FOCUS NOTE

MESSAGING STANDARDS IN FAST PAYMENTS

Part of the World Bank Fast Payments Toolkit

FEBRUARY 2022

WORLD BANK GROUP

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

CONTENTS

SETTING THE CONTEXT AND BACKGROUND

SETTING THE CONTEXT

The World Bank has been monitoring closely the development of fast payment systems (FPS) by central banks and private sector players across the globe. This comprehensive study of FPS implementations has resulted in a policy toolkit. The toolkit was designed to guide countries and regions on the likely alternatives and models that could assist them in their policy and implementation choices when they embark on their FPS journeys. Work on the FPS Toolkit work was supported by the Bill and Melinda Gates Foundation. The toolkit can be found at *fastpayments.worldbank.org* and consists of the following components:

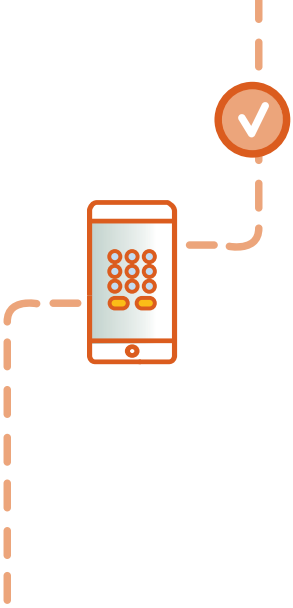
1. The main report, Considerations and Lessons for the Development and Implementation of Fast Payment Systems
2. Case studies of countries that have already implemented fast payments
3. Short focus notes on specific technical topics related to fast payments

This note is part of the third component of the toolkit and aims to provide inputs on the technical implications of messaging standards used in payment systems with a focus on fast payments. This topic is of relevance as new players enter the payment service industry and as fast payments continue to mature in many markets.

BACKGROUND

The mass adoption of fast payments and changing business dynamics around the globe have created an environment in which upgrades, along with new implementations, are becoming a key trend in the payments industry. Costs and risks are associated with such tasks, but with deep research and prior knowledge of the factors, operators can mitigate the risk and lead to benefits for society as a whole.

This technical note on messaging standards addresses the key questions that implementors face when choosing messaging standards (ISO 8583, ISO 20022, or proprietary) while implementing fast payments. The first section of this note presents a brief introduction of messaging standards. The second section presents a comparative analysis of the following aspects of messaging standards: message specification, standard characteristics, and operational capabilities. The third section analyzes the impact of messaging standards on transaction flow and processing steps, customer-authentication models, and performance and scalability. The fourth section addresses the experience of payment system operators with proprietary systems. The last section presents key takeaways and proactively provides a decision framework for choosing message formats while implementing fast payments.



1 INTRODUCTION TO MESSAGING STANDARDS

"A messaging standard defines the syntax, structure, and semantics of a family of messages that are exchanged between counterparts."[1]

A messaging standard defines the syntax, structure, and semantics of a family of messages that are exchanged between two or more parties trying to communicate and transfer information. Globally, three main types of messaging standards are used in FPS: ISO 8583, ISO 20022, and proprietary.

According to IBM, a messaging standard "defines the syntax, structure, and semantics of a family of messages that are exchanged between counterparts." These standards are necessary for allowing a common understanding of transmitted data across linguistic, regional, or system boundaries. Using a messaging standard ensures that the data exchanged is understood correctly and is machine friendly, resulting in cost reduction and efficiency. In addition, messaging standards describe the fields/data elements that are part of a message and can be used for various use cases. In some cases, the definition and usage of the hierarchical messages is also provided where multiple messages are to be exchanged between two parties.

ISO 8583

Originally published by the International Organization for Standardization (ISO) in 1987, ISO 8583 has been at the core of payment systems for many payment system operators, banks, and other financial institutions across the globe. Though usage is restricted mostly to legacy systems and processes, it is the messaging standard used most for card transactions processed globally.

Since its inception, three versions have been released—ISO 8583:1987, ISO 8583:1993, and ISO 8583:2003. The most common version remains ISO 8583:1987, which is used by dominant card-based payment providers, such as Mastercard and Visa.

The ISO 8583 messaging standard comprises the following three parts:[2]

- Part 1: Interchange message specifications
- Part 2: Application and registration procedures for Institution Identification Codes (IIC)
- Part 3: Maintenance procedures for codes

Each payment message that uses this standard is identified by a four-digit message type indicator (MTI), in which each digit has its own significance. The first digit indicates the version of the messaging standard, the second digit denotes the message class, the third digit provides the message function, and the fourth digit indicates the origin of the message. (For details on ISO 8583 MTIs and the significance of each digit, refer to appendix A.)

The Faster Payment System in the United Kingdom, Immediate Payment Service (IMPS) in India, and Transferencias en Línea (TEF) in Chile are systems that are based on ISO 8583 messaging standards.

ISO 20022

Revered as the global standard for the exchange of electronic messages between financial institutions, both for payment as well as nonpayment transactions, ISO 20022 is now the messaging standard that most FPS utilize. The ISO introduced it in 2004 to provide a standardized platform for message development in one eXtensible Markup Language (xml) rulebook.

ISO 20022 is based on a flexible framework that allows user communities and message-development organizations to define message sets on internationally agreed approaches, using business semantics. Using richer, higher standardization, quality, and carrying capacity of data than other standards, ISO 20022 easily adapts and is driving improved payment outcomes by providing both structured and unstructured data fields.

ISO 20022 has formed the Real Time Payments Group (RTPG), comprising board members from more than 17 countries, to bring international users together to create global market practices. The group's objective is to document a consistent and harmonized view of ISO 20022 message components, business processes, elements, and data content with respect to FPS in different market implementations.

ISO 20022 is very detailed and divided into 32 message types.[3] The most common types used can be understood as the following:

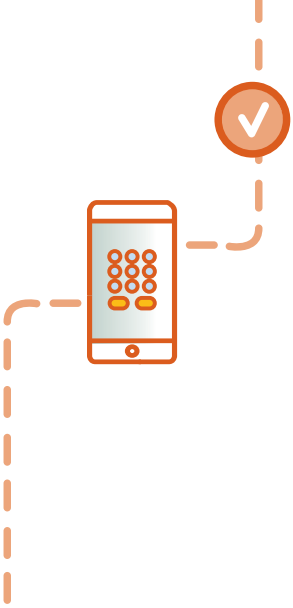
- Payment initiation (pain.XXX.XXX.XX)
- Payment clearing and settlement (pacs.XXX.XXX.XX)
- Account management (acmt.XXX.XXX.XX)
- Administration (admi.XXX.XXX.XX)
- Cash management (camt.XXX.XXX.XX)
- Payment remittance advice (remt.XXX.XXX.XX)

The Clearing House Real Time Payments (TCHRTP) in the United States, New Payments Platform (NPP) in Australia, and Fast and Secure Transactions (FAST) in Singapore are FPS that use the ISO 20022 messaging standards.

PROPRIETARY

Proprietary payment messages are a unique message format defined by a country/region/monetary authority for facilitating payments. This messaging format is generally localized and requires extensive adoption by the entire payment ecosystem to be successful. Proprietary messages can be XML based, such as ISO 20022 messages, or non-XML based, such as ISO 8583 or SWIFT MT messages. Proprietary messages offer high levels of customization and can take advantage of the acquired experience/resources of a payment system implementor, enabling common platforms and fewer user training requirements.

Both the Unified Payments Interface (UPI) in India and Sistema de Pagos Electrónicos Interbancários (SPEI) in Mexico are examples of FPS with a proprietary messaging format. Both use XML-based message formats.



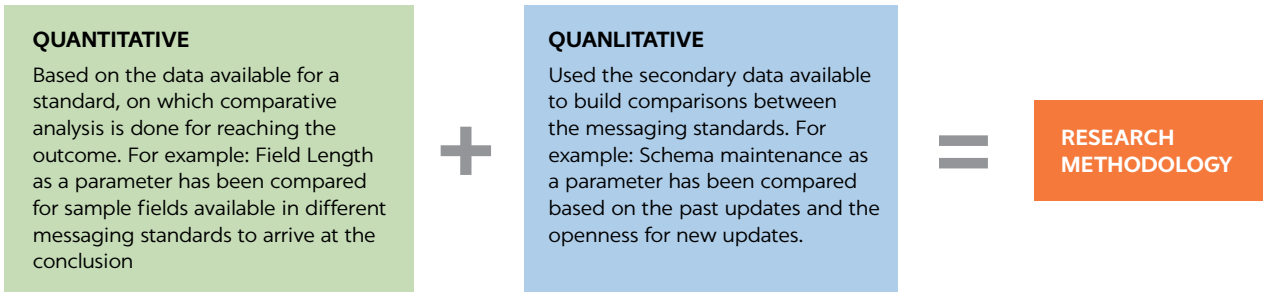
2 COMPARATIVE ANALYSIS OF MESSAGING STANDARDS

The purpose of this section is to bring out the various characteristics of the three most-used messaging standards in FPS around the world—ISO 8583, ISO 20022, and proprietary. This section is divided into two subsections: an overview of the messaging standards, with functionalities listed as lacking, basic, and/or comprehensive on the basis of each parameter examined, and detailed information backing up the summary table. The detailed analysis is done based on the 14 parameters and three categories shown in table 1.

