



SecuritiesTransferHub
by guidance

STH consultation, 2026.05.15

Topics

- Technical details of operation
 - Process Description
 - STH Admin and its Functions
 - STH Client
- Questions
- Questionnaire

01

Message composition



SecuritiesTransferHub
by guidance

Unified and structured message format

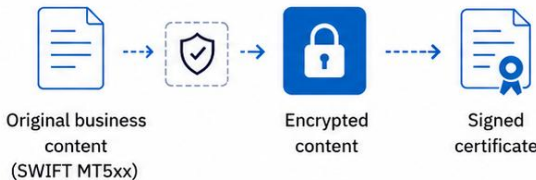


BUSINESS MESSAGE

The message contains all necessary metadata and business content.



BUSINESS CONTENT ENCRYPTED WITH TRUSTED CERTIFICATE



The business content is encrypted with the trusted certificate, so only the authorized recipient can decrypt it.



CONTENT INTEGRITY ENSURED WITH HASH VALIDATION



The hash value ensures that the business content has not been altered during transmission. Any modification is detectable.



STANDARDIZED

A unified structure for all business messages



SECURE

Encryption and hash ensure confidentiality and integrity



COMPLIANT

Identifiers and timestamps enable full auditability



FLEXIBLE

Easily extensible metadata and new content types



Payload content and format

- The business content of the message is contained in the Payload block
- The STH does not see the Payload block
- The content and form of the Payload depends on the agreement of the business partners.
- The format of the Payload message. Options:
 - SWIFT FIN MT5xx message format
 - json, yaml or xml metadata message
- Expectations:
 - A uniform format in agreement with the participants



Message Envelope fields

- **messageId**: unique technical identifier of the message.
- **correlationId**: identifier used to associate processes and related transactions.
- **senderId**: identifier of the sending party.
- **receiverId**: identifier of the receiving party.
- **createdAt**: time when the message was created.
- **messageType**: type of business message.
- **idempotencyKey**: key used to filter out repeated submissions.
- **security**: block containing encryption and signature metadata.
- **payload**: encrypted content stored in Base64 format.



Security block

- recipientCertificateId: a reference to the recipient's certificate.
- encryptedContentKey: symmetric encryption key, encrypted with the recipient's public key.
- iv: initialization vector (a unique and random 12 bytes must be specified for each message)
- hash: authentication tag for integrity protection.
- signature: the sender's digital signature.

Algorithms

- encryption algorithm: AES-256-GCM/RSA-OAEP
- hash algorithm: SHA-256



Encryption and signature model

- The client generates a single-use AES key.
- The payload is encrypted with the AES-256-GCM algorithm using this key.
- The AES key is encrypted with the recipient's public key using the RSA-OAEP method.
- A hash is created from the relevant fields of the message.
- The sender digitally signs the message with their private key.
- The STH verifies the hash code.
- The STH verifies the sender and signature.

