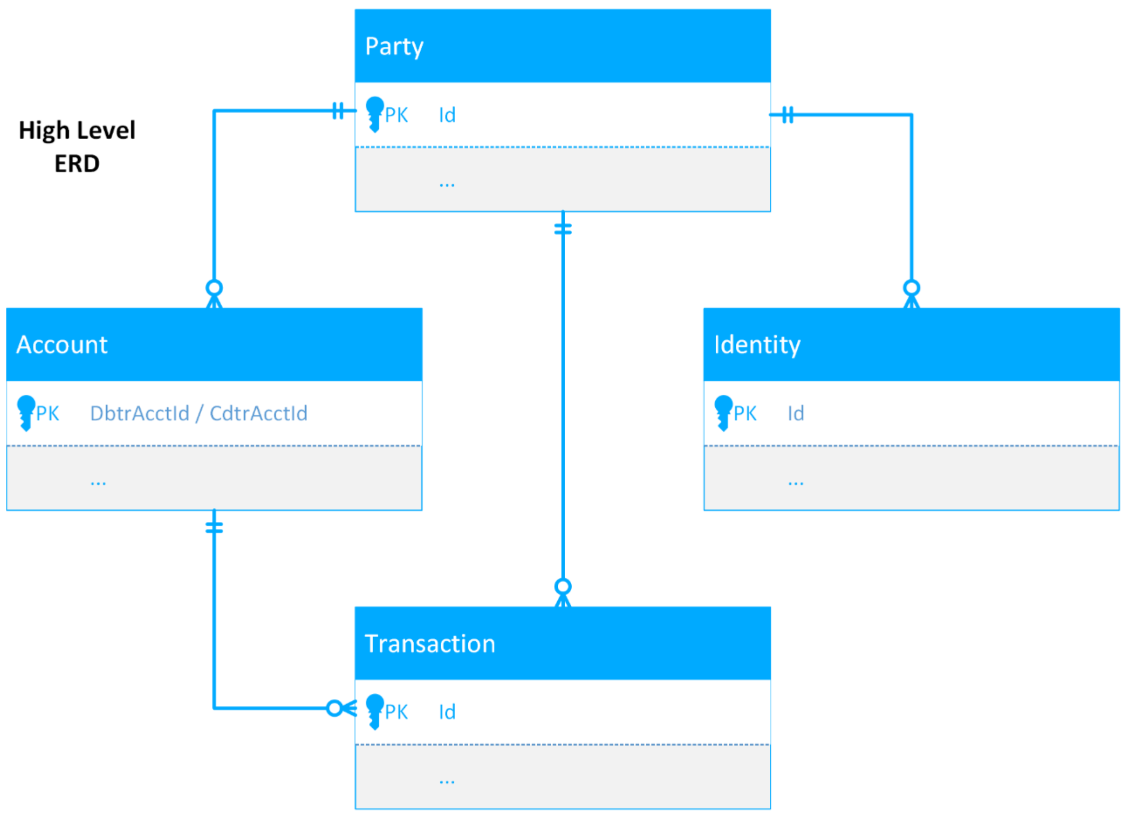


Figure 7: EFD-ERD

Entity Descriptions

Use the separate Implementation Guides for detailed solution development, not the outlines here. Below are tables detailing the attributes of each of the four entities within the EFD Messaging System. These are designed to identify the data structure clearly. They outline the Attribute Name, Description, Mandatory or Optional condition, and its presence within specific EFD Messages (Request, Response, or MI Sidecar). The separate EFD Message Implementation Guides listed in Section 9 will also help to equip stakeholders with the necessary information to integrate the EFD Messaging Service effectively.

Entity: Party			**Use Case 1**	**Condition**	**Request**	**Response**	**Mi Sidecar**
Attribute Name		**Description**					
ClntId	varchar 25	Client ID. It can be the same as the Client Key.		O			
ClntNm	varchar 140	Client Name (Customer)	Y	M	Y	Y	Y
ClntTp	varchar 30	Client Type		O			
PmryAdr1	varchar 255	Primary Address 1		O			

PmryAdr2	varchar 100	Primary Address 2		O			
PmryAdr3	varchar 100	Primary Address 3		O			
PmryPstlCd	varchar 50	Primary Post Code/Zip		O			
PmryCtry	varchar 40	Primary Country		O			
ClntRltshDt	ISODate	The date on which the client relationship began with the FI/PSP	Y	O	Y	Y	Y
ResCtryCd	varchar 50	Permanent Resident Country Code Country of tax jurisdiction	Y	O	Y	Y	Y

Table 6: Entity Descriptions - Party

The Identity entity contains a repeatable set of data attributes identifying meta data about an item used in verifying an individual and/or organisation.