TABLE 1 **Categorization of Parameters Used for Research on Comparative Analysis of Messaging Standards**

PARAMETER CATEGORY	PARAMETERS	PARAMETER DESCRIPTION
Message specifications	• Message format	Comparison based on the messaging standard format
	• Field length	Comparison based on the length of the most-used fields in transaction messages
	• Message size	Comparison of overall size of similar messages of different standards
	• Remittance information	Comparison of amount of remittance-information carrying capacity of a messaging standard
Standard characteristics	• Character set	Comparison of messaging standards' openness to accommodating different characters and languages
	• Message customization	Comparison of the extent of customization feasible in a messaging standard
	• Message standardization	Comparison of the extent of standardization in a messaging standard
	• Scheme maintenance	Comparison of the frequency of updates and change/maintenance requests from the standard
	• Future prospect	Predictive comparison of the messaging standards
	• Nonpayment information	Comparison of the ability to carry nonpayment information
Operational capabilities	• Interoperability	Comparison based on capability of messaging standard for multiple FPS collaborations
	• Operational considerations	Comparison of messaging standards based on convenience of operations
	• Data analytics compatibility	Comparison of messaging standards based on the ability to support data analytics
	• Ease of reconciliation	Comparison based on support for auto and manual reconciliation

FIGURE 1 Research Methodology for Comparative Analysis of Messaging Standards



2.1 SUMMARY

The comparative analysis of messaging standards is done using mixed methodology in which both quantitative and qualitative research is done to integrate perspectives.

Table 2 maps the three messaging standards against the parameters for comparison with respect to FPS. The representation is done in a way that allows the comparison of two parameters if a parameter is a benefit of more than one messaging standard.

ISO 8583 defines the majority of the fields/data elements as standard but also has a few reserved fields for passing implementation-specific information. These fields are unstructured and allow data to be entered in free-text ASCII or binary format. ISO 8583 is the standard of choice where infrastructure capabilities such as storage and network efficiency are weak, because it is smaller than other messaging standards. Recently, there have been no updates to the messaging standard; the last version was released in 2003, and no major future modifications are anticipated. The use of unstructured data, a lack of fields, such as remittance information, and limited field lengths adversely affect the standard's operational (handling customer claims, return requests, reports generation, and value-addition tasks such as new product offering) and reconciliation capabilities.

TABLE 2 Summary of Messaging Standards Based on Parameters

PARAMETER	ISO 8583	ISO 20022	PROPRIETARY
Message format	○	●	●
Field length	○	⊙	●
Message size	●	○	●
Remittance information	○	●	⊙
Character set	○	⊙	●
Message customization	○	⊙	●
Message standardization	⊙	●	○
Scheme maintenance	○	⊙	●
Interoperability	⊙	●	○
Future prospect	○	●	⊙
Operational considerations	○	●	⊙
Nonpayment information	○	●	⊙
Data analytics compatibility	○	●	⊙
Ease of reconciliation	○	●	⊙

○ Lacking ⊙ Basic ● Comprehensive

ISO 20022 is considered as the global standard for the exchange of electronic messages between financial institutions. It offers standardized messages with the capacity to carry both structured and unstructured data. Although the standard has field lengths greater than such previous standards as ISO 8583, there are also unstructured subfields present in key fields, such as address, which can be used in addition to the structured fields, thus enhancing the data-holding capacity. There are regular yearly updates for the messages in the standard, based on change requests raised by the participants and approved by a committee comprising members from various nations holding different interests. The standard fares well in the capacity to carry remittance information in both structured and unstructured format. This information can be used for auto reconciliation of invoices and helps in bookkeeping, in addition to providing support to data analytics tools. Overall, the standard is best suited when network capacity is stronger, and the requirement is to have a standardized message with a higher data-carrying capacity. As one of the most accepted international standards, it leads to high feasibility of interoperability with other schemes and systems

Proprietary messages are uniquely defined for a country/region and are best suited for addressing niche requirements. They can take up any format or structure or support

any character set. Because of this, they are preferred when local languages are to be used during a transaction. Proprietary messages are the most customizable messages; the field presence and lengths can be customized to meet local requirements, which can save considerable operational costs. Due to the extent of customization, they lack the standardization that is essential for cross-border payments, but with the use of middleware, there have been successful implementations of interoperability. Proprietary messages are the standard of choice when the implementors prefer flexibility over standardized messages, or when niche requirements cannot be fulfilled by the available messaging standards.

2.2 DETAILED COMPARATIVE INFORMATION

Each parameter evaluated for the messaging standards can be categorized as a benefit or limitation of that particular standard based on the methodology adopted. The legends below were used to summarize the comparison.

Benefit	▲
Limitation	▼
Neutral	◆
Undetermined	◇

1. MESSAGE FORMAT

Overview

This parameter compares the messages based on the format that the messaging standard follows. Both ISO 8583 and ISO 20022 have clear definitions of the message structure and fields. On the other hand, message structure and fields in proprietary messages can be defined as per requirements. While ISO 8583 has unstructured fields, ISO 20022 has both structured and unstructured fields. Proprietary messaging standards can leverage the customization and define fields to meet the requirements of legacy systems, saving translation time, cost, and effort.

A. ISO 8583 ▼

ISO 8583 has 128 fields/data elements (as defined in ISO 8583:1987, but this can go up to 192 elements, as defined in later releases) that can store unstructured data—that is, data that is in free-text format. In these data elements, the data present might not be distinguishable from the various components present. For example, in the address fields, the street name and building name might not be easily identified separate from the entered data.

B. ISO 20022 ▲

ISO 20022 offers both structured and unstructured fields. The structured fields help distinguishing the components of a field. For example, ISO 20022 has structured fields for address, which means the address field is further divided into subfields such as building number, street name, city, state, and so on. In addition to these subfields, unstructured address lines can be used to carry additional data for the user.

C. Proprietary ▲

Proprietary messages are uniquely defined, specific to an FPS for a country/region. They have the advantage of modification as per requirements but require careful analysis of current and future scope while designing the structure. In proprietary standards, format acts as an advantage, as the system can be built to match the legacy systems, avoiding the translation time, cost, and effort.

2. FIELD LENGTH

Overview

This parameter compares the standards based on the most common fields, such as name, address, amount, account number, institution, and transaction identifiers. For large data sets, ISO 8583 is limited to capturing the data in the defined fields. For example, address fields may be unable to carry the detailed address of a proprietary business where "care of" details are also present. ISO 20022 has structured fields with ample space to capture such details. For proprietary messaging standards, field lengths can be customized as per the requirements, making it a suitable option.

A. ISO 8583 ▼

ISO 8583 has shorter field length than ISO 20022, while comparison with proprietary messaging standards cannot be defined, as the field length is customizable. (For details on the ISO 8583 field lengths used for comparison, refer to appendix B.)

B. ISO 20022 ▲

ISO 20022 has a greater number of defined fields and longer field lengths than ISO 8583. Comparison with proprietary messaging standards cannot be defined, as the field length is customized to the FPS implementation requirement. (For details on the ISO 20022 field lengths used for comparison, refer to appendix B.)

C. Proprietary ▲

Proprietary messages are highly customizable. This adds the flexibility to introduce new fields and define the length to meet the requirements while implementing.

(For details on proprietary the field lengths used for comparison and taking UPI as an example, refer to appendix B.)

3. MESSAGE SIZE

Overview

This parameter is to compare the standards based on the size of message. The size of the transaction message varies with the messaging standard chosen for the scheme. Both ISO 8583 and proprietary messages are most suitable if message size is the key consideration. ISO 8583 has a small size that is largely attributed to fewer fields and a binary or ASCII data format. ISO 20022 consumes much more space than ISO 8583, while proprietary messages can be defined in a way that makes minimum tags/fields mandatory, saving on space. ISO 20022 is approximately five times bulkier than ISO 8583, while implementors of proprietary messages in Mexico claim ISO 20022 is seven times heavier than their proprietary implementation.

A. ISO 8583 ▲

The size of the payment messages is smaller in ISO 8583 format than in ISO 20022. This is due to the adoption of a binary format, along with the limited amount of information being transferred. Hence, less bandwidth is required to process these transactions.

B. ISO 20022 ▼

Message size is larger than ISO 8583. Hence, comparatively greater bandwidth is required to process transactions and may create capacity and performance issues for regions that lack good infrastructure connecting end users, payment service providers (PSPs), and the FPS operator.

C. Proprietary ▲

Message size for proprietary messages varies with the implementation, format, character sets, and type of information contained in a message. This cannot be generalized, but the implementors have the advantage of choosing the message attributes to fit the requirements and meet the data-handling capacity of the system.

4. REMITTANCE INFORMATION

Overview

Remittance information is used by financial institutions to establish the link between the transaction and the purpose of the transaction. This parameter compares the messaging standards' capability to carry remittance-related information. ISO 20022 messages are the most suitable, as they have clearly defined remittance fields, with both structured and unstructured data used for various business use cases. ISO 8583 lacks predefined remittance fields, while for proprietary messages, it depends on the implementation.

A. ISO 8583 ▼

There is no predefined remittance field, but custom fields are reserved for national use (57–60 and 112–119) and private use (61–63 and 120–127), and each field is 999 characters long. The implementors and financial institutions can use these fields to capture remittance information.