02

Operating principle



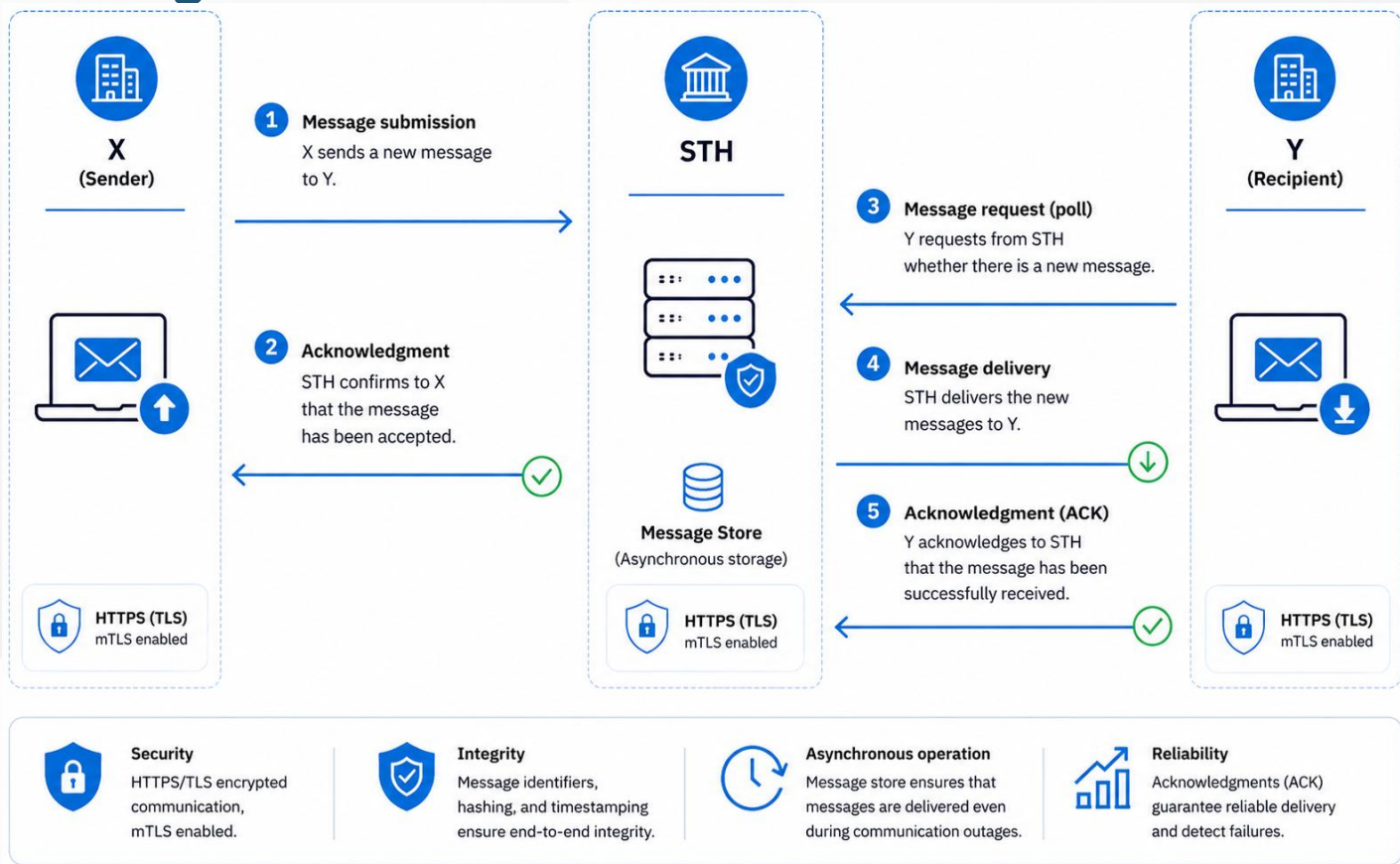
SecuritiesTransferHub
by guidance

Communication

- HTTPS / mTLS encrypted connection
- REST protocol
- The server is always the STH, it is to be called
- No service offering on the client side



Operating model



Message lifecycle, server-side statuses

- **accepted:** the message was accepted by the server.
- **delivered:** the message was delivered to the receiving client by the server.
- **client_received:** the receiving client successfully received the message.
- **acked:** the receiving client successfully parsed the message.
- **nacked:** the receiving client failed to parse the message (the message is faulty).
- **duplicate:** a resubmission was made with the same idempotence key.
- **poll_timeout:** the poll ended without a message.



Long-polling process

- The client makes a GET /messages/poll call with their own receiverId.
- The client specifies the wait time with the waitSeconds parameter.
- If there is a message waiting, the server returns the message envelope immediately.
- If no message is available, the server keeps the connection open for the specified time.
- The client then starts a new request-response cycle.
- If a new message arrives within the time window, the server responds immediately.
- If no message arrives, the server responds with a 204 No Content response at the end of the time window.

03

Demo app



SecuritiesTransferHub
by guidance

04

STH Admin



SecuritiesTransferHub
by guidance



Dashboard



SecuritiesTransferHub
by GIANCE

Dashboard

Message List

Certificate Management

User Management



Dashboard

Number of messages sent but not received

13

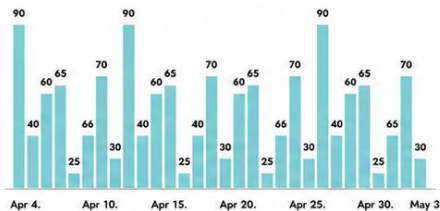
Number of messages sent in the last month

1240

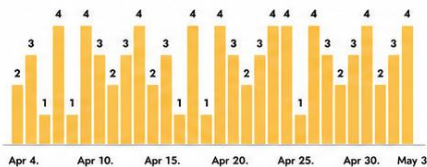
Certificate expiration date

2026.12.02.

