**Business Justification**

**for the development of new ISO 20022 financial repository items**

1. **Name of the request:**

Signed Information and Digital Certificate Notification Messages

1. **Submitting organisation(s):**

Cross-Border Interbank Payment System (CIPS Co., Ltd.)

The Bund Square, 100 South Zhongshan Road,

Shanghai 200010,

China

1. **Scope of the new development:**

This submission is concerned with a set of messages related to the signed information and digital certificate notification between participants.

The following table outlines the financial instruments, business area and business process of this request.

|  |  |
| --- | --- |
| Financial Instruments | Administration |
| Business Area | Administration (admi) |
| Business Process | Business Information |

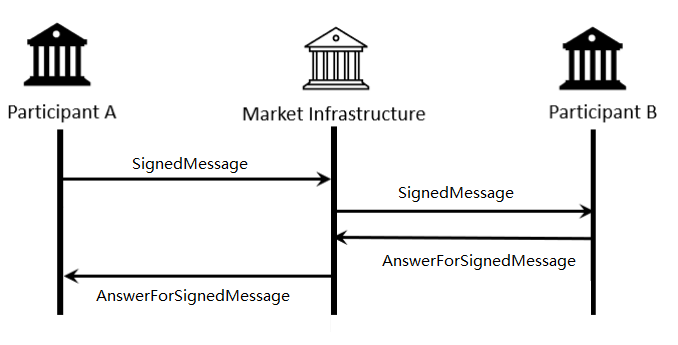
In order to get the signed information notification of participants, we will submit the below four messages:

* SignedMessage (Scenario 1)
* SignedMessage is sent from a participant to a payment market infrastructure for transmitting sensitive/ important information which need to be signed (e.g., the information data of payment notice, contact, letter of credit, collection, letter of guarantee). Without any change to the packed content, a payment market infrastructure forwards the message to another participant. After receiving the message, the payment market infrastructure/participant replies AnswerforSignedMessage.
* AnswerforSignedMessage (Scenario 2)
* AnswerforSignedMessage is sent from a participant to a payment market infrastructure as a response of SignedMessage. Without any change to the packed content, a payment market infrastructure forwards the message to a participant.
* RequestToDownloadDigitalCertificate (Scenario 3)
* RequestToDownloadDigitalCertificate is sent from a participant to a payment market infrastructure for downloading the digital certificate of all or some participants which contain the information of participant such as member code, public key of the digital certificate, the validity period of the certificate etc. After receiving the message, the payment market infrastructure replies a DigitalCertificateBindingNotice message to the participant.
* DigitalCertificateBindingNotice (Scenario 4)
* Scenario 4.1:

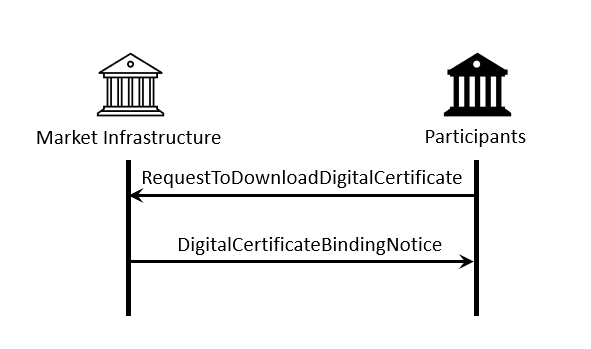
DigitalCertificateBindingNotice is sent from a payment market infrastructure to a participant after receiving a RequestToDownloadDigitalCertificate message to inform the participant about any change of digital certificate.

* Scenario 4.2:
* DigitalCertificateBindingNotice is sent from a participant to a payment market infrastructure about any change of the digital certificate such as replacing a participant’s original digital certificate with a new one, deleting old certificate etc. After receiving the message, the payment market infrastructure replies a ReceiptMessage[[1]](#footnote-1) to the participant and broadcast this message to all participants in the system. All participants reply a ReceiptMessage to the payment market infrastructure after receiving the DigitalCertificateBindingNotice message.