(For details on the ISO 8583 remittance information fields, refer to appendix C.i.)

B. ISO 20022 ▲

ISO 20022 provides rich remittance information in the multiple fields available at a granular level. The remittance information can be structured or unstructured or both, and it can be sent with the payment or a separate message can be sent with the remittance information of the original payment (by providing a reference to the original payment). (For details on the ISO 20022 remittance information fields, refer to appendix C.ii.)

C. Proprietary ▲

Proprietary messages have the flexibility of adding remittance information as per the requirement. Thus, implementors can choose to provide remittance information fields and customize the lengths. (For details on proprietary remittance-information fields and taking UPI as an example, refer to appendix C.iii.)

5. CHARACTER SET

Overview

Character sets are the different characters that can be used and are supported by a messaging standard. This parameter helps to establish the different characters in a messaging standard that are available for use while transmitting a payment/nonpayment transaction message. Proprietary messages are the best suite for character-set support, as local languages can also be part of proprietary messages, while both ISO 8583 and ISO 20022 do not support that. ISO 8583 is based on ASCII or binary, while ISO 20022 supports UTF-8 characters. (For a comparison of UTF-8 and ASCII, refer to appendix D.)

A. ISO 8583 ▼

ISO 8583 messages can be encoded in either an ASCII or a binary character set, where ASCII is the most-used character set. In ASCII format, the message type is four bytes long, as the ASCII-coded characters are sent as text, while in binary encoding, the message type is two bytes long.

The ASCII character set is limited to 256 characters, which might not be enough to represent different language structures.

B. ISO 20022 ◆

ISO 20022 uses XML 1.0, which supports UTF-8 (encodes characters of variable length using one to four eight-bit bytes), UTF-16 (encodes characters of variable length using two or four eight-bit bytes), and many more. Since UTF-8 is the most efficient method to transport characters lengthwise, ISO 20022 uses only UTF-8. The only exception is exotic characters, for which UTF-8 becomes lengthier, but these characters are rarely required in ISO 20022 messages.

ISO 20022 does not support local languages, for which a workaround needs to be crafted. For example, to continue the use of local languages and special characters in implementation in the Single Euro Payments Area, a broader character set was defined, along with a conversion table and best practices, while migrating to ISO 20022.

C. Proprietary ▲

Proprietary messages are advantageous in that the user can choose the character set and is not bound by an external entity governing the messaging standard. This means that proprietary messages can support local characters that are otherwise not supported by ISO 8583 or ISO 20022. For example, UPI in India supports the UTF-8-character set.

6. MESSAGE CUSTOMIZATION

Overview

This parameter takes into consideration the ability to customize a messaging standard to adapt and implement any specific requirement or use case. Proprietary messages are the most customizable message formats, permitting the implementor to customize at the most granular level according to the requirements, while both ISO 8583 and ISO 20022 are governed by an international body, thus making changes to the structure/fields difficult, as the changes go through various levels of review and approval.

A. ISO 8583 ▼

ISO 8583 provides limited options for customization, as it defines many standard fields that remain the same in all systems. It provides only limited fields for passing network-specific details. For adapting the standard for own use, the network-specific fields are used to provide custom usages.

The fields 57–60 and 112–119 are reserved/available for national use, and fields 61–63 and 120–127 are reserved for private use. Only these fields can be used to carry proprietary information not included in the defined fields.

B. ISO 20022 ▼

ISO 20022 defines a standard set of fields, tags, and the structure of the message, with limited customization options. The customization comes into play when implementing schemes, when the optional fields are made mandatory at the scheme end as per the business use cases.

ISO 20022 also provides some unstructured fields, which can be used to capture information for which structured fields are not present or information is bigger than the space provided. In addition, based on the implementor, a type of message can have different purposes. For example, pacs.008 with structured remittance information carrying the unique transaction code of the original transaction acts as a payment return message in RTP in the United States, while returns are done using pacs.004 message in NPP in Australia.

C. Proprietary ▲

Proprietary messages are the most customizable messages and are not governed by an external organization. This permits solutions to be implemented for the requirements in any phase of the FPS without external interference and certifications required. For example, UPI in India has tags to capture the geocode, location, IP, operating system, and so forth of both the payee's and the payer's mobile devices used to make the transaction.

Key Takeaways

Proprietary messages are the most customizable message formats, permitting the implementor to customize at the most granular level according to the requirements, while both ISO 8583 and ISO 20022 are governed by an international body, thus making changes to the structure/fields difficult, as the changes go through various level of review and approval.

7. MESSAGE STANDARDIZATION

Overview

This parameter highlights the level of standardization in a messaging standard. Message standardization makes it easier for interoperability and ease of access/understanding for users using different FPS systems. ISO 20022 is the most standardized message, with predefined structure, syntax, and format, followed by ISO 8583 and proprietary messages.

A. ISO 8583 ▲

ISO 8583 defines many standard fields (data elements) that remain the same in all systems. ISO 8583:1987 (the most common version) has a total of 128 data fields, of which 96 fields are standardized—that is, they are defined by the standard and, hence, have the same meaning in various implementations.

B. ISO 20022 ▲

ISO 20022 is more standardized than the other two types of messages. The business message syntax is internationally agreed, and developers and user organizations make use of common message structure, form, and meaning to exchange transaction information globally. As the standard is not controlled by a single interest or party, anyone in the financial services industry can use it.[4]

ISO 20022 created the RTPG with the objective of bringing members of the international payments community together to focus on standard market practices. The focus is to build a global market practice for ISO 20022 in a retail real-time system by providing foundation-level usage guidelines that can be enhanced as per the requirements. It covers different real-time payment use cases covering overlay services and request-to-pay transfers besides the basic credit transfer.

(For details on the scope of the RTPG, refer to appendix E.)

C. Proprietary ▼

Proprietary messages are the least standardized messages. Even if they are built on the same messaging format, language, or structure, integrating a proprietary system with another proprietary or standardized system requires extensive research and a compatibility check.

8. SCHEME MAINTENANCE

Overview

Schema maintenance is used for providing regular updates, fixing bugs, and addressing new/changed requirements. This parameter compares the messaging standards on the openness for schema maintenance. Schema maintenance is the easiest with proprietary messages due to localized development and maintenance, followed by ISO 20022, where yearly updates are provided based on open change requests. ISO 8583 is the least favorable because of a lack of updates in recent years.

A. ISO 8583 ▼

Version updates of ISO 8583 are infrequent, and there are only three versions: 1987, 1993, and 2003. This means that the schema is not changed easily with changes in business requirements. In addition, a new version does not imply that organizations using the standard need to migrate to new version. A classic example is ISO 8583:1987: the oldest version is most widely used. This version is used by Visa and Mastercard.

B. ISO 20022 ▲

Considering the vast scope covered by ISO 20022, the authority publishes regular updates. In general, there are yearly updates at the message-type level, rather than the entire set of messages. The updates are done based on the change requests shared by the partner, and since the standard is governed by a central entity, the updates are done at the global level.[5]

Only those change requests that are approved are included in the future versions of a message type. This means that if country- or region-specific changes are to be made, they might not be included in the standard, leaving little room to accommodate such changes.

A new version of a message type may not necessarily mean that the participants need to migrate to that version. It is on the payment operator of the schemes to decide to take action. If the payment operator does not migrate to the newer version, the operator risks skipping the new features and the change requests as part of the release. In addition, in case of interoperability, if one of the party migrates but the other doesn't, translators would be required to find common ground between the parties.

C. Proprietary ▲

Proprietary messages are the most flexible in terms of schema maintenance, as they can be updated as and when the requirement changes for the region/payment operator. They are not governed by an international entity; thus, the changes are at a local level and, hence, require less scrutiny and research into the impact of these changes.

On the other hand, building and maintaining a proprietary solution would involve considerable time, cost, and effort. Proprietary standards need to maintain an appropriate level of governance and schema management frameworks. If the scheme lacks documentation and processes for business continuity, coding is inherently opaque and hard to understand.

9. INTEROPERABILITY

Overview

Interoperability in this context refers to two or more systems communicating with each other so that participants/users from one system can transact with participants/users in the other systems participating in the interoperability arrangement. Because of the standard-

ization, the availability of a vast number of fields, and the capacity to carry structured data, ISO 20022 is most favorable for interoperability, while proprietary messages would require translators/converters/development for interoperability, making them least favorable.

A. ISO 8583 ▼

ISO 8583 has unstructured fields and an absence of predefined key fields, assisting cross-border payments. Due to the absence of structured fields, the data interpretation may not be the same in different countries/regions. For example, assuming "ABCDE" is a building that is a restricted entity in the creditor's country, when data such as "ABCDE Avenue" (that is, the name of the street not linked to the building ABCDE) is entered in the unstructured address field for the transaction, it may lead to a false anti-money-laundering or sanction hit in case of interoperable systems. SWIFT[6] estimates that approximately 10 percent of international payments are delayed for compliance checks as false positives and wasted investigations. That is a significant volume; a marginal decrease could save organizations considerable operational costs and enable faster international payments for customers.

No examples of collaboration between two FPS operating on ISO 8583 are known.