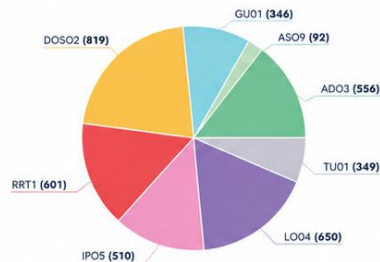
Number of messages in the last 30 days



Average response time of messages (hours)



Messages by recipient





Message management



SecuritiesTransferHub
by GIANCIE

[Dashboard](#)[Message List](#)[Certificate Management](#)[User Management](#)

Messages

[Filters](#)

Sent date	Message ID	Prior message	Direction	Sender / Recipient	Status
2026.05.13. 10:23:01	6c0d9f8a-2b71-4f55-a912-e7d4c3b2a109	4f9c1d7a-8e55-4b77-a902-b6d3e1f2c700	➡ sent	RES99	confirmed
2026.05.10. 09:10:43	3f8c2d91-7a4b-4c8e-b1f2-9d7a6c5e4f10	73e1c5d9-4a22-47ff-9b61-2e8d0f7a4c11	⬅ received	FOR45	in transit
2026.04.30. 23:45:11	550e8400-e29b-41d4-a716-446655440000	4f9c1d7a-8e55-4b77-a902-b6d3e1f2c700	⬅ received	GUI01	sent
2026.04.25. 18:12:54	73e1c5d9-4a22-47ff-9b61-2e8d0f7a4c11	8d1f7c3a-6b92-4e88-a504-2c9f5d7a1e33	➡ sent	RES99	confirmed
2026.04.20. 08:05:03	ac5f2d7e-9b33-41aa-8d70-5c1e4f7a2b88	6c0d9f8a-2b71-4f55-a912-e7d4c3b2a109	⬅ received	FOR45	in transit

1 2 3 4 5 6 ... 67 68

Message: 550e8400-e29b-41d4-a716-446655440000

Sent date: 2026.04.30. 23:45:11
Message ID: 550e8400-e29b-41d4-a716-446655440000
Prior message: 4f9c1d7a-8e55-4b77-a902-b6d3e1f2c700
Message reference: e3b0c442-98fc-1c49-afbfc-4c8996fb924
Direction: ⬅ received
Sender / Recipient: GUI01
Status: ● sent

Message timeline

2026.05.13. 12:21:12 GUI01 sent ●
2026.05.13. 12:22:43 Prior message 550e8400-e29b-41d4-a716-446655440000 created
2026.05.13. 12:30:54 RES99 received the message ●
2026.05.13. 12:31:03 RES99 confirmed the message ●



Central functions

- Certificate management
 - Authentication: mTLS
 - Signature
 - Encryption
- Participant management
 - Organization, name, identifiers, certificates
- Message delivery rules (who can send to whom)
- Alerts



Client functions

- User Management
 - Registering new users to the organization
 - Managing accounts (password, 2FA, ...)
- Reports, summaries