Entity: Identity			**Use Case 1**	**Mandatory**	**Request**	**Response**	**Mi Sidecar**
Attribute Name		**Description**					
SbjtIdr	varchar 50	Subject Identifier. Unique number for subject and bank		M	Y	Y	
VrfctnElmt	varchar 50	Verification Element. Claims are taken directly from the bank.		M	Y	Y	
VrfctnPrc	varchar 50	Verification process used		M	Y	Y	
TrstFrmwk	varchar 255	Trust framework being measured against Uses a CodeSet for the value		M	Y	Y	
AssrncLvl	varchar 30	The assurance level is based on the trust framework used. Uses a CodeSet for the value		M	Y	Y	
TxId	varchar 50	Transaction Identifier refers to the transaction used in the check_details.		M	Y	Y	
TxTp	varchar 50	Transaction Type Uses a CodeSet for the value		M	Y	Y	
ChckMtd	varchar 50	A string representing the check done. This includes processes such as checking the authenticity of the document or verifying the user's biometric against an identity document. Uses a CodeSet for the value		M	Y	Y	

ChckMtdTp	varchar 50	String denoting the type of electronic record. Uses a CodeSet for the value		M	Y	Y	
ChckMtdSrc	varchar 200	The JSON object contains information about the source of this record.		O	Y	Y	
Clms	varchar 50	Identity attribute being claimed		M	Y	Y	
ClmsNm	varchar 50	Name of the account holder		M	Y	Y	
ClmsAdr	varchar 50	Address of the account holder		O	Y	Y	

Table 7: Entity Descriptions - Identity

Entity: Account contains the data attributes directly related to Debtor and Creditor account information

Entity: Account			Use Case 1	Mandatory	Request	Response	Mi Sidecar
Attribute Name		Description					
MsgId	UUIDv4 Identifier	Message Identification A universally unique identifier provides an end-to-end reference for an EFD messaging exchange.	Y	M	Y	Y	Y
DbtrNm	Varchar140	Debtor's Name on the account	Y	M	Y	Y	Y
DbtrDtBirth	ISODate	Account holder's date of birth	Y	M	Y	Y	Y
DbtrAcctId	varchar 34	Unique and unambiguous identification for the account between the account owner and the account servicer. Account Number. Otherwise, IBAN must be used.	Y	M	Y	Y	Y
DbtrAcctIBAN	varchar 31	International Bank Account Number (IBAN)		O	Y	Y	Y
DbtrBICFI	varchar 11	Debtor BICFI Business identifier code (BIC)		O	Y	Y	Y
DbtrAgtMmbId	varchar 6	Identification of a member of a clearing system (e.g. Sort Code)	Y	M	Y	Y	Y
DbtrAcctRef	varchar 35	The debtor provides Debtor Account Reference Information to identify the underlying account needed for routing - agency banking/HOCA, etc.	Y	O	Y	Y	Y

DbtrAcctOpnDt	ISODate	Date on which the account and related basic services are effectively operational for the account owner.	Y	O	Y	Y	Y
DbtrAcctTvr	FractionDigits TotalDigits 18	Monthly average of the received amounts over a year (payments coming in). Comply with ISO 4217 Array “Ccy“ with ISO 4217 + “Amt“ up to 18 digits	Y	O	Y	Y	Y
DbtrAcctTpCd	varchar 4	Specifies the nature or use of the account type in a coded form.	Y	O	Y	Y	Y
DbtrAcctSubTpCd	varchar 4	Debtor Account SubType Code Specifies the nature or use of the account subtype in a coded form.	Y	O	Y	Y	Y
DbtrAcctSIC	varchar 5	SIC code classifies business establishments and other statistical units by the economic activity they are engaged in. UK SIC 2007	Y	O	Y	Y	Y
DbtrAcctBizStartDt	ISODate	Business Incorporation/start date	Y	O	Y	Y	Y
DbtrAcctAmtBal	Array	Debtor Account Amount Balance Debtors' current available balance. Array “Ccy“ with ISO 4217 + “Amt“ up to 18 digits	Y	O	Y	Y	Y
CdtrNm	varchar 140	The creditor's Name on the account	Y	M	Y	Y	Y
CdtrDtBirth	ISODate	Creditor Date of Birth The specific date on which the individual was born.	Y	O	Y	Y	Y
CdtrBizStartDt	ISODate	Creditor Business Start Date Business Incorporation/start date.operational for the creditor account owner.	Y	O	Y	Y	Y
CdtrBizSIC	varchar 5	Creditor Business Sector Code SIC code classifying business establishments	Y	O	Y	Y	Y
CdtrBizLEI	varchar 20	Creditor Business LEI	Y	O	Y	Y	Y
CdtrAgtMmbId	varchar 6	Creditor Agent Member Identification Example: UK sort code	Y	M	Y	Y	Y
CdtrAcctId	varchar 50	Creditor Account Identification Otherwise, IBAN must be used.	Y	M	Y	Y	Y

CdtrAcctRef	varchar 50	The debtor provides Creditor Reference Information to allow the identification of the underlying account needed for routing - agency banking/HOCA, etc.	Y	O	Y	Y	Y
CdtrAcctOpnDt	ISODate	Creditor Account Opening Date	Y	M	Y	Y	Y
CdtrAcctRef	varchar 35	Creditor Account Reference					
CdtrAcctIBAN	varchar 31	International Bank Account Number (IBAN)		O	Y	Y	Y
CdtrBICFI	varchar 11	Creditor BICFI Business identifier code (BIC)		O	Y	Y	Y
CdtrAcctTpCd	varchar 4	Creditor Account Type Code Specifies the nature or use of the account type in a coded form.	Y	O	Y	Y	Y
CdtrAcctSubTpCd	varchar 4	Creditor Account SubType Code Specifies the nature or use of the account subtype in a coded form.	Y	O	Y	Y	Y
CdtrAcctTvr	Array	Creditor Account Turnover Monthly average of the received amounts over twelve months Array “Ccy“ with ISO 4217 + “Amt“ up to 18 digits	Y	M	Y	Y	Y
CdtrAcctBal	Array	Creditor Account Balance Creditor current available balance, including agreed overdraft facility.. Array “Ccy“ with ISO 4217 + “Amt“ up to 18 digits	Y	O	Y	Y	Y
CdtrAcctLastCdt	ISODate	Creditor Account Last Credit Before this query, what was the date when the last credit was posted to the account?	Y	O	Y	Y	Y

Table 8: Entity Descriptions - Account

Entity: Transaction contains the data attributes related to the payment intent.