B. ISO 20022 ▲

ISO 20022 is the preferred method for interoperability due to standardization and wide acceptance. One of the key improvements over other standards and steps toward interoperability is the implementation of structured address fields. With defined and consistent fields such as Street Name, Building Number helps prevent false positive sanction hits. For example, assuming "ABCDE" is a building that is a restricted entity in the creditor's country, when data such as "ABCDE Avenue" (that is, the name of the street not linked to the building ABCDE) is entered in the ISO 20022, it will be entered in a structured street field. With the help of that field, the sanctions system can easily identify and differentiate it from the restricted entity.

A common messaging format and business process standards are the backbone for a payment system with lower operational complexity and greater consistency.

The following are examples of live ISO 20022 interoperable systems:

1. PromptPay (Thailand) and PayNow (Singapore) in April 2021
2. PromptPay (Thailand) and DuitNow (Malaysia) in June 2021

While various payment systems are eyeing interoperability by leveraging common standards, the use of ISO 20022 provides further flexibility in implementation. For example, solution operators and service providers that implement ISO 20022 standards may employ various types of data elements that meet their specific use cases, and these elements may vary across different geographies or different types of users that need to interact with each other.

C. Proprietary ▼

Proprietary messages are least interoperable because they are more localized than standardized. To be interoperable with the proprietary messages, either party or both parties in the FPS interoperability arrangement need to use translators to have a common communication medium between them. For example, UPI, which is based on the XML format, has tags that are different than those in ISO 20022 or another proprietary implementation; hence, for such interoperability, a translator is required to map the messages between the two payment schemes. In addition, the complexity increases with variance in mandatory and nonmandatory fields.

However, there are examples of integration of BHIM UPI with Singapore, where the integration is done based on the QR code. Any UPI user can scan a code at a merchant registered with NETS to accept UPI payments and make the transactions. The payments are debited in Indian rupees, while the merchant is credited in Singapore dollars.

UPI in India has integrated with the National Electronic Toll Collection (NETC) platform in India to allow seamless recharging of the prepaid toll-payment device FASTag by initiating the transaction directly from the BHIM UPI application. The user needs to enter the UPI ID in a predefined format (Vehicle_number@Issuer Bank) and directly add the recharge amount with the help of PIN authentication. The transaction flows between two different platforms that have their own defined messaging standards.

10. FUTURE PROSPECT

Overview

This parameter helps examine the future prospects of a messaging standard and what to expect from the standard in the near future. ISO 20022 is emerging as a global standard since it has the ability to adapt to new technologies and advancements in the payments domain, while proprietary messaging standards would be the standard of choice when the requirements are niche and not generic.

A. ISO 8583 ▼

ISO 8583 is an international standard for payments originated from cards. It also has deep roots in the banking industry, and it would require considerable investment to migrate away from it.

In the fast payment space, there are examples such as PromptPay in Thailand, where, rather than migrating all at once to ISO 20022, the implementors have granted flexibility to participants to migrate at their own pace. In the transition period, translators are being used to convert ISO 8583 messages originated from financial institutions to ISO 20022, so that all parties in a transaction are on the same ground. There are also examples such as TEF in Chile, which has no plans to migrate to another standard and will continue using the standard for its existing FPS system.

No major changes are expected in the ISO 8583 format.

B. ISO 20022 ▲

ISO 20022 is emerging as an open global standard for payments data and is the expected future standard of fintech innovation and competition.

- ISO 20022 has formulated the RTPG to deliver usage guidelines for ISO 20022 as a global market practice for retail real-time payments. The group is currently focused on interbank payment messaging but plans to cover payment initiation, settlement, and remittance data as well.
- ISO 20022 utilizes a rich data format promising higher quality than other standards. This leads to improved payment outcomes that adapt to new requirements and are not controlled by a single beneficiary/user/party but representatives from different parts of the globe.
- ISO 20022 banks on more transparency and better remittance information for customers than other standards. This means improved analytics, less human intervention, accuracy in compliance processes, and the performance of multilevel fraud checks. All this leads to enhanced customer experience.
- A foundation for end-to-end automation, leveraging a single standard for all business domains and processes, leading to enhanced straight-through processing (STP).
- According to SWIFT,[7] almost 200 market-infrastructure-driven initiatives are implementing the ISO 20022 standard or are considering adopting it for payments and securities-transformation projects.
- Further, rich payment data allows digital reconciliation. This offers banks the opportunity to reevaluate their business models and market positioning.

C. Proprietary ▼

Proprietary messages are being used by countries/operators that want to leverage their existing infrastructure or have specific requirements that cannot be met by using the global standards—for example, capturing details about the mobile devices used for transactions done by UPI (such as the geocode, IP, operating system, and so on) that cannot be captured by either ISO 8583 or ISO 20022. Such requirements can be met only by using proprietary messages, and, thus, the implementors rely heavily on proprietary messages. As today's world is moving toward interoperability and cross-border payments, the requirement is to build an inclusive system where exclusive fields (unavailable in other standards) should be nonmandatory.

11. OPERATIONAL CONSIDERATIONS

Overview

This parameter distinguishes the standards based on the operational factors, abilities, or issues related to the working of systems implemented using the three different messaging standards. ISO 20022 is a heavier message but comes with benefits such as easier troubleshooting, compliance with global standards, and so on, while ISO 8583 is a lighter message that is harder to operate because of format and structure limitations. Proprietary messages cannot be generalized but, in general, are designed to comply with local standards and context.

A. ISO 8583 ▼

- ISO 8583 messages are lighter and require less bandwidth and storage space.
- ISO 8583 troubleshooting is difficult, as ASCII or binary digits need to be converted to drive meaning.
- ISO 8583 uses consistent standards, resulting in fewer processing errors.
- A lack of predefined remittance fields leads to higher manual interventions in case of reconciliation and returns.

B. ISO 20022 ▲

- With ISO 20022, troubleshooting and maintenance are faster, as the standard employs flexible and modern technologies and a globally accepted language, resulting in simpler translation.

- ISO 20022 uses consistent standards, resulting in fewer processing errors.
- Since ISO 20022 is a standard format, it allows faster deployment with less customization per financial institution.
- ISO 20022 allows the use of rich data sets to drive compelling business intelligence.

ISO 20022 complies with changing global requirements, such as requirements from the Financial Action Task Force, anti-money-laundering and know-your-customer requirements, extended remittance data, and so on.

C. Proprietary ◇

Proprietary messages may/may not have structured data, definite positions, or format. This plays a major role in operational considerations.

- Proprietary messages can make it easier to comply with the local anti-money-laundering and know-your-customer checks (wherever applicable).
- Based on the message structure, definition, and availability of documentation, the troubleshooting and handling can be made easier.
- Proprietary messages are generally not supported out of the box by automated reconciliation software and are tweaked to meet these requirements.

12. NONPAYMENT INFORMATION

Overview

Nonpayment information as a parameter relates to the ability of a messaging standard to be used outside the actual transaction (payment) message. Nonpayment information is available in both ISO 8583 and ISO 20022, while proprietary messages can also implement it. The extent of detail and number of messages are higher in ISO 20022 than in ISO 8583, giving an advantage to the former. On the other hand, for proprietary, these messages need to be built but can be effective in meeting specific requirements.

A. ISO 8583 ◆

ISO 8583 has limited nonpayment messages,[8] which are available under the following categories:

- X5XX: Reconciliation message
- X6XX: Administrative message
- X7XX: Fee collection message
- X8XX: Network management message

B. ISO 20022 ▲

ISO 20022 has made different nonpayment messages available for use. These nonpayment messages are used for such purposes as reconciliation, cash management, and account management. The following are the most commonly used nonpayment messages[9] in faster payment implementations across the globe:

- camt.054: Bank to customer debit credit notification
- camt.055: Customer payment-cancellation request
- camt.056: Financial institution to financial institution payment-cancellation request
- pain.002: Customer payment status report
- remt.001: Remittance advice
- admi.001: Administration message

C. Proprietary ▲

Proprietary messages have the flexibility to build nonpayment information messages specific to a task (such as name verification) and may skip the implementation of an entire set of messages. For example, UPI in India has an application programming interface named "Check Txn Status" that allows PSPs to request the status of the transaction after the specified timeout period.

13. DATA ANALYTICS COMPATIBILITY

Overview

This parameter analyzes the openness of a messaging standard to integrate with data analytics tools to provide useful insights for the transactions being made using the implemented FPS. The more structured the data, the better its readability by humans and machines and, hence, the better the analytics. Thus, ISO 20022 is the most suitable when data analytics is the key deciding factor, followed by proprietary standards and ISO 8583.

A. ISO 8583 ▼

ISO 8583 uses "free-format" fields to define supporting information related to a transaction. This limits the extent of data that can be collected in a standard format for performing contextual analysis, thus hindering the data analytics capability. For example, analytics could be used to analyze customer demographics and make offerings. Since the address fields are free format, extracting regions or cities would be difficult.

B. ISO 20022 ▲

ISO 20022 leads to more efficient financial messaging by standardizing and harmonizing payments message formats.

It increases STP rates while simplifying cost-intensive processes such as payment processing, data analytics, transaction investigation, and reporting.

ISO 20022 allows three times more data storage than previous standards, such as ISO 8583. This provides improved data management, along with formulating dashboards, which provide essential insights that give a competitive advantage to implementing institutions.

