FMSB Publishes Transparency Draft of Standard for Sharing of Standard Settlement Instructions

Published on 12 July 2024

This Financial Markets Standards Board ("FMSB") Transparency Draft is applicable to Firms when sharing their own SSIs, or where they manage their clients' SSIs as part of their commercial relationship (for example where they perform custodial or prime brokerage services), in relation to their clients' SSIs. This Standard does not apply to Firms' management of their counterparties' SSIs.

The proposal is structured in two main parts:

- Standard: proposes Core Principles for the channels, processes, and governance around sharing of SSIs, and
- Templates: proposes standardised templates, based on industry-standard taxonomy, for use in residual cases where SSI instructions are sent manually.

FMSB is seeking views on the Standard and Templates, the final version of which will form part of the annual attestation that each FMSB Member Firm is expected to make annually and which non-Members are encouraged to consider for adoption.

FMSB is also seeking views on a selection of potential authentication options to address the vulnerabilities in the manual sharing of SSIs, which is reproduced after the consultation questions which follow, but which will not form part of the Standard.

Background

Standard Settlement Instructions (SSIs) specify the "where" of delivery/settlement after the execution of any financial transaction. The most significant cause of fails at the settlement stage, after lack of inventory, is incorrect or missing SSIs[1]. Human intervention is necessary to resolve exceptions prior to settlement, especially to remediate incorrect SSIs. This inefficiency is likely to become a greater risk with more jurisdictions moving towards accelerated settlement, including the UK's planned move to T+1 in 2027 as outlined in the *Geffen Report*[2], leaving less time to input or amend the correct settlement details.

A significant factor is the continued use of manual SSI exchanges, which are prone to errors from transposition, and due to a lack of standardisation in taxonomy and format, are difficult to automate for ingestion by the receiving counterparty. However, errors may also occur even with the use of industry-wide automated SSI sharing solutions, due to insufficient discipline around their usage.

In April 2022, FMSB was approached by the Bank of England and FCA to continue the work begun by the Post-Trade Task Force they established. In *Charting the Future of Post Trade* the Task Force proposed recommendations to remedy these procedural inefficiencies. Amongst others, it recommended *"[S]tandardisation of data models and message formats*

[1] Charting the Future of Post-Trade - Report of Task Force - April 2022 (bankofengland.co.uk)
[2] Accelerated_Settlement_Taskforce_Report.pdf (publishing.service.gov.uk)

for the automated settlement process". Standardisation could also pave the way for future digitalisation and automation.

The proposed FMSB Standard takes forward this recommendation.

Purpose

This Standard aims to increase the adoption of electronic solutions that allow for standardisation and pre-authentication of settlement instructions, and which facilitate Straight-Through-Processing, to improve efficiency of SSI management by recipient counterparties and reduce settlement fails through incorrect SSIs.

Where such electronic solutions are not legally or operationally feasible, this Standard incorporates templates for manual sharing of SSIs which incorporate an industry-standard taxonomy (based on ISO 20022), which should minimise ambiguity around SSI data fields and allow for recipient counterparties to automate their ingestion.

Approach

FMSB creates all of its content by consensus. The FMSB working group for this Standard is chaired by Tim McLeod, Global Head of Lending & Liquidity Operations and Head of EMEA Investment Operations at Blackrock, and consists of reference data, operational, and change function representatives from FMSB members.

The manual templates have been designed in conjunction with the International Securities Association for Institutional Trade Communication (ISITC) through their Reference Data working group, with a focus on the receipt of manual SSIs by a broker from a client/instructing party or through an agent of the client who manages their settlement (e.g. custodian, prime broker, or other outsourced function).

FMSB would now like to seek feedback from a broader range of market participants to verify the outputs, and to ensure that they are compatible with manual exchanges of SSIs at other parts of the trade lifecycle.

Next Steps

FMSB invites comments on any or all of the proposed Standard and Annexes. We also encourage respondents to consider the specific consultation questions which follow. Please respond by 18 October 2024. As far as possible, please collate all responses from your organisation.