* Indicators with an Asterix identify an Optional attribute condition within that specific message type.

Entity: Transaction			Use Case 1	Mandatory	Request	Response	Mi Sidecar
Attribute Name		**Description**					
IntrBkSttlmAmt	Array	Interbank Settlement Amount Amount of money moved between the instructing agent and the instructed agent. Sub-array containing “currency” and “amount”. Array “Ccy“ with ISO 4217 + “Amt“ up to 18 digits	Y	M	Y	Y*	Y
PurpCd	varchar 4	Purpose Code Underlying reason for the payment transaction, as published in the EFD Solution purpose (reason) code list.	Y	O	Y	Y	Y
TrChCd	varchar 4	Transactional Channel Code Identifies the type of communication channel used to initiate the payment., as published in the EFD Solution channel code list.	Y	O	Y	Y	Y
ClntRltshDt	varchar 4	Client Relationship Start Date The date on which the client relationship began with the FI/PSP	Y	O	Y	Y	Y
ResCtryCd	varchar 2	Residence Country Code Client Permanent Resident Country Code - Country of tax jurisdiction Using ISO 3166-1 alpha-2	Y	O	Y	Y	Y

Table 9: Entity Descriptions - Transaction

15 Design Principles

Due to the breadth of services and interests within the financial services ecosystem, settling on a methodology for sharing EFD data points has led to a purist view for standardisation aligned with our Standards Framework approach. The data values included within EFD messages reflect the actual underlying data without interpretation. All data interpretation, therefore, rests with the sending and receiving organisations' risk engine calculations when deciding how to act on the EFD message content. The legitimate interest and format of the data have been agreed upon with ICO.

1) **Security and Privacy by Design:** Ensuring customer data is protected with rigorous security and privacy measures that align with regulatory standards.

2) **Extensibility:** Providing a flexible framework that supports the inclusion of a common, minimum set of data elements and can adapt to encompass additional data as required without compromising data validation standards. Data availability and quality across the model varies by organisation and the specific transaction being analysed.

3) **No Interpretation:** Data interpretation is the responsibility of the sending and receiving organisations, avoiding standardisation of data meaning and leaving risk assessment at the discretion of the involved parties.

4) **Accuracy and Integrity:** Maintaining the highest data accuracy and integrity levels to ensure trust and reliability in the EFD Service.

5) **Customer-Centricity:** Prioritising the needs and rights of customers in handling and utilising their data.

6) **Transparency:** Upholding complete openness about data handling practices, allowing customers and PSPs to understand how their information is used.

7) **Standardization without Interpretation:** Adhering to a standardised approach where data values in EFD messages reflect the underlying data without interpretation, the sending and receiving organisations are left responsible for data analysis.

8) **Legitimate Interest and Data Format:** Engaging with regulatory bodies like the ICO to discuss the legitimate interest and format of data, ensuring that the EFD Service remains within legal frameworks.

9) **Collaboration and Iteration:** Encouraging ongoing collaboration among financial institutions to refine and enhance the EFD Messaging Standard over time.

10) **Responsiveness to Change:** Ability to quickly adapt to evolving threats in the financial landscape to maintain the effectiveness of fraud prevention strategies.

11) **Interoperability:** Ensuring the EFD Messaging Standard can work seamlessly across different platforms and systems within the financial ecosystem.

16 High-Level Architecture of Pay.UK EFD Service

Introduction

The Enhanced Fraud Data (EFD) Messaging Standard is a pioneering initiative by Pay.UK designed to significantly bolster the financial industry's defences against increasingly sophisticated fraud tactics. At the heart of this initiative is the EFD Service, a robust framework facilitating the secure and efficient exchange of fraud-related data between Payment Service Providers (PSPs). This exchange is pivotal in enhancing the detection and prevention of fraudulent transactions across the payment ecosystem.

A critical evolution in the deployment of the EFD Service has been the Confirmation of Payee (CoP) Service architectural transition from the Open Banking (OB) infrastructure to a dedicated environment managed directly by Pay.UK. This strategic shift reflects our commitment to maintaining the service's technical prowess while optimising it for greater efficiency enhanced PSP experiences, and a streamlined cost structure. The migration was executed as a like-for-like transfer, ensuring continuity in service capabilities, operational patterns, and PSP expectations without compromising the security and reliability that participants have come to trust.

EFD Service Infrastructure

The EFD Service Infrastructure managed and operated by PayUK, serves as the foundation for the Enhanced Fraud Data (EFD) Messaging Standard, a critical component in the fight against financial fraud. This infrastructure is meticulously designed to support the secure, efficient data exchange between Payment Service Providers (PSPs), enabling them to enhance fraud detection mechanisms and safeguard the financial ecosystem.