Regulators, reporting firms, market watchdogs, and customers require unambiguous data for analysis. For this, they place confidence in the rich and structured data provided by ISO 20022 messages.

The combination of the ISO 20022 migration, which creates usable data, and the analytics that could be applied to this data has the potential both to increase significantly the access of the unbanked to financial services and to create new revenue streams.

C. Proprietary ◇

Data analytic tools use historical data, and the insights are applied to the current business to provide better services, which directly relates to better revenue. To reap the benefits of data analytics, the more structured the data, the clearer the insights. Since proprietary systems do not have a defined format/structure, compatibility with data analytics tools increases as the data becomes more structured.

14. EASE OF RECONCILIATION

Overview

Reconciliation is used to compare two set of records for correctness and agreement with each other. This parameter is used to compare the messaging standards based on reconciliation capability and the use of automated reconciliation tools. In the context of financial institutions, reconciliation is comparable, as the basic details required and shared are the number of records, the total amount, and the differential, in the case of deferred settlements. In this section, the customer-reconciliation capabilities of messaging standard will be compared. Reconciliation is easier when detailed information is present. Hence, ISO 20022 is more suitable when reconciliation is the deciding factor, followed by proprietary standards and ISO 8583.

A. ISO 8583 ▼

Reconciliation is a cross-check method or a bookkeeping method that requires detailed data for better understanding and readability. For a business customer (such as a merchant), accurate details mean a clear picture of the business, including cash flows, strengths, and improvement areas, while for individuals, it helps in expense and cash management. ISO 8583 relies heavily on unstructured data and lacks predefined remittance fields, restricting the standard's ability to provide rich data, lowering the automated reconciliation potential. Techniques such as implementor's guidelines on the usage of separators, or specifying positions in fields to distinguish the different elements present, can aid reconciliation.

B. ISO 20022 ▲

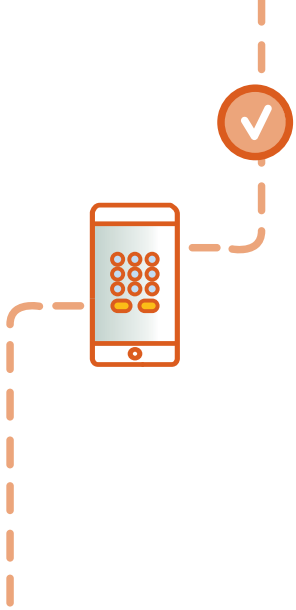
Reconciliation is easier when the data is structured, and remittance fields are available.

ISO 20022 helps customers in automated account reconciliation or payment management "on behalf of" other parties because of the large remittance data that can be carried with the payment messages. Enabling easier and quicker exchange of data between customers, service providers, and technology partners, ISO 20022 will further help to meet the objectives of open banking.

ISO 20022 with ERI (extended remittance information) allows the addition of detailed information about a transaction, including linked documents, line items, extending the automated reconciliation potential.

C. Proprietary ◇

Reconciliation for a proprietary messaging standard is subject to the implementation of the messaging standard. If the messaging standard has structured data, reconciliation is comparatively easier and automated tools can be deployed. If the messaging standard is unstructured, it would aid the process of automated reconciliation if a country/region would define the positions/fields in the message that would be used for reconciliation. If the data is unstructured and no defined places are available, then automated reconciliation cannot be done. Hence, reconciliation for proprietary standards largely depends on the implementation of the format and cannot be generalized, but proprietary messages give the flexibility to change the structure of a message to meet this requirement.



3 PROXY DATABASES

The choice of a messaging standard has huge implications on the transaction flow and processing steps, customer authentication, and performance and scalability in FPS. This section is divided into three subsections: (i) linkage between transaction flow and processing steps with messaging standards; (ii) customer-authentication models; and (iii) system performance and scalability.

The subsection on linkage between transaction flow and processing steps with messaging standards assesses the impact of the choice of a messaging standard by utilizing the four major payment flows, based on which multiple use cases can be developed to meet the business requirements.

The subsection on customer-authentication models assesses the impact of the choice of a messaging standard by analyzing the fields available for carrying the customer-authentication details.

The subsection on system performance and scalability assesses the impact of the choice of a messaging standard by analyzing four specific aspects—message size, STP, data truncation, and the addition of new use cases.

3.1. LINKAGE BETWEEN TRANSACTION FLOW AND PROCESSING STEPS WITH MESSAGING STANDARDS

In general, the entire payments transaction, from initiation to completion, occurs seamlessly in a few seconds. A transaction takes a lot of intermediate steps, including exchange of communication messages between multiple participants for transaction closure. Transaction flow between participants varies in different payment schemes and depends on the use cases and design implemented. However, the exchange of transaction messages and corresponding data fields depends on the messaging standard adopted as part of implementation.

The three most widely implemented transaction flows in FPS have been detailed here to represent the linkage between transaction flows and processing steps with the choice of messaging standards. These flows can be leveraged to enable multiple business use cases as per the design requirement during implementation. In addition, these flows can be implemented in multiple ways, and different messages provided by a messaging standard can be used to achieve the same outcome. Here, indicative processing steps for transaction flows are illustrated, while alternatives, such as clubbing two processing steps into one or using alternative routes, are always feasible.

With a shift toward the inclusion of nonfinancial institutions in the payment infrastructure, these players enable a wider range of customer services and features by riding on the FPS. These nonfinancial institutions are represented either as third-party players in some regions or as overlay service providers in other regions. These third-party players or overlay service providers can be represented along with channels in the transaction flows presented below and connected to a financial institution's core payment engine to enable use cases. The messaging standard for communicating between a channel and a financial institution's core engine is defined by the financial institution or central payment scheme, and the same is leveraged by these third-party or overlay service providers to integrate with the ecosystem.

The following flows are used in the document:

1. **Proxy verification/resolution flow:** Proxies or aliases make payments easy by replacing the complicated and long account/card details with a simple proxy/virtual address to transfer funds or initiate other financial or nonfinancial transactions. User account details are mapped to unique proxies such as mobile numbers, email addresses, or user-defined proxies. As part of the transaction flow, a name or other details are pulled from the payment scheme against the proxy for the initiator to verify the correct destination party.
2. **Successful/rejected transaction flow:** These are typical flows of a real-time credit transfer transaction in which the transaction initiated by the debtor is successfully credited to the customer. Or the creditor financial institution rejects the transaction because of issues such as when the creditor's account is incorrect, closed, or dormant, or some other restriction is placed on the creditor's account.
3. **Request-to-pay flow:** This flow can be used to cover use cases in which a customer of a financial institution requests a payment from another customer—for example, a merchant requesting funds from a customer for services offered by the merchant.

(For details on the ISO 8583 and ISO 20022 message types and the fields used in the flows below, refer to appendix F.i and appendix G.i, respectively.)

3.1.1 Proxy Verification Flow

1. ISO 8583

A customer initiates a transaction from the channels using proxy or alias details of the creditor party using a proprietary format or X200 messages. The proxy ID details need to be verified, and creditor details such as name need to be fetched, to verify the creditor before a transaction is processed. The debtor's core payment engine sends an X200 message to the FPS, filling in proxy ID details using standard or private fields. This X200 message is then forwarded to the creditor's financial institution, which responds with an X210 message carrying the verification response. The FPS then sends this response message back to the debtor's financial institution. The proxy verification can be performed by either the FPS or the creditor's financial institution (as indicated in the flow), based on the implementation design of the FPS.

(For details on the processing steps, messages used, and important fields, refer to appendix F.ii.)

2. ISO 20022

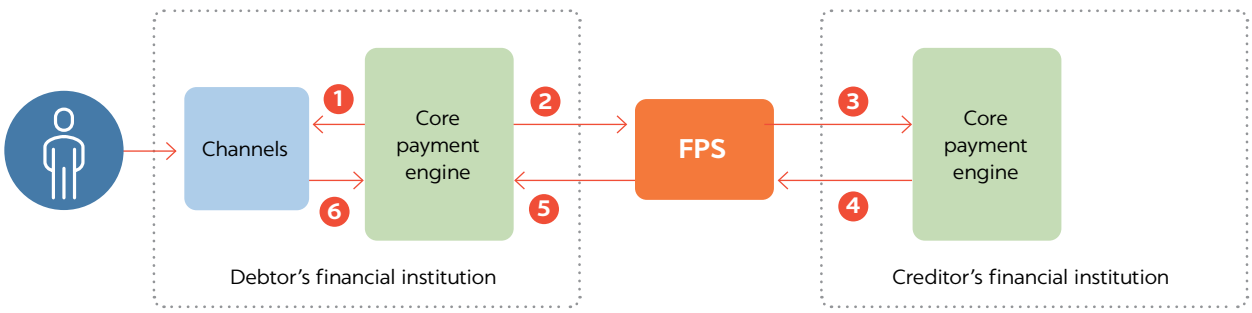
A customer initiates a transaction from the channels using the proxy or alias details of the creditor party. The proxy ID details need to be verified, and creditor details such as name need to be fetched, to verify the creditor's identity before a transaction is processed. The core payment engine sends an acmt.023 message to the FPS, filling in proxy details. This acmt.023 message is then forwarded to the creditor's financial institution, which responds with an acmt.024 message filling in the proxy verification details. The FPS then sends this response message back to the debtor's financial institution. The proxy verification can be performed by either the FPS or the creditor's financial institution (as indicated in the flow), based on the implementation design of the FPS.