A webinar will be held between 14:00 and 15:00 (London) on 17 September 2024 to answer any questions on the proposed Standard and encourage participation in the consultation. Interested parties are invited to register their interest in attending by contacting us at the email address below.

Please address any comments or enquiries by email to: secretariat@fmsb.com.

Privacy Policy

FMSB's privacy policy can be found at www.fmsb.com.

FMSB Publishes Transparency Draft of Standard for Sharing of Standard Settlement Instructions

Consultation Questions

Part I *monitors coverage: to verify where SSIs are currently exchanged between market participants and ensure that representatives of all relevant party types have been consulted.*

Part II & III *ask for substantive views on the Templates in Annex 1, the underlying Taxonomy, and authentication options.*

Part IV *considers the Core Principles contained in the Standard.*

If your firm is involved in multiple functions and/or performs multiple actions, please indicate to which an answer relates. Multiple answers are accepted.

Part I: Trade Lifecycle and Involved Parties

Figure 1 shows a (simplified) typical trade lifecycle from left to right.

The first column shows the key participants by function types, while the second shows the types of firms which may perform these functions (they have been deliberately separated as some types of firms may perform multiple functions).

The blue stars denote where these functions are active along the trade lifecycle.

The green ticks denote whether these functions typically send and/or receive SSIs as part of the trade lifecycle.

Fig. 1

1. Please indicate which function(s) you are responding for, and which type of firm you are in columns 1 and 2 respectively. If your answer is restricted to a specific market segment (e.g. product, geographic, client type) please also indicate.

2. Please comment on the contents of Figure 1 – for example, are any functions or firm types missing and are the blue stars and green ticks accurate?

3. In line with FMSB's mandate and as highlighted in the Introduction to the Standard, the Standard and templates are intended to apply to wholesale market participants and not to retail market participants. Is this distinction appropriate? Is additional guidance required on this scope?

4. Please indicate the latest point at which you would be <u>required</u> to send and/or receive SSIs to perform your function(s).

5. Please indicate when you <u>currently</u> send and/or receive SSIs.

6. For each send or receive, please indicate:
    a. your counterparty type, how you authenticate manual SSIs, and conditions for any you determine do not need authentication.

    b. The percentage that are manual, and patterns, if any, for their distribution.

Part II: Taxonomy & Templates

The templates linked in Annex 1 of the Standard include the proposed data fields and format for manually shared SSIs. Their usage is intended to be part of the FMSB Standard, where the use of pre-authenticated industry solutions is not possible. The underlying taxonomy has been developed in conjunction with ISITC, and is consistent with ISO 20022.

The PDF smart form is intended for individual SSIs and provides guidance through filters and validation.

The Excel documents are intended for bulk additions/amendments or deletions.

1. Please indicate any changes you would make to the manual template(s):

    i. Data fields

    ii. Explanations

    iii. Ease of use of the layout

    iv. If the templates are not relevant for you, please indicate this, and why (e.g. you send 100% of SSIs to your counterparties through pre-authenticated industry solutions):

2. Do you have a preference between the file formats or do you have another suggestion?

3. Are there any other issues you see with the taxonomy or template(s)?

Part III: Authentication

The supporting materials in Part V contain a high-level illustration of vulnerabilities in the manually shared SSI process, and a non-exhaustive list of authentication options which may help to mitigate.

Authentication will not form part of the Standard.

1. Please indicate your views on the authentication options presented, either alone or together with one or more options.

    i. Do they address the vulnerabilities indicated and to a sufficient level?

    ii. Are they easy to implement and use?

2. Are there any other vulnerabilities to the authentication options provided?

Part IV: Core Principles

1. Do the Core Principles strike the right balance between promoting the early and automated communication of SSIs, and access to the market?

2. Do you agree with the scope of the Core Principles? Should the Standard cover any aspects of a recipient of SSIs and how they manage reference data?