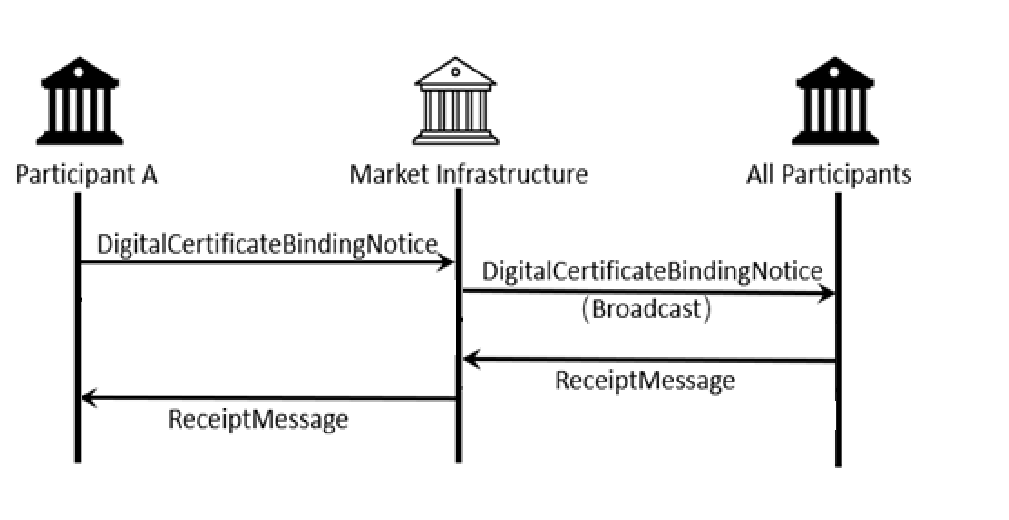
The following diagram depicts the Signed Information and Digital Certificate Notification messages flows:



Scenario 1& Scenario 2



Scenario 3& Scenario 4.1



Scenario 4.2

CIPS proposes that all SEGs and TSG should be assigned the evaluation of the candidate ISO 20022 messages.

CIPS supports optional use of BAH with all of the proposed messages.

CIPS intends to deploy the future messages in the ISO 20022 XML syntax.

1. **Purpose of the new development:**

Currently, there are no relevant ISO 20022 messages that could perform the task of system notice management in different scenarios. Developing the new messages helps to fill the existing gap and enhances the implementation of ISO 20022 in a wide range of sectors, especially payment and settlement. Thus, CIPS decides to pursue standardized and transparent messages to better manage signed information and digital certificate notification messages in the system.

Generic benefits to the industry are highlighted as follows:

* Standardise business process of signed information and digital certificate notification
* Satisfy the needs for specific business scenarios
* Develop ISO 20022 messages which can be implemented by market participants more easily and at a lower cost
* Ensure efficiency, accuracy and consistency of signed information and digital certificate transmission

1. **Community of users and benefits:**

These messages are designed to address the needs of CIPS to inform participants of signed information and digital certificate notification messages but are designed to be capable of adoption in similar contexts by other organisations as well.

Benefits and savings:

* Participants: use of a common nomenclature and terminology among participants by adopting a single standard will enhance the efficiency and transparency of signed information and digital certificate in the field of payment and settlement.
* Payment market infrastructure: mediates communication between participants by providing participants signed information and digital certificate notification. Standardized format and business information will improve the efficiency and security of signed information and digital certificate management.

Adoption scenario:

Signed Information and Digital Certificate Notification Messages were designed and successfully put into operation in CIPS system since 2015. They are currently being used by all CIPS participants. After this ISO 20022 submission has been approved, participants will continue to use these messages and the commonality of these messages will be improved.

Volumes:

As of December 2020, CIPS has more than a thousand participants using CIPS system for payment and settlement. More than 10,000 trades had been executed and use CIPS system for message transmissions on a daily basis. It is expected to be continued growth as the expanding scale of cross-border business and the growing demand for cross-border transactions.

Sponsors and adopters:

The adoption is advocated and designated as mandatory by CIPS and it is already deployed to all participants in the timeframes established.

1. **Timing and development:**

CIPS plans to complete the message develop and registration process in Q3 2022.

The Business Justification will be submitted to the RA in October 2021 and seek approval by the RMG.