05

STH Client

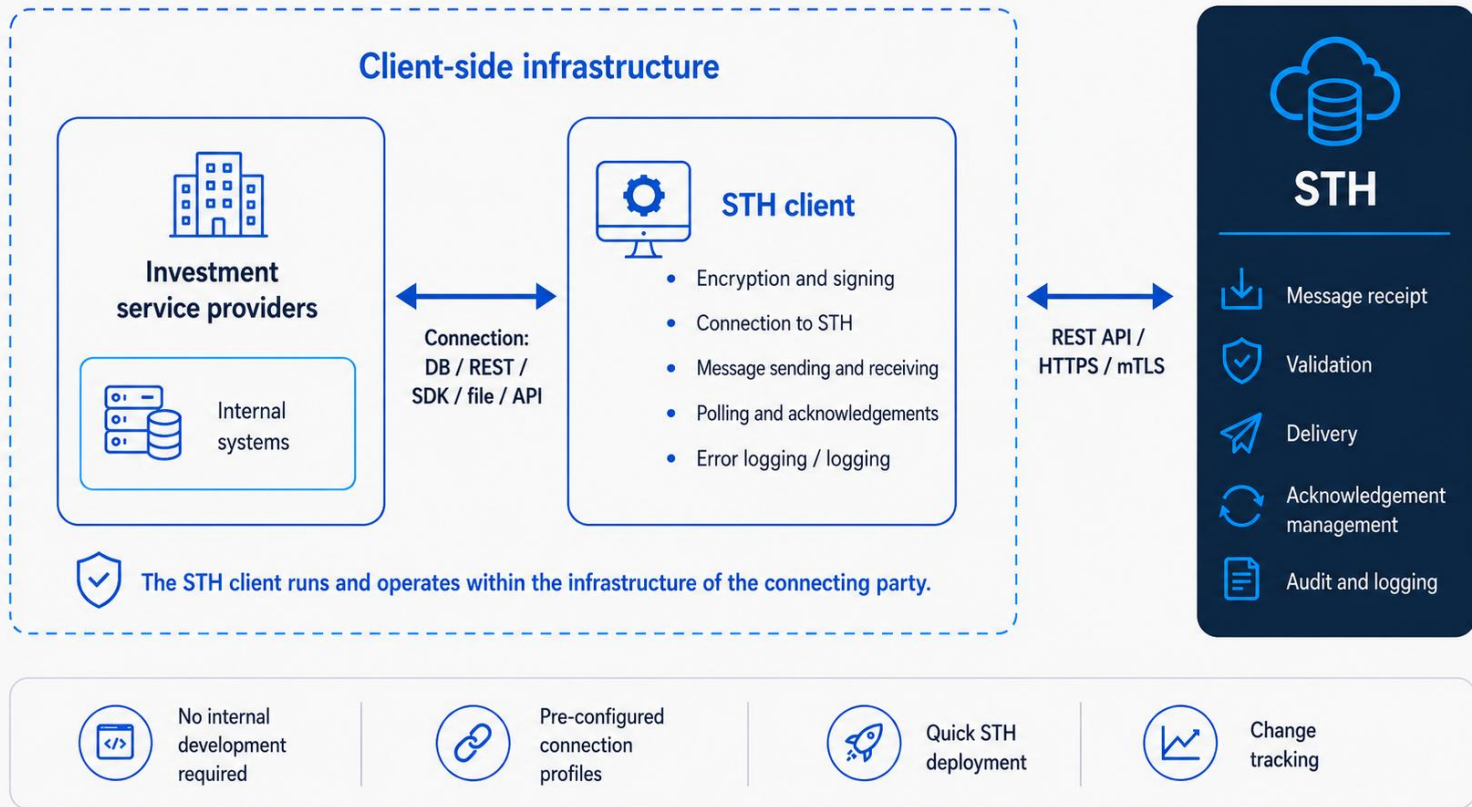


SecuritiesTransferHub

by guidance



STH kliens (opcionális)





Technical details

- Containerized SpringBoot based application
- Minimal resource requirement
- Fixed communication and integration module
- DB and File customization in case of non-standard integration
- In case of UI module
 - Angular interfaces
 - Authentication integration
 - Message sending integration



Advantages, functions

- Simple and fast connection
- Internal interfaces (REST, MQ, SDK, DB, file, ...)
- Message format conversions
- Metrics
- Internal admin interfaces
 - Message management
 - Alerts
 - Manual messaging if required (as a BCP solution: create a message on the interface and send it)