(For details on the processing steps, messages used, and important fields, refer to appendix G.ii.)

3. Proprietary

A customer initiates a transaction from the channels using the proxy or alias details of the creditor party. These details need to be verified, and creditor details such as name need to be fetched, to verify the creditor's identity before a transaction is processed. The core payment engine sends a proxy verification message to the FPS with proxy ID details. This message is then forwarded to the creditor's financial institu-

FIGURE 2 **Proxy Verification Flow: Request Initiated by the Debtor for New Transaction**



tion, which responds with the proxy verification and creditor details. The FPS sends this response message back to the debtor's financial institution. The proxy verification can be performed by either the FPS or the creditor's financial institution (as indicated in the flow), based on the implementation design of the FPS.

(For details on the processing steps, messages used, and important fields, refer to appendix H.i.)

3.1.2 Successful/Rejected Transaction Flow

1. ISO 8583

A payment initiated by a customer using channels of the debtor's financial institution using a proprietary format or X200 messages is forwarded to the core payment engine. The core payment engine sends an X200 message to the FPS, which, after validation, is passed to the creditor's financial institution. The creditor's financial institution processes the message and sends back a response to the FPS, using X210 messages. The response message could be positive (that is, all the details are correct and the customer can be credited) or negative (that is, the customer cannot be credited). This message is be passed by the FPS to the debtor's financial institution, which takes action on the transaction based on the response received and notifies the customer.

Please note: In most implementations, there is no step 5 (from the scheme to the core payment engine of the creditor's financial institution) in the flow using an ISO 8583 message—that is, the creditor's bank settles the customer's account and then sends a response to the scheme if the transaction is successful. The same approach has been followed here.

(For details on the processing steps, messages used, and important fields, refer to appendix F.iii.)

2. ISO 20022

A payment initiated by the customer at channels is forwarded to the core payment engine using proprietary format messages or ISO 20022-specific pain.001 messages. The core payment engine sends a pacs.008 message to the FPS, which, after validation, passes it to the creditor's financial institution. The creditor's financial institution processes the transaction and sends back a pacs.002 message to the FPS. The response message could be positive (that is, all the details are correct and the customer can be credited) or negative (that is, the customer cannot be credited). On receipt of a positive pacs.002 message from the creditor, the FPS sends an FPS-generated pacs.002 message to the financial institutions of both the debtor and the creditor for posting to their customer's account. Otherwise, a negative pacs.002 message is sent to the debtor's financial institution, stating that the transaction was rejected.

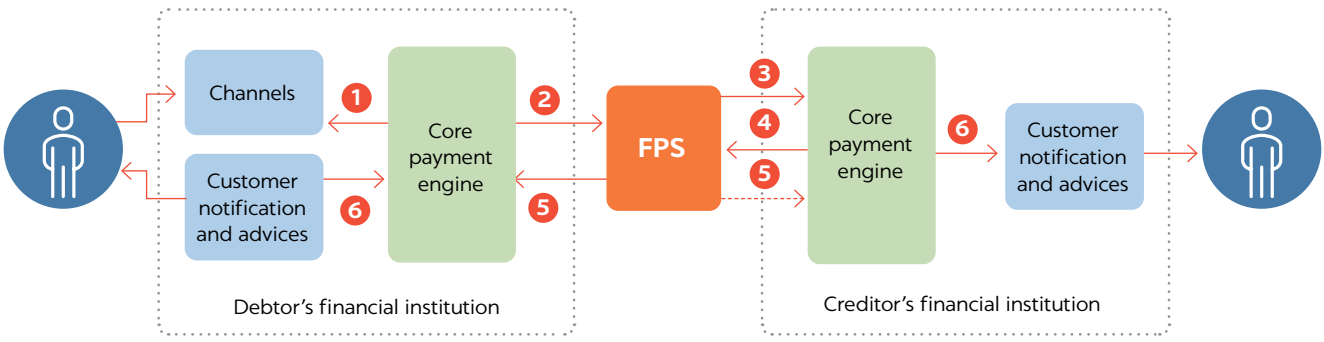
(For details on processing steps, messages used, and important fields refer to appendix G.iii)

3. Proprietary

A payment initiated by the customer at channels is forwarded to the core payment engine. The core payment engine sends a proprietary credit-transfer message to the FPS, which, after validation, passes it to the creditor's financial institution. The creditor's financial institution processes the transaction and sends a confirmation message back to the FPS. The response message could be positive (that is, all the details are correct and the customer can be credited) or negative (that is, the customer cannot be credited). On receipt of a positive confirmation message from the creditor, the FPS sends an FPS-generated settlement message to the financial institutions of both the debtor and the creditor for posting to their customer's account. Otherwise, a negative confirmation message is sent to the debtor's financial institution, stating that the transaction was rejected.

(For details on the processing steps, messages used, and important fields, refer to appendix H.ii.)

FIGURE 3 **Successful/Rejected Transaction Flow: Request Initiated by the Debtor for New Transaction**



3.1.3 Request to Pay

1. ISO 8583

This flow is unavailable in the ISO 8583 messaging standard out of the box.

2. ISO 20022

A customer raises a request for payment using channels provided by a financial institution. The core payment engine sends this message to the FPS in the form of a pain.013 message, and the FPS, after validation, passes it to the debtor's financial institution. The debtor's financial institution notifies the customer and requests an authorization. The authorization response is sent back to the core payment engine, which sends a pain.014 message back to the FPS. The FPS forwards the response to the creditor's financial institution, which notifies the customer.

If the debtor agrees to pay, the debtor's financial institution raises a new transaction on behalf of the customer, and the flow is similar to a successful transaction flow. Otherwise, no action is taken, and the return request is closed.

(For details on the processing steps, messages used, and important fields, refer to appendix G.iv.)

3. Proprietary

A customer raises a request for payment by using channels provided by a financial institution. The core payment engine sends this request to the FPS in the proprietary format. After message validation, the FPS passes it to the debtor's financial institution, which notifies the customer and requests an authorization. The authorization response is sent back to the core payment engine, which sends a proprietary authorization response back to the FPS. The FPS forwards the response to the creditor's financial institution, which notifies the customer.

If the debtor agrees to pay, the debtor's financial institution raises a new transaction on behalf of the customer, and the flow is similar to a successful transaction flow. Otherwise, no action is taken, and the return request is closed. (For details on the processing steps, messages used, and important fields, refer to appendix H.iii.)

3.2 CUSTOMER-AUTHENTICATION MODELS

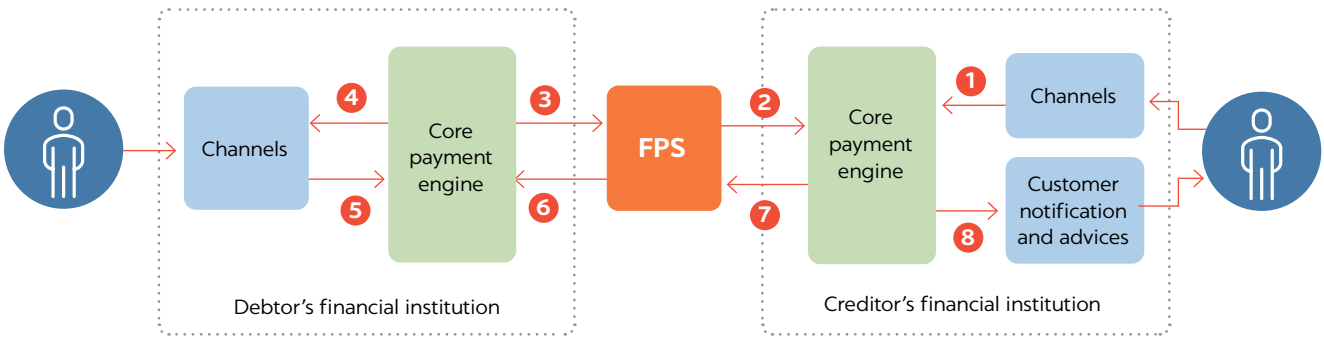
In a world of digital payments, a customer holds several financial accounts with a single or multiple PSPs. For these accounts, the first layer of security ensured by the service provider is by authenticating customers before giving them access to their account. The most common factors for authentication are passwords, PINs, and other knowledge-based identifiers. Financial institutions are innovating the use of new factors, such as inherence (such as biometrics) or possession (such as using security tokens as time-bound dynamic codes), even combining different factors to enhance security.

Customer-authentication factors can be classified into the following broad categories:

a. **Something the customer has (possession factors):** These factors include items that are physical objects, such as smart cards, smart phones, mobile binding, hard or soft tokens, keys, and so on. These factors rely on a unique string of random characters, numbers, or letters generated using predefined algorithms or real-time random character generators. This string is then used to access the system, rather than the credentials, provided the customer already has the required permissions.

b. **Something the customer knows (knowledge factors):** These factors include memory-based items such as passwords, combinations, and PINs that are used to authenticate a customer. These are the most widely used authentication factors. They rely on letters, numbers, strings, or special characters, or combinations of them, in a case-sensitive format. The substitute for a customer-controlled, static, knowledge-based authenticator is a dynamically generated one-time password, which is valid only for a limited period.