Core Components of the EFD Service Infrastructure

At the heart of the EFD Service Infrastructure lie several key components, each playing a vital role in the overall functionality and security of the service:

- **Directory Services**: Functioning as the central registry, Directory Services authenticate and authorise PSPs participating in the EFD Messaging Standard. This component ensures that only verified entities can send and receive EFD messages, maintaining the network's integrity and trustworthiness.

  By acting as the gatekeeper for EFD messaging, the Directory Services play a pivotal role in maintaining the integrity and trustworthiness of the ecosystem. They are responsible for:

  - Verifying PSPs' identity and authorisation status initiating or responding to EFD requests.
  - Facilitating secure message routing by providing PSPs with the necessary endpoint details and security tokens for communication.
  - Ensuring all interactions within the EFD Service adhere to the established security protocols and compliance standards.
- **Sending and Receiving PSP’s System Environment:** Both the Sending and Receiving PSPs maintain their system environments, which include customer-facing internet services (web, app), backend services, and fraud analysis services. These environments are designed to initiate and respond to EFD messages, analyse potential fraud risks, and ensure customer transactions are processed securely and efficiently.

- **EFD MI Provider:** Considered a potential opportunity for external FinTech collaboration, the EFD MI Provider plays a crucial role in analysing the data generated by EFD messaging. With its API endpoint, the EFD MI Provider collects Management Information (MI) Sidecar messages, providing valuable insights into the usage, performance, and effectiveness of the EFD Service. While it can be part of PayUK's system environment, its potential to be managed by a FinTech underscores the open and inclusive nature of the EFD ecosystem.

This structured approach clarifies the operational dynamics among participating entities and highlights the critical importance of each entity's contribution to the collective fraud detection and prevention effort.

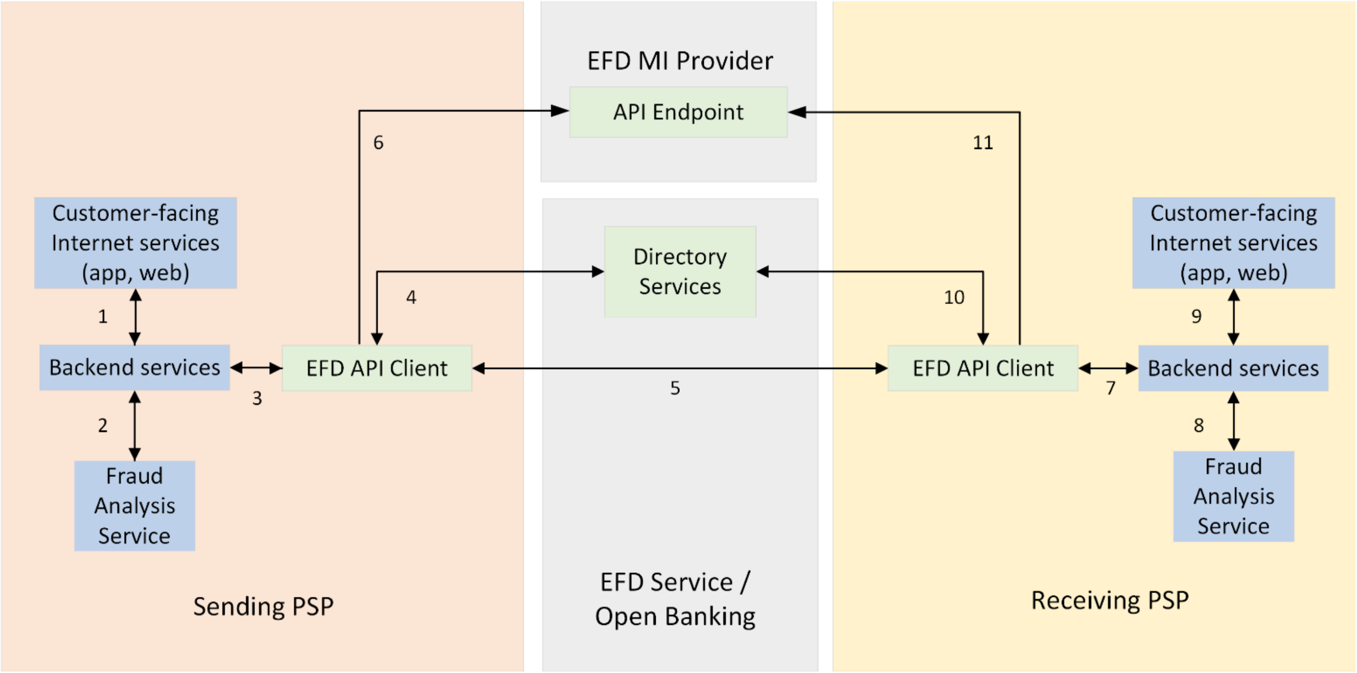


Figure 8: High-level Service Components & Communication Flows

Communication Flows and Service Components

The architecture of the PayUK EFD Service flows is characterised by a series of defined communications that facilitate the seamless exchange of fraud-related data between various system components. These flows are crucial for enabling the operational capabilities of the EFD Messaging Standard, allowing Payment Service Providers (PSPs) to interact securely and efficiently.