06

Infrastructure

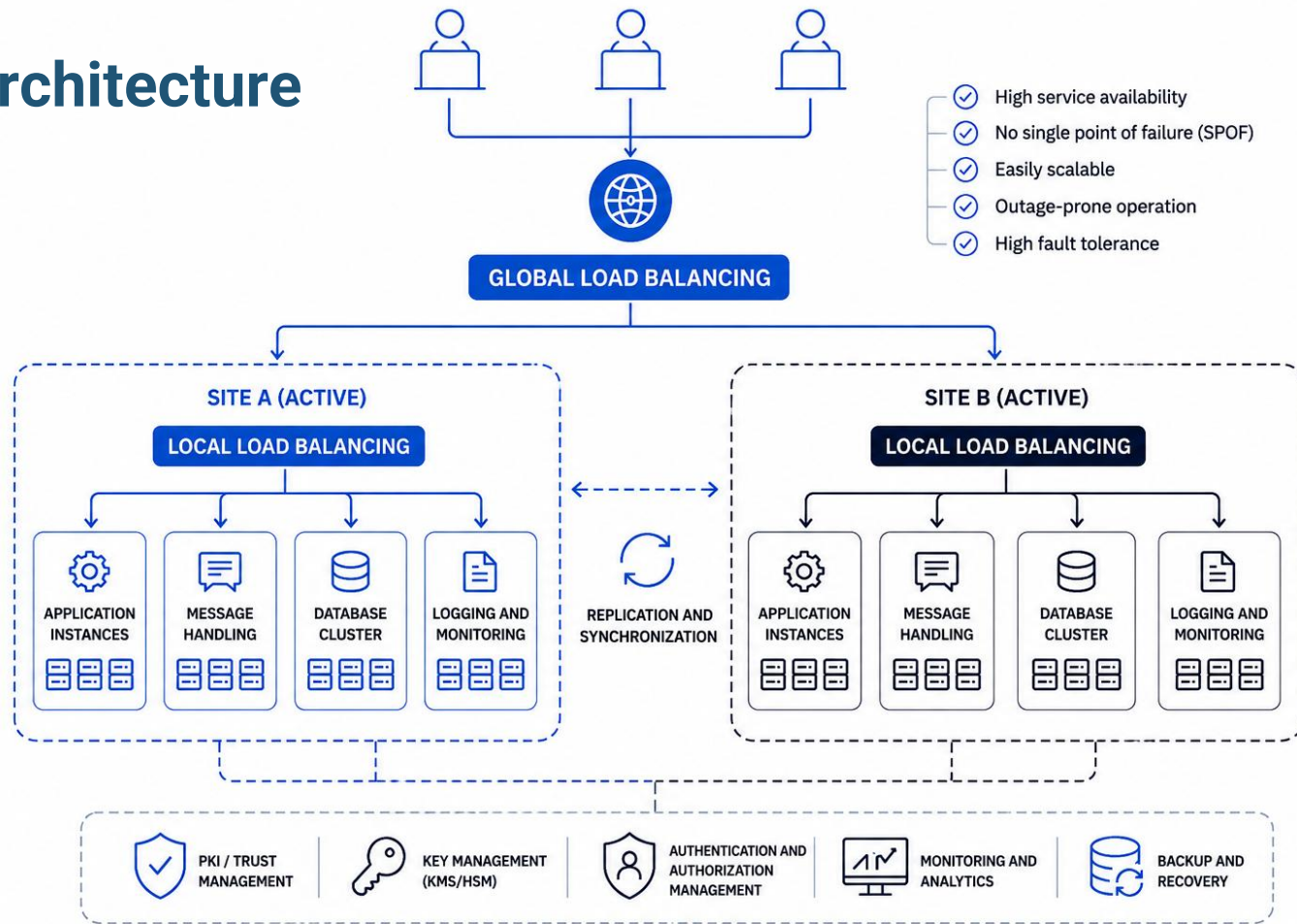


SecuritiesTransferHub

by guidance



Architecture



Environment

- Domestic service provider
- Georedundant servers, redundant power and internet supply
- High security compliances
- Containerized applications running in Kubernetes architecture
- Scalable architecture
- Audited

Introduction

- Initial DEV environment
- Provision of test environment(s)
- Receiving and sending side mocking
- Developer and operator support
- Full support

07

Questions



SecuritiesTransferHub

by guidance



Already asked

- STH operation and infrastructure?
- Pricing and subscription conditions?
- “Critical mass” required to launch a service?
- Technical details of STH Client?
- Connection without STH Client?
- How would parties be identified?
- Message storage time?
- Message format?

08

Questionnaire



SecuritiesTransferHub
by guidance

Why ask?

- It helps us with our work
- It helps us stay in touch
- You can also express your unique insights and needs
- We will not share results or answers with anyone else



<https://forms.cloud.microsoft/e/2y6CU0f7R3>

09

Next steps



SecuritiesTransferHub

by guidance

Next steps

Technical directions

- Development
- DEV environment setup
- Finalization of technical documentation
- Infrastructure definition
- Test environment setup
- IT security audit

Legal, business direction

- Pricing Strategy Creation
- Statements of Intent
- Compliance Checks
- Contract Development
- Compliance Audits

Thank you for your attention!



<https://sth.guidance.hu>

Monori Antal – antal.monori@guidance.hu
Varga Zsombor – zsombor.varga@guidance.hu



SecuritiesTransferHub

by guidance