

Procedure to Connect via Interledger Protocol (ILP)

This document provides step-by-step instructions for financial institutions to establish secure ILP connectivity with IFB Bank. The ILP connection is safeguarded with AES-based protocol transformation via <https://intfiba.netlify.app>, analogous to the processes utilised for IPIP and SFTP messaging.

1. Registration and Initial Access

If you wish to connect to our ILP channel as a financial institution, please email us at admin@intfiba.com using only the business email address associated with your institution (no Gmail or similar personal email accounts are accepted).

Upon registration, 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.

2. 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).

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. Communication Parameters

The following technical parameters must be strictly adhered to when establishing ILP communication with IFB Bank:

- Protocol: Interledger Protocol (ILP) over BTP/STREAM
- Connector Endpoint: Provided per counterparty upon successful KYC/KYB onboarding
- Transport Security: TLS 1.3 enforced with Perfect Forward Secrecy; cipher suites restricted to BSI TR-02102-2 approved list (2025 edition)
- Authentication: BTP token (rotated every 90 days); token revocation available within 24 hours
- Addressing: Open Payments Payment Pointer (HTTPS well-known endpoint: `/.well-known/pay/*`) or static BTP peering as fallback
- Rate-Limiting: 500 packets per minute; exceeding this threshold will return HTTP 429
- Micropayment Validation: Three €0.01 test packets, fulfilment within ≤ 1000 ms
- Burst Validation: €1 throughput burst, $< 0.5\%$ packet-loss, < 750 ms mean round-trip latency
- Escrow and Conditional Fulfilment: STREAM conditional logic with cryptographic fulfilment and auto-revert if settlement finality not achieved
- Settlement Finality: Each ILP packet triggers ISO 20022 PACS.009 routed to TARGET2 or approved Nostro correspondent; beneficiary credit only after confirmed FMI settlement
- Escrow Timeout: If finality not achieved by T+0, exception logged per Basel III operational-risk requirements

- AES Key Handling: Input AES Code issued via message board; transformed to Output AES Code via <https://intfiba.netlify.app>; Output Code valid for one ILP message only, with a one-hour validity window
- Logging: All ILP packets, ISO 20022 messages, and compliance events logged and retained for seven years per PSD2 and ISO 27001
- VPN Access: ILP connector reachable only via restricted VPN tunnel (two-time access per Input AES issuance)
- Confidentiality: BTP tokens encrypted at rest with AES-256; breach notification window 24 hours