1. **From the Sending PSP to PayUK and the Receiving PSP**:
    - The customer-facing Internet Services (web, app) within the Sending PSP's system initiate the process by communicating (1) payment details to their Backend Services.
    - These Backend Services then assess the payment request for fraud risk (2) and prepare an EFD Request Message, leveraging the EFD API Client (3).
    - The EFD API Client engages with PayUK's Directory Services (4) to verify the Receiving PSP's endpoint details and secure a communication token.
    - Subsequently, the EFD API Client sends the EFD Request Message directly to the Receiving PSP's EFD API Client in a Peer-to-Peer manner (5).

- Additionally, the Sending PSP’s EFD API Client forwards an EFD MI Sidecar Message to the EFD MI Provider’s API endpoint (6) to contribute to the collective intelligence on fraud detection.

2. **Within the Receiving PSP’s System**:
   - Upon receipt, the EFD API Client routes the EFD Request Message to the Receiving PSP’s Backend Services for processing (7), which is analysed for fraud risk (8).
   - Although not directly interacting with the customer in this scenario, the Backend Services prepare an EFD Response Message (9), which is sent back to the Sending PSP using the same Peer-to-Peer communication established earlier.
3. **External Communications**:
   - Both the Sending and Receiving PSP’s EFD API Clients interface with PayUK’s Directory Services to authenticate and retrieve necessary communication tokens (10), ensuring a secure and verified data exchange.
   - Furthermore, both PSPs are responsible for sending their respective EFD MI Sidecar Messages to the EFD MI Provider, enriching the dataset available for fraud analysis (11).

General Security and Data Protection

Incorporating stringent security measures is paramount within the EFD Service Infrastructure to protect sensitive data and ensure compliance with regulatory standards. These measures include:

- **Transport Layer Security (TLS)**: All communications within the EFD Service utilise TLS encryption, safeguarding data in transit between PSPs and PayUK components against interception and unauthorised access.
- **Authentication and Authorisation**: Leveraging advanced mechanisms through Directory Services, the EFD Service verifies each PSP's identity and authorises their access based on predefined roles and permissions, ensuring that only legitimate entities can participate in the data exchange process.
- **Data Integrity and Non-Repudiation**: Digital signatures and secure message protocols ensure the integrity of EFD messages, allowing PSPs to verify the authenticity of the information exchanged and prevent tampering.

Operational Excellence and Scalability

Designed with operational excellence in mind, the EFD Service Infrastructure supports high availability, scalability, and resilience. It accommodates the dynamic nature of financial transactions and the evolving landscape of fraud tactics, ensuring PSPs have a reliable tool for proactive fraud prevention.

- **High Availability**: Redundancy and failover mechanisms ensure the EFD Service remains operational, minimising downtime and maintaining continuous service availability for PSPs.
- **Scalability**: The infrastructure is built to efficiently handle varying volumes of EFD messages, allowing for seamless scaling to accommodate growth in the number of transactions and participants.

In summary, the EFD Service Infrastructure provides a robust framework underpinning the EFD Messaging Standard, facilitating secure, efficient, and compliant data exchanges crucial for enhancing fraud detection and prevention across the payment ecosystem. Through its comprehensive design and focus on security, the infrastructure ensures that PSPs can confidently engage in the service, contributing to a safer financial environment for all stakeholders.

17 Change Management and Version Control

Change Management Process

The Change Management Process ensures that all modifications to the EFD Messaging Standard are methodically evaluated and integrated. This involves:

- **Proposal Submission:** Stakeholders can submit change requests detailing the need and impact of the proposed change.
- **Review and Approval:** A dedicated EFD Service committee reviews these proposals, assessing their feasibility, compliance, and potential impact on the current ecosystem.
- **Implementation and Documentation:** Approved changes are systematically implemented. Each change is documented, providing a clear rationale and user implications.

Version Control System

This version control is critical for maintaining the integrity of the EFD Messaging Standard, with the version identifier included in the message requests/responses. The version control system:

- **Tracks Changes:** Documents all modifications, including minor edits and significant overhauls.
- **Maintains Historical Records:** Keeps an archive of all previous versions, allowing for easy reference and rollback if necessary.
- **Ensures Consistency:** Guarantees that all users are working with the most current version of the standard.

Stakeholder Engagement

Active engagement with stakeholders is vital for the standard's evolution. This includes:

- **Feedback Mechanism:** Establishing channels for continuous feedback, suggestions, and reporting issues.
- **Regular Updates:** Communicating updates and changes to all stakeholders promptly.
- **Inclusive Decision-Making:** Ensuring a diverse range of voices from the payment ecosystem is considered in the change process.

Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment is developed at the outset of designing any EFD Service. Once the service is live, any significant changes to the EFD Messaging Standard, including introducing new data fields or altering messaging content, will revisit the DPIA for the particular EFD Service. This assessment ensures:

- Privacy Concerns are Addressed
- Compliance with Data Protection Laws
- Stakeholder Consultation

This comprehensive approach to Change Management and Version Control ensures the EFD Messaging Standard remains robust, relevant, and effective in the ever-evolving landscape of digital payments, data minimisation and security.