Candidate ISO 20022 message models and Message Definition Report will be developed and submitted to the RA in Q1 2022.

A pilot will be organized with CIPS participants to test the candidate message in May 2022. The purpose is to ensure that the documentation of the messages is accurate and consistent and to verify that the approved messages can be implemented with no adverse effects on communication infrastructures and applications.

Candidate ISO 20022 message models and Message Definition Report will be submitted for SEG(s) review and approval in June 2022.

We know that there is no other standard initiative involved in an effort to submit a Business Justification relating to signed information and digital certificate notification.

After the whole process is completed, this message can better serve participants and can be used in a more unified way.

1. **Commitments of the submitting organisation:**

CIPS confirms that it can and will:

* undertake the development of the candidate ISO 20022 business and message models that it will submit to the RA for compliance review and evaluation. The submission must be compliant with the [ISO 20022 Master Rules](http://www.iso20022.org/documents/general/ISO20022_MasterRules.ZIP) and include a draft Part 1 of the Message Definition Report (MDR) compliant with the [template for MDR part 1](http://www.iso20022.org/documents/general/ISO20022_MasterRules.ZIP) provided by the RA, the [ISO 20022 Message Transport Mode](http://www.iso20022.org/documents/general/MessageTransportModes.xls) (MTM) that CIPS recommends to consider with the submitted message set, and examples of valid instances of each candidate message;
* address any queries related to the description of the models and messages as published by the RA on the ISO 20022 website.

CIPS confirms that it will promptly inform the RA about any changes or more accurate information about the number of candidate messages and the timing of its submission to the RA. If CIPS does not submit the candidate messages within the timing announced in section F and does not inform the RA beforehand, the business justification may lapse and require re-submission of a new business justification for approval by the RMG.

CIPS confirms that it intends to organize any testing of the candidate messages once they have been reviewed and qualified by the RA and before its submission to the SEG(s) for approval. The testing is expected to complete in May 2022 and the candidate message will be re-submitted to the RA for SEG(s) approval. CIPS confirms that it will promptly inform the RA about any changes or more accurate information about the timing of this re-submission to the RA. If CIPS does not re-submit the candidate messages as announced and does not inform the RA beforehand, the business justification may lapse and require re-submission of a new business justification for approval by the RMG.

CIPS confirms that it is committed to undertake the future message maintenance.

CIPS confirms its knowledge and acceptance of the ISO 20022 Intellectual Property Rights policy for contributing organisations, as follows.

*“Organizations that contribute information to be incorporated into the ISO 20022 Repository shall keep any Intellectual Property Rights (IPR) they have on this information. A contributing organization warrants that it has sufficient rights on the contributed information to have it published in the ISO 20022 Repository through the ISO 20022 Registration Authority in accordance with the rules set in ISO 20022. To ascertain a widespread, public and uniform use of the ISO 20022 Repository information, the contributing organization grants third parties a non-exclusive, royalty-free license to use the published information”.*

1. **Contact persons:**

* JI Chenjue [jicj@cips.com.cn](mailto:jicj@cips.com.cn)

Staff- Standardization Department, CIPS

* Weiwei Shen sww@cips.com.cn +86 21 63120212

Assistant General Manager - Standardization Department, CIPS

1. **Comments from the RMG members and relevant SEG(s) or SubSEG(s) and disposition of comments by the submitting organisation:**

**Round 1 Review**

**France:**

* The Securities SEG should be involved in the review of the message definitions (for example for the CIPS System Status Notification review) to make sure that the requested additional messages are not yet covered by existing ISO 20022 message definitions.
* Response by CIPS
* We agree that proposed messages should be reviewed by all SEGs and TSG.

**Norway:**

* Signature is relevant not only for payment/finance, but also for all other types of files containing sensitive information that needs to be signed. Hence we wonder if the message type should be camt, and if Payment SEG is the correct entity to evaluate.
* Has CIPS explored weather there are other existing, relevant standards that could be used for this purpose? It is not clear from the document weather CIPS has done so or not apart from that there is no ISO 20022 message type that can be used.
* Response by CIPS
* We agree that the message type for BJ 194 could be revised to Administration (admi).
* We have studied the existing standards and regrettably they cannot serve the purpose performed by BJ 193 and BJ 194.