3. For your own SSIs, what (if any) obstacles do you see to compliance with Core Principle 1?

4. If you manage clients' SSIs, what (if any) obstacles do you see to compliance with Core Principle 1?

5. Which circumstances could result in the settlement account not being identifiable by the point of trade, as referenced in Core Principle 3?

6. Compliance with Core Principle 4 is designed to give delivering counterparties sufficient parameters to identify the appropriate settlement account. In circumstances in which more than one account is capable of receiving a product, it is anticipated that clients will indicate the chosen account as a preference at the point of trade. Please provide your views.

Part V: Supporting Materials on Authentication

What is authentication?

Authentication is the process through which organisations validate the identities of individuals, applications, and services transmitting Standard Settlement Instructions (SSIs), ensuring they are authorised to conduct and finalise one or more transaction processes. In the specific context of SSIs, it is a check against unauthorised individuals directing assets towards accounts in the name of persons other than the legally contracted recipient.

Vulnerabilities

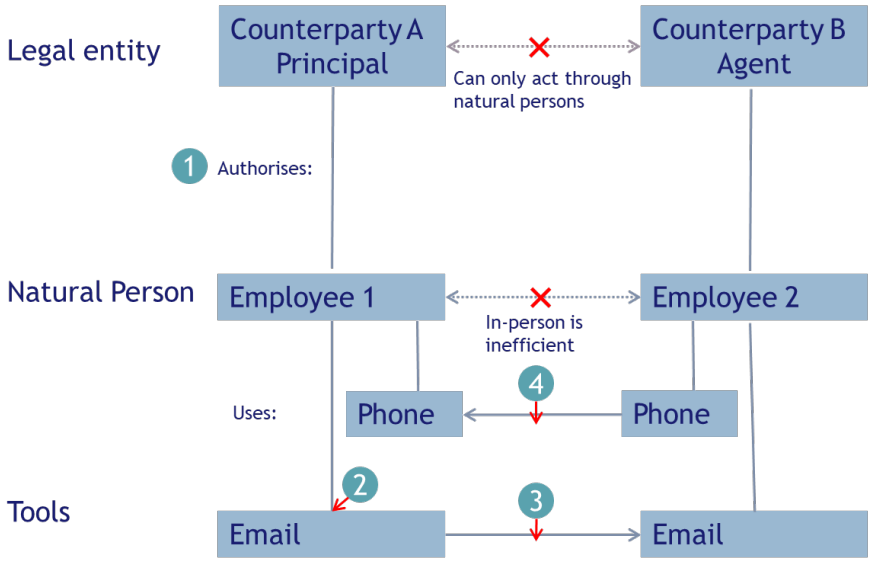

Fig.2

Securities transactions are overwhelmingly contracted between corporate persons, but as non-natural persons do not have consciousness, they rely on natural persons to act on their behalf – with exactly which actions can be performed by which natural persons delegated down from the directors of the legal entity (#1 in Fig. 2).[1]

However, contemporary volumes of trade, much of it cross-border, rule out the ability to conduct such authentication in person. Rather, authentication needs to be conducted remotely, leaving potential weaknesses, as the use of tools to facilitate these remote correspondences creates another link in the chain that is vulnerable to interception.

Market-leading SSI solutions are designed to be, and are accepted by the market as, secure. Only individuals with the authority to act on behalf of the respective entity have the access to add, amend, and delete SSI details and these details are immutable unless changed by the same individual(s). This ensures that the counterparty receiving the SSI data direct from the solution-provider can be sure that they are legitimate instructions made by the client without further investigation. Such solutions also allow changes to be

[1] As authority to contract is well-established and not unique to SSIs, this paper does not consider it in detail.

disseminated to the market at large in one go, rather than rely on bilateral updates to counterparties, and for those counterparties to automatically ingest such changes through the use of APIs.

Issues with authentication of manual instructions today

SSIs which are shared through "manual" channels e.g. email are not as secure. Several vulnerabilities arise from manual SSI authentication arrangements. These are amplified as SSIs are the first data points in a chain for settlement – in other words, for subsequent processes involving a trade, there are natural checks which will flag an incorrect account to which to settle – provided the SSI itself is accurate.