FIGURE 4 Request-to-Pay Flow: Request Initiated by the Creditor



c. **Something the customer is (inherence factors):** These factors refer to biometric authentication, in which parts of the human body—the face, fingerprints, and so on—are used to authenticate a customer. Biometric authentication relies on the unique biological characteristics of an individual. Its higher adoption rate lately is attributed largely to user convenience and resistance to spoofing. Biometric authentication does not require the physical aspect that a customer presents to match a stored copy exactly; rather, it is the most likely match. The biometric authentication model can use a variety of physical aspects, such as facial recognition, voice recognition, fingerprint scans, iris scans, and so forth.

Using the factors mentioned above, different customer-authentication models can be implemented. They can be classified into the following two broad types:

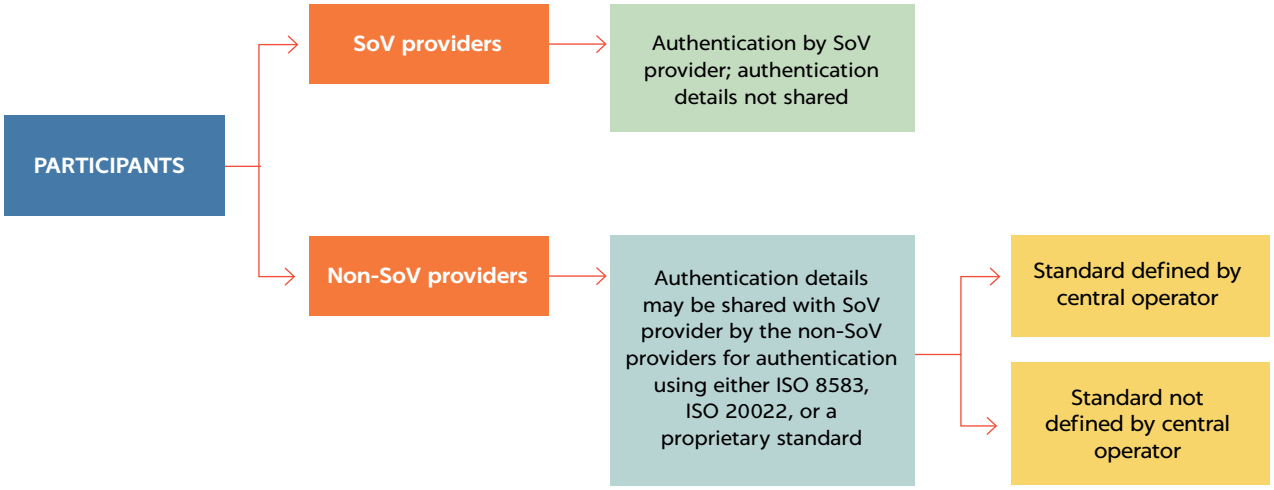
1. **Single-Factor Authentication Model:**
   In single-factor authentication, any one of the above factors is used to verify a customer. The most common form of single-factor authentication is using passwords or PINs.
2. **Multifactor Authentication Model:**
   Multifactor authentication models use more than one factor to identify a customer. Multifactor authentication increases the level of confidence in an authentication due to its multilayer security implementation, making it difficult to breach, compared to single-factor authentication.

Central operators and financial institutions across the globe have been shifting toward multifactor authentication (two-factor authentication) to validate the end customer before providing any financial/nonfinancial services. Use of these customer-authentication models is also influenced by the payment ecosystem of the country/region of implementation. Lately, only the financial institutions had access to their customer accounts and would enable payment services over the central payment scheme of the region. With changing guidelines and movement toward open economies, operators/regulators have enabled non-store of value (SoV) service providers—also referred to as third-party providers[10]—to have access of customers' accounts, to enhance customer experience. With respect to fast payments, customers have been provided access to services via either of the following providers, based on the scheme design and local regulations:

1. Store of value (SoV) providers:
SoV providers store customer funds in accounts (such as prepaid, savings, credit, and so on), from which financial or nonfinancial transactions are initiated. Here, account details are readily available with the financial institution, making it easy to authenticate the customer without sharing the authentication details over the network.

2. Non-store of value (non-SoV) providers:
Non-SoV providers do not hold the customer accounts and rely on customers of other institutions. Hence, one of the key actions required as part of a transaction is sharing the authentication details over a secure channel with an SoV provider for authentication. Only after receiving a successful response is the customer given access to the payment system.

FIGURE 5 Types of Participants and Authentication Methods



Customer-authentication details are required to be shared across the network in the scenario defined in figure 5. Different messaging standards define different set of fields for capturing customer authentication, thus enabling various authentication models. A detailed description of the available fields in each of the messaging standards is below:

3.2.1 ISO 8583

Different customer-authentication methods are implemented by different schemes relying on ISO 8583. Most of the implementations do not support non-SoV accounts; hence, there is no transfer of authentication details. In these cases, the SoV providers can choose to authenticate the customers by using any messaging standard for internal communication—for example, FPS in the United Kingdom and IMPS in India, where the authentication as a requirement is done at the remitter bank in line with scheme guidelines.

In the case of non-SoV providers, if ISO 8583 is the preferred standard for customer authentication, a predefined data element (DE 52) can be used to authenticate a customer along with the data elements reserved for national use (57–60, 112–119) and private use (61–63, 120–127), as described below:

- **DE 52: Personal identification number**
  Implementors can use this element to authenticate the customer, along with such other data elements as "Account Identification." This field is mandatory for card-based payment mechanisms and can be used to carry authentication details for a customer in the FPS. In use, this field is encrypted using symmetric keys exchanged between the payee's financial institution and the FPS and decrypted by the FPS and re-encrypted using different keys exchanged between the FPS and the payer's financial institution. Including a non-SoV provider in this flow will require suitable encryption for the flow between the non-SoV provider and FPS.
- **Fields reserved for national and private use:**
  National and private fields provided in ISO 8583 can be used to capture additional authentication details of the customer. These can capture any information related to customer-authentication factors, such as passwords, token-based information, and so forth.

3.2.2 ISO 20022

ISO 20022 is the most widely used standard in FPS across the globe. Different schemes that have implemented ISO 20022 rely on different customer-authentication methods. Similar to ISO 8583, most implementors have not necessarily relied on any standard but have left it to the participants to ensure that the customer is authenticated. In these cases, the SoV providers can choose to authenticate the customers by using any messaging standard for internal communication—for example, RTP in the United States, where the authentication as a requirement is done at the remitter bank.

In the case of non-SoV providers, if ISO 20022 is the preferred standard for customer authentication, ISO 20022 messages carry tags for customer authentication in various messages used in the transaction flow. In the Payment Initiation (pain.001) message, the Authorisation <Authstn> tag in the Group Header <GrpHdr> can carry details required for customer authentication. (For details on the <Authstn> tag, refer to appendix I.)

In case an implementation allows mandates (pain.009 and similar), fields are available to enter the authentication details. They are part of the Authentication <Authntcn> tag present in the Mandate <Mndt> tag of the message. (For details on the <Authntcn> tag, refer to appendix J.)

Apart from the above, ISO 20022 has defined different message sets for card transactions that can carry card and customer-authentication details.

CASE STUDY 1 NPP AUSTRALIA

In NPP in Australia, financial institutions have deployed a combination of multifactor authentication methods to protect customers from account compromise. Non-SoV providers are accessed through the channels of SoV providers. Hence, authentication is done at the SoV provider itself. While submitting a transaction from the channels, if an overlay service (a non-SoV provider) is selected as a method, pain.a09, a proprietary application programming interface, is used, which asks the NPP participant (a SoV provider in this case) to create a payment resource.

3.2.3 Proprietary

Proprietary messages cannot be generalized, as the authentication depends on the implementation and can have different authentication regulations across different implementations. UPI in India is one of the most successful FPS implementations globally using a proprietary standard. It has engaged varied payments service providers (SoV providers and third-party providers) in the ecosystem; hence, the authentication mechanism deployed is much sophisticated.

UPI has deployed two-factor authentication: first at the mobile application in the form of "mobile binding," and then in the form of a PIN/password, which is validated at the SoV provider. As designed, a customer may use the UPI mobile application provided by either a SoV or a non-SoV provider. If a non-SoV provider is chosen for the transaction, authentication details captured by the non-SoV application provider are securely shared with the SoV provider after the authentication information is processed using a trusted common library provided by NPCI.

Mobile Binding

Mobile device binding is the process by which the customer's mobile device is bound with the UPI application during registration. The device is then validated every time the customer accesses the application to conduct a transaction. Mobile binding is used as one of the authentication factors in UPI.

(For details on the mobile binding process, refer to appendix K.)

Trusted Common Library

A trusted common library is provided by NPCI for capturing customer-sensitive information. The PIN travels over the secure channel from UPI to the issuing bank using encryption based on public key infrastructure, where the PIN is encrypted using the public key at UPI, and it is decrypted by the issuing bank at its end using its private key.[11] This library is used to provide the same user experience over different SoV and non-SoV applications. In addition, it provides a unique platform for financial institutions, which don't have to rely on different third-party applications for encrypting user credentials.