18 Security

The Enhanced Fraud Data (EFD) Messaging Standard, based on the infrastructure used by the Confirmation of Payee (CoP) Service, incorporates a comprehensive security framework designed to protect the integrity, confidentiality, and availability of financial data exchanges. Recognising the critical role of security in preventing fraud within digital payment ecosystems, the EFD Messaging Standard leverages established security principles and technologies to ensure that all communication and data handling processes meet the highest security and compliance standards.

Key Security Components

- **Open Banking OAuth2 Framework**: The EFD Messaging Standard adopts the Open Banking OAuth2 security framework, a robust model for managing access and identity. This framework ensures that only authenticated and authorised entities can initiate or respond to EFD messages. Utilising OAuth2 provides a secure foundation for API interactions, safeguarding against unauthorised access and ensuring that each transaction can be traced back to a verified entity.
- **Certificates**: Transport and signing certificates are central to the security model, which ensures secure communication channels and verifies the authenticity of messages exchanged between participants. The EFD Messaging Standard mandates using certificates issued by trusted Certificate Authorities (CAs), ensuring all participants engage in a trusted network. Transport Layer Security (TLS) certificates encrypt data in transit while signing certificates provide non-repudiation by verifying the message originator's identity.
- **Token Authentication**: The EFD Messaging Standard adheres to Financial-grade API (FAPI) compliant token authentication methods to ensure secure access to APIs. Token-based authentication mechanisms such as private_key_jwt and tls_client_auth offer robust security features, including short-lived access tokens and stringent token issuance policies. This approach minimises the risk of token theft or misuse, adding a layer of security to API interactions.

The EFD Messaging Standard establishes a secure and resilient framework for exchanging fraud-related data by integrating these key security components. These measures are vital for protecting against external threats and reinforcing the trust between participating financial institutions, ultimately contributing to the overall effectiveness of fraud detection and prevention within the payment ecosystem.

Enrolment and Onboarding

The EFD Messaging Standard's enrolment and onboarding process ensures that all participating entities are authenticated and authorised to engage securely within the EFD ecosystem. This process leverages the principles established by the Open Banking Directory, which is pivotal in managing participant data and facilitating secure communications.

- **Directory Services**: The Directory serves as a central registry for all participants in the EFD service. It maintains a comprehensive list of authenticated entities, including their roles (e.g., EFD Requester, EFD Responder), certificates, and authorised software. The directory supports the secure exchange of EFD messages by ensuring only verified participants can access the service.

- **Dynamic Client Registration (DCR)**: Participants undergo a secure onboarding process through Dynamic Client Registration, a mechanism that automates the exchange of security credentials. DCR streamlines the enrolment of new participants by allowing them to register their software clients and obtain necessary authentication tokens seamlessly. This process ensures that each participant's software is authorised and possesses the correct security certificates for secure EFD message exchanges.

Message Security

Securing the integrity and confidentiality of EFD messages is paramount to the standard's effectiveness in combating fraud. The EFD Messaging Standard incorporates several layers of security to protect messages from unauthorised access, tampering, and eavesdropping.

- **Non-repudiation** is a vital aspect of the EFD Messaging Standard, and it is ensured through digital signatures based on the JSON Web Signature (JWS) standard. These signatures are crucial in verifying the sender's identity and preventing denial of message origination. Each EFD message is signed by the sender's private key, which can be authenticated by the recipient using the sender's public key, thereby ensuring the message's integrity and origin authenticity.
- **Encryption and Data Integrity** are vital to the EFD Messaging Standard's security measures. The standard mandates using Transport Layer Security (TLS) 1.2 or higher to protect data in transit. This protocol establishes a secure communication channel between participants, ensuring that message contents remain confidential. Data integrity checks are also performed to verify that the message has not been altered during transmission.

These security measures are integral to the EFD Messaging Standard, ensuring participants exchange sensitive data securely and reliably. By adhering to rigorous enrolment, authentication, and message protection protocols, the EFD service mitigates the risk of fraud and enhances the security of digital payments within the financial ecosystem.

Authorisation Domains and Role Profiles

The EFD Messaging Standard operates within a framework of defined authorisation domains and role profiles, ensuring that participants have appropriate permissions for the actions they are authorised to perform within the EFD ecosystem. This framework facilitates a secure and efficient operation by delineating each participant's capabilities and responsibilities.

- **Authorisation Domains**: The standard recognises two primary authorisation domains that reflect the regulatory landscape and operational needs:
    - **Pay.UK Domain**: This domain governs entities operating under the UK's payment systems regulations, ensuring they adhere to the standards and practices required for secure and compliant data exchange within the UK financial system.
    - **PSD2 Domain**: For participants subject to the Second Payment Services Directive (PSD2) in the European Economic Area, this domain provides a regulatory framework that supports secure, innovative, and competitive payment environments across Europe.

  Each domain prescribes specific authentication and authorisation mechanisms tailored to its regulatory and operational context, ensuring that participants meet the stringent security requirements inherent to financial data exchange.

- **Role Profiles**: Within these authorisation domains, participants are assigned specific role profiles that define their permissions and responsibilities in the EFD service. Key role profiles include:
    - **EFD Requester**: Entities authorised to initiate EFD requests to gather data for fraud detection. They are responsible for ensuring the security and compliance of their data requests.
    - **EFD Responder**: Participants tasked with responding to EFD requests. They must securely provide the requested data per the EFD standard and applicable regulations.
    - **EFD Service Provider**: The entity overseeing the EFD service's operation, ensuring it runs smoothly and securely and complies with all relevant laws and standards.