Unauthorised access to a sender's account (#2 in Fig.2), impersonation, or interception of a legitimate email (#3 in Fig.2) are all vulnerabilities which can be exploited by criminals. In addition, the lack of standardisation of manually-sent SSIs means that manual input is required by the recipient to populate their reference databases, increasing the opportunities for error, and reducing the efficiency of resources.

In order to address the risk of settlement fail, or even worse, incorrect delivery, SSIs that are not received through authorised channels must be confirmed through a "call back" (#4 in Fig.2) to the counterparty, adding a further layer of cost, inefficiency, and the potential for bottlenecks.

The use of call backs in specific scenarios is a risk appetite question for the receiving counterparty. Some firms have succeeded in eliminating call backs in certain scenarios, provided a combination of parameters are met which address the vulnerabilities listed above. The rest of this paper outlines some of these potential solutions, which firms may consider applying either separately or in tandem (multi-factor authentication).

Potential Solutions

It is assumed that legal authority is considered at the point of onboarding a counterparty; therefore, the six solutions identified below only consider vulnerabilities 2-3 identified in Fig.2.

	E-Signature	Email (TLS) encryption	Check Sum
Description	• Confirms that document has been signed electronically and is invalidated if tampered with	• "Handshake" performed to confirm security	• An SSI is passed through a function to obtain a much shorter checksum to be compared between parties
Impact	• Ensures data integrity (no tampering at #3 in Fig.2)	• Ensures data integrity (no tampering at stage #3 in Fig.2)	• Verifies data integrity - reduces time taken for checks
Availability	• Subscription by sender	• N/A – generally standard across industry	• Various open-source algorithms available
Installation	• Web-based • API • App	• N/A – generally standard across industry	• Varies
Steps Taken by Sender	• Upload document, add recipients, signature, and any other fields	• N/A – generally standard across industry	• An SSI is passed through a function to obtain a much shorter checksum to be compared between parties
Steps Taken by Receiver	• Click on email link • Click to sign	• Check for encryption on incoming message	• An SSI is passed through a function to obtain a much shorter checksum to be compared between parties
Underlying Technology	• Public Key Infrastructure	• Public Key certificate	• Varies
Legal Significance	• US: recognised in Electronic Signatures in Global and National Commerce Act ("ESIGN") and state and territory versions of the Uniform Electronic Transactions Act ("UETA") • EU: recognised in eIDAS regulation		

Vulnerabilities	• Compatibility with Excel to be explored • Email of receiver may be compromised – additional signer verification recommended • Banking and Wire Transfer Agreements are recognised as requiring further assessment	• Not immune to attacks	• Requires accuracy of entry into manual template • Does not verify data authenticity

	Signature matching	SSIs uploaded onto a site	Copy in colleagues
Description	• Physical signature of client is obtained pre-trade • E-Signature incorporates physical signature	• SSI sender uploads a copy of the SSIs onto their domain	• SSI sender to copy in a defined number of other individuals with same domain ending
Impact	• Reduces likelihood of email interception / data authenticity (no man-in-the-middle attacks at #2 in Fig.2)	• SSI receiver can immediately compare for data integrity • Domain name proves data authenticity • Reduces bottleneck for checks	• Eliminates solo bad actors
Availability	• Universal	• Any market participant with a domain name (typically all non-retail)	• Universal
Installation	• Save copy of physical signature	• Requires domain	• N/A
Steps Taken by Sender	• Attach copy of physical signature to relevant electronic document	• Upload content to existing web host	• CC other individuals
Steps Taken by Receiver	• N/A	• Open link to document	• Check email recipients
Underlying Technology	• N/A	• N/A	• N/A
Legal Significance			
Vulnerabilities	• Physical signatures may be stored on a user's computer hence compromise of an email may not be detected	• Internal controls around access to domain hosting	• Does not eliminate collusion