**Cross SEG Harmonisation:**

* The technical nature of the message definitions could apply for any ISO 20022 business area. The Payments SEG can perform the review but it probably should be run by the other SEG groups for information as well.
* Response by CIPS
* We agree that proposed messages should be reviewed by all SEGs and TSG.

**Payments SEG:**

* The SEG who will review the candidate messages submitted by CIPS will need some support from the TSG given that these are technical messages.
* Response by CIPS
* We agree that proposed messages should be reviewed by all SEGs and TSG.

**Switzerland:**

Provided in the document below.



Response by CIPS

1. We agree that there is demand in wide-ranging ISO 20022 domains for support of signed message exchange. Given the generic nature of the proposed messages, we welcome the evaluation of the BJ by all other business SEGs.

2. The proposed messages can be used to carry information, such as business notification, letter of credit, payment collection and letter of guarantee. The elements include Transaction Type Name, Title, Content, Attachment, Attachment Content, all of which require signature. The messages are decrypted and analyzed for business purposes, and so the payment market infrastructure serves as the business actor rather than technical middleman.

3. We agree with optional support for the BAH an evaluation by TSG.

The proposed messages are generic free-style ones where signed information could be added. Signature elements are not included in the business messages and encryption mechanisms are not involved.

**Round 2 Review**

**Further Clarifications for SASFS**

**Clarifications related to BJ 194:**

1. Participant A sends an encrypted message to MI that relays the message to participant B without making any changes. MI itself could decrypt and analyze the message for business purposes.

SASFS> The behaviour described seems to imply that participant A encrypts the message with the public key of the MI (and not the public key of participant B) before sending the message to the MI. Could you confirm this?

**CIPS> Participant A signs the message with its private key before sending it to MI. MI sends the message to participant B without changing the structure and content of the message to participant B. the participant B verifies the signature with the public key of A.**

2. CIPS messages consist of message header, signature and message body.  Message header and signature are not included in the message definition of the BJ. Security key information is part of the signature. Participants uses private keys to encrypt messages and the receiving participant decrypt the message with public keys. This is in line with the conventions of payment systems and it involves no security concerns.

SASFS> The process that you describe seems to apply to the approach for signing messages (using the private key of the sender) instead of the process for encrypting messages (using the public key of the message recipient). Could you please confirm this.

**CIPS> Yes, that’s right, and we have updated the BJ as attached.**

3. The scenarios in BJ 194 are specific to PKI protocols.

4. As explained in Answer 1, MI both relays the encrypted message and analyzes it for its own purpose.

SASFS> Could you please clarify whether the MI encrypts the message to be forwarded to participant B with the public key of the receiving participant B?

**CIPS> I may have twisted the meaning in the process of translation. I should clarify that public and private keys are used for signing rather than encryption. Signature is used for preventing denial by the message sender or falsification before the message reaches the receiving party.**

SASFS> Could you also please clarify whether the message forwarded by the MI to participant B contains the signature of participant A? Can you please further clarify that there is no signature of the MI in the message to be forwarded to participant B.

**CIPS> Yes, it contains the signature of participant A. there is no signature of the MI the message forwarded to the participant B.**

5. The first encrypted message from A to the MI and the second encrypted message from MI to B are identical in terms of message structure and content.

SASFS> Can you confirm that the message ID and creation date of the message are also unchanged.

**CIPS> Yes, that’s right.**

6.Participant A uses private key to encrypt the message while participant B uses public key for decryption. Public key information is broadcast to designated participants in the payment system.

SASFS> Do you employ both encryption and signing for all messages? As stated before, the process described seems to apply to signing, not to encryption. This should be clarified.

**CIPS> Signing is applied to certain elements of a message in order to prevent falsification or denial. The clarification should be “Participant A uses private key to sign the message while participant B uses public key for verifying the signature. Public key information is broadcast to designated participants in the payment system.”**

1. ReceiptMessage is sent by the transaction administrator to a member of the system to acknowledge the receipt of one or multiple messages sent previously. The message identifier of it is camt.025.001.03(Receipt V05). [↑](#footnote-ref-1)