Software statements and assertions underpin these role profiles and digitally signed statements issued by an authorised body (e.g., Open Banking Directory). These statements certify a participant's software client, detailing its capabilities, permissions, and the security measures it employs. This certification process ensures that all software clients participating in the EFD service are verified and trusted, enhancing the overall security posture of the ecosystem.

The EFD Messaging Standard ensures that participants are appropriately authenticated and authorised by establishing clear authorisation domains and role profiles. This fosters a secure environment for exchanging fraud-related data.

Secure Communication Protocols

The EFD Messaging Standard employs rigorous secure communication protocols to safeguard participant data exchange and ensure message confidentiality, integrity, and availability. These protocols are fundamental to maintaining the trust and reliability of the EFD service, especially when handling sensitive financial information and fraud-related data.

- **Transport Layer Security (TLS)**: The core of EFD's secure communication is the mandatory use of Transport Layer Security (TLS) version 1.2 or higher. TLS provides a secure channel between two parties, encrypting data in transit to prevent eavesdropping and tampering by unauthorised parties. This ensures that all information exchanged between EFD participants remains confidential and intact from origin to destination.
- **API Security Standards**: The EFD Messaging Standard adheres to the financial-grade API (FAPI) security standards and is designed to provide robust security for web APIs. FAPI standards include strong authentication mechanisms, authorisation protocols, and data encryption, offering high protection for sensitive financial data. Critical aspects of FAPI compliance include:
    - **Authentication and Authorization**: We utilise the OAuth 2.0 framework for secure authorisation of API access, ensuring that only authenticated clients can access restricted resources.
    - **Access Tokens**: Short-lived access tokens are issued that provide temporary, scoped access to an API, minimising the risk of token compromise.
    - **Rate Limiting and Throttling** involve implementing measures to control the number of requests a client can make to an API within a given timeframe, protecting against abuse and ensuring service availability.

Together, TLS and FAPI standards form the backbone of secure communication within the EFD ecosystem, supported by additional practices such as:

- **Certificate Pinning**: Enhancing security by ensuring that clients verify they are connecting to the correct server using a known, pre-shared certificate, preventing man-in-the-middle attacks.
- **Regular Security Audits**: Conduct periodic security assessments and reviews of the communication protocols, infrastructure, and implementation to identify and remediate potential vulnerabilities.

By leveraging these secure communication protocols, the EFD Messaging Standard ensures that participants can confidently exchange data, knowing that the mechanisms in place robustly protect against a wide array of cyber threats and vulnerabilities. This commitment to security is crucial for the effectiveness of the EFD service in combating fraud and enhancing the security of digital payments across the financial ecosystem.

Certificate and Authorization Management

Effective certificate and authorisation management, a crucial aspect of the EFD service, is not just about maintaining the security and integrity of the Enhanced Fraud Data (EFD) Messaging Standard. It's about you, as a participant, ensuring that all entities involved in the data exchange are authenticated and authorised to participate, thereby bolstering the overall trustworthiness of the system.

- **Certificate Management**: Certificates play a pivotal role in establishing secure communications and authenticating the identities of EFD service participants. The EFD Messaging Standard mandates the use of digital certificates for both transport layer security and message signing, adhering to the following practices:
    - **Issuance and Renewal**: Digital certificates are issued by trusted Certificate Authorities (CAs) and are subject to renewal at regular intervals to ensure continued security. Participants must manage their certificates actively, including timely renewal and revocation where necessary.
    - **Revocation Checks**: To counter the risk of compromised certificates, the EFD service implements Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP). These mechanisms allow participants to verify a certificate's status in real-time, ensuring it has not been revoked before establishing a communication channel or accepting a signed message.
    - **Certificate Pinning**: To further secure communications, participants are encouraged to implement certificate pinning, where clients verify the server's certificate against known, pre-shared certificates. This practice prevents man-in-the-middle attacks by ensuring that the connection is made with the genuine server.
- **Authorisation Management**: The EFD service utilises a robust framework for managing participant authorisations, ensuring only authorised entities can send and receive EFD messages. Key components include:
    - **Role-Based Access Control (RBAC)**: Participants are assigned specific roles within the EFD ecosystem, each with predefined permissions that determine what actions they can perform. This role-based approach ensures that participants have access only to the functionalities necessary for their operations, minimising the risk of unauthorised data access or manipulation.
    - **Dynamic Client Registration (DCR)**: DCR is an automated process that allows new clients to register with the EFD service securely. Through DCR, participants obtain the credentials

and tokens for API access, ensuring that all entities interacting with the system are authenticated and authorised.

- **Regular Access Reviews**: Used to maintain a secure and compliant environment, the EFD service conducts regular reviews of participant access rights. These reviews help identify and rectify discrepancies or outdated authorisations, ensuring access permissions remain aligned with current roles and responsibilities.

By adhering to stringent practices for certificate and authorisation management, you, as a participant, play a crucial role in ensuring the secure foundation of the EFD Messaging Standard. These measures are critical and essential for protecting the system against unauthorised access and ensuring that all communications and transactions are conducted securely and reliably within the EFD ecosystem.

19 General Implementation Guidelines

In addition to the specific EFD Message implementation guides separately identified in section 9, the following applies across the EFD framework information should be used in the general development of the EFD Service.

Notation Conventions

The EFD Message Standard provides JSON-specific implementations.

Character Set

JSON messages allow the full range of global language requirements (the full Unicode character set encoded using UTF-8). Additional reading is available at RFC 8259, The JavaScript Object Notation (JSON) Data Interchange Format.

The EFD's Customers must be able to support the following character set commonly used in international communication, as follows:
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
/ – ? : ( ) . , ‘ +

Plus, the following additional special characters:
! # $ % & ' * + = ? ^ _ ` { | } ~ " ( ) , : ; < > @ [\ ]

Plus, the following additional characters to support UK diacritics:
â ê î ô û ŷ ŵ á é í ó ú ý ẃ ä ë ï ö ü ÿ ẅ à è ì ò ù ỳ ẁ
Â Ê Î Ô Û Ŷ Ŵ Á É Í Ó Ú Ý Ẃ Ä Ë Ï Ö Ü Ÿ Ẅ À È Ì Ò Ù Ỳ Ẁ

To cater to indigenous languages within the UK beyond English, i.e., Irish, Scots, Scots Gaelic, and Welsh, other characters containing diacritics will also be used.

This requires using Unicode subsets Latin-1, Latin Extended-A alphabet and Latin Extended Additional Alphabet.

Extending the character set beyond the Basic Latic character set will promote greater inclusivity and allow Customers to populate names and addresses accurately.

Where a more restrictive character set is required, such as the UETR, we have defined XML Pattern facets to restrict each element within the schemas.

Identifications and identifiers must respect the following:

- Content is restricted to the basic Latin character set.
- Content must not start or end with a '/'.
- Content must not contain '//'s.
- Spaces are not permitted in identification (*Id*) fields.

The following characters must be escaped within the JSON as follows:

Original Character	Escape Sequence
\	\\
"	\”

Table 10: JSON Escape Characters

The following special characters comply with JSON syntax but **must not be used** within text elements:

Original Character	Escape Sequence
Backspace	\b
Tab	\t
Cr	\r
Lf	\n
Form feed	\f

Table 11: Special Characters

To assist Customers who provide services for indirect Agencies that cannot accept or process this extended Latin-based character set, we have provided a mapping table below that allows Customers to ‘downgrade’ the characters to their Basic Latin equivalents.

Special Characters Mapping Tables

Generally, all accented characters should have accents removed.

1. Mapping of letters with diacritical sign – accent acute:

Glyph	Á	É	Í	Ó	Ú	Ý	Ẃ	á	é	í	ó	ú	ý	ẃ
Latin letter	A	E	I	O	U	Y	W	a	e	i	o	u	y	w

2. Mapping of letters with diacritical sign – circumflex:

Glyph	Â	Ê	Î	Ô	Û	Ŷ	Ŵ	â	ê	î	ô	û	ŷ	ŵ
Latin letter	A	E	I	O	U	Y	W	a	e	i	o	u	y	w

3. Mapping of letters with diacritical sign – accent grave:

Glyph	À	È	Ì	Ò	Ù	Ỳ	Ẁ	à	è	ì	ò	ù	ỳ	ẁ
Latin letter	A	E	I	O	U	Y	W	a	e	i	o	u	y	w

4. Mapping of letters with diacritical sign – umlaut/diaeresis:

Glyph	Ä	Ë	Ï	Ö	Ü	Ÿ	Ẅ	ä	ë	ï	ö	ü	ÿ	ẅ
Latin letter	A	E	I	O	U	Y	W	a	e	i	o	u	y	w

Date and Time

ISODate

All dates must be represented in UTC format as defined in ISO 8601. Dates will be interpreted as the local date in the United Kingdom, taking account of summer and winter time (UTC+01:00 and UTC+00:00, respectively). For example: 2021-06-01

ISODateTime

All times must be represented in Coordinated Universal Time (UTC) as per ISO 8601. UK local time offset must be added, taking account of summer and winter time (UTC+01:00 and UTC+00:00, respectively). For example 2021-06-01T11:00:01.123+00:00

Message and Transaction Identifiers

The ISO20022 standard has defined several elements that can be used to unambiguously identify certain aspects of a business message, such as an ISO20022 message or transaction. The EFD's traceability function has been designed to utilise the Unique End to End Transaction reference (UETR) as the Message Id

Message-Id

Please see UETR below.

UETR

The UETR (Unique End-to-End Transaction Reference) is a 36-character universally unique identifier which provides an end-to-end reference of a payment transaction; it is designed to be unique across systems and does not need an authority to administer its allocation.

Since the reference must be unique across systems, Pay.UK has mandated the usage of the UUIDv4 standard compliant with RFC 4122. These UETRs can be generated "in-house" using the algorithms published within RFC 4122 or publicly available libraries.

Within financial transactions, the principal use of the UETR is to uniquely identify a payment from the initial payer (Debtor Agent) right through to the final payee (Creditor Agent).

For EFD Messaging, the UETR will be generated by the initial requestor and used by the responder.

20 Appendix

Tables

Figures

SHOW YOUR SUPPORT FOR EFD MESSAGING

We are keen to hear all forms of feedback regarding this innovative new standard and encourage you to communicate with the Standards Team at Pay.UK

You can reach us at the following email address
standards@wearepay.uk