- The trusted common library provided by NPCI is required to be integrated with PSP applications for capturing credentials, such as passwords, PINs, MPINs, biometrics, and so on.
- Authentication details are captured and base 64 encoded by the trusted common library and sent back to the PSP for subsequent transport throughout the payment cycle in UPI.

Key Takeaway

Customer authentication is subject to the requirements and regulations of a country/region, based on which implementation of FPS has been done. Each messaging standard provides certain predefined fields that can be used to authenticate the customer. Most implementations allow SoV providers to implement the authentication locally and define a set of guidelines for implementing authentication by non-SoV providers.

3.3 SYSTEM PERFORMANCE AND SCALABILITY

System performance is the amount of useful work that can be done using a system. The accomplished work is measured against preset known standards, such as efficiency, accuracy, and speed of executing a set of instructions (transactions in the case of a payment system). On the other hand, scalability is the system's ability to handle increased work while not compromising the performance of a system. A system is considered as scalable if it does not need to be redesigned to accommodate an increased workload. The more scalable the system, the better its prospects for the future. The performance and scalability of a system depends on the following system parameters:

1. **System Design**

   This parameter relates to the complexity of the design of the system. A complex system would adversely affect system performance and limit its scalability, as dependence on different components in the system would increase. The complexity of system design can be attributed to the number of components in the system, the hops a transaction will take, dependence on one component for multiple tasks, and interdependence between components. All of these factors are crucial while designing the system. A simple system design would mean better performance, compared to a complex system design.

2. **Hardware Capabilities**

   This parameter relates to the hardware components of the system and their capabilities affecting the system performance. The higher the configuration of hardware used in a system, the better the system performance would be, keeping other factors common. For example, the higher the processing power of the processor, the greater the number of transactions that can be processed in a predetermined time frame, leading to better performance.

3. Network Capabilities

In a payment system, transactions are sent from one system to another, which requires network connectivity between the different parties involved in the transaction. So the better the network capabilities of the system, the better the system performance would be and the greater the scalability would be. For example: The better the throughput and the less the latency, the better the system performance.

However, the performance and scalability of any payment scheme is determined by the design, hardware, and network capabilities of the system. These factors are further influenced by characteristics of the messaging standard, such as message size, STP, data truncation, and adoption of new use cases.

1. Message Size

The message size is directly related to the information-holding capacity, richness of the message format, and structure of the message. Message size plays an important role in measuring the system performance, as the larger the size, the longer the processing time and the greater the hardware requirements, while the processing speed would be less, and vice versa. ISO 8583 messages are approximately five times lighter than ISO 20022 messages. This is due to the limited amount of information being transferred, thus saving on the memory required for storage. In addition, less bandwidth is required to process these transactions, increasing the speed and efficiency of the system. In comparison, ISO 20022 messages are bulkier. Their bigger size is attributed to the presence of nested tags in the XML format, the structure of the message, the message-holding capacity, and the message format. Hence, the bandwidth required to process transactions is comparatively higher and may create a capacity problem at some locations, due to unavailability of good network infrastructure. The message size for a proprietary message varies based on implementation, the format, the character sets, and the type of information contained in a message. Generalizing about the message size of proprietary formats is difficult, but implementors have the advantage of being able to choose the message attributes to fit the requirements, as well as meet the data-handling capacity of the system. In addition, since the messaging standard is not standardized, implementors have the flexibility to remove unused fields/tags, which is not feasible in messaging standards such as ISO 20022.

2. Straight-Through Processing

STP means the automatic processing of payment transactions, with no manual intervention required. STP is key to system performance, as it reduces the processing time and the resources required for manual intervention from operators while increasing the speed, efficiency, and accuracy of the system. ISO 8583 messages are unstructured and rely heavily on free format. For example, in address fields, there is no demarcation of address parameters such as city or state, which makes it vulnerable to misinterpretation. This type of data is difficult for the processing system to process, leading to increased manual intervention and, hence, decreasing the STP rate. In contrast, ISO 20022 messages are structured and have supporting unstructured fields to pass additional information. The data entered in these fields can be differentiated easily, which helps in processing the payments. For example, address fields have city, state, country, subdivision, and other subfields, making it easy for the system to interpret and process the data automatically and leading to decreased manual intervention and, hence, increasing the STP rate. The structure of a proprietary messaging standard varies based on implementation and cannot be generalized. Implementors of proprietary systems have the freedom to choose between structured or unstructured fields and, in the case of free text fields, to define separators at the field level to make the data more understandable. The STP rates achieved are usually higher using a proprietary message format.

3. Data Truncation

This parameter is used to compare the messaging standards based on the data-carrying capacity of a messaging standard. The greater the data-carrying capacity, the greater the information that can be carried from the message sender to the receiver. The less the data-carrying capacity, the greater the data truncation would be, to fit in the data, leading to loss of data. If the data entered is larger than the space available, how the data is truncated—such as by truncating the first or last characters that do not fit in the defined space—will depend on the implementing system. ISO 8583 has shorter field lengths than ISO 20022 in such essential fields as name, address, and identifiers. These data fields are required for the accuracy of the payment transaction. For example, in the case of ISO 8583, the 140-character limit applied to the address fields may not be sufficient to capture all the information contained in international correspondence addresses. ISO 20022 messages have more field lengths

in essential fields than ISO 8583 messages. ISO 20022 provides both structured and unstructured fields for capturing the data. Unstructured fields can be used over and above the structured fields to provide extensibility to the transaction-related data. For example, the address field <PstlAdr> in ISO 20022 has unstructured fields in addition to the structured fields. As per the latest specification for payment clearing and settlement messages, there can be seven instances of the 70-character unstructured address line for each party involved in the transaction. These additional unstructured address lines, along with the structured data, provide sufficient field length to capture most of the data, increasing the accuracy of transaction. On the other hand, proprietary messages have the advantage of allowing the message structure and field lengths to be tweaked as and when required based on the requirements. The field lengths can be defined keeping in mind the regional requirements, and implementors can cut off excessive fields/field lengths that are predefined in standardized message formats, increasing the efficiency of the transaction messages.

4. Addition of New Use Cases

This parameter is used to compare the messaging standards based on the use cases that can be implemented and the openness of the messaging standard to incorporating new use cases. Use cases may range from features enhancing customer experience, increasing target market, or enabling cross-border transactions. This capability to undertake new use case with ease plays a major role in defining the scalability of a messaging standard. ISO 8583 has limited business use cases for FPS due to its inclination toward the interchange of card-originated transactions. In the current scenario, certain use cases cannot be implemented using the messaging standard out of the box, such as request-to-pay messages and remittance information messages. In addition, no recent updates for ISO 8583 limit the addition of new use cases by changes in the message structure, while ISO 20022 is an open standard that can adapt to changing needs and new approaches within the payments industry. Since ISO 20022 is not controlled by a single interest, it is open to changes and can be used by anyone in the financial industry. It has been designed with the dynamic nature of business requirements in mind, allowing for better compatibility with business use cases. The majority of the current use cases for FPS can be implemented using ISO 20022, and the messaging standard has a dedicated change-request portal for the participants to submit their requirements for the rest. If approved, the changes become part of the yearly or emergency upgrade cycle. Proprietary messaging standards are best suited for incorporating niche or local use cases based on demographic, geographic, infrastructural, or regulatory requirements. Whenever a new requirement is encountered, proprietary messaging standards can accommodate such requests better than other standards, as no third party is needed to make or approve such changes in the messaging standard.

4 PAYMENT SYSTEM OPERATORS' EXPERIENCE WITH PROPRIETARY SYSTEMS

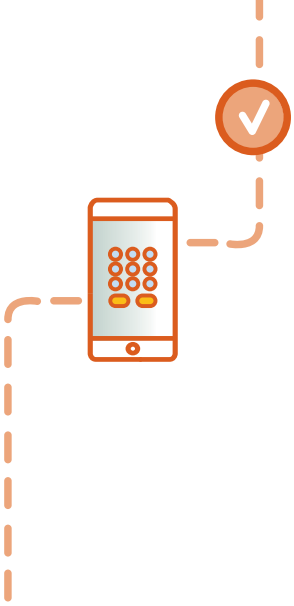
Proprietary systems require detailed research and analysis of the requirements, the process, available technologies, infrastructure, stakeholders, expected outcomes, and key influencing factors, such as cost, before a decision is taken. All these requirements need to be carefully considered while designing the system to match the expected outcome, making the research and design phase the most crucial phase of the implementation using a proprietary messaging format. Although there are many challenges when implementing a proprietary system, implementors in certain cases feel that these challenges are outweighed by the perceived benefits. The experiences of the central operators in deciding, implementing, and operating FPS based on a proprietary messaging standard for UPI in India and SPEI in Mexico are recounted in case study 2 and case study 3, respectively.

CASE STUDY 2 UPI IN INDIA

UPI in India was launched on April 11, 2016, based on a proprietary messaging standard. Before choosing a proprietary messaging standard, various feasibility analyses were done to understand how existing standards, such as ISO 20022, fit a set of preliminary requirements. The major reasons for the choice was the belief that, in the case of the standard messages, the UPI implementors would be dependent on different versions released by the ISO, while for a proprietary standard, that decision would lie with them. In addition, ISO 20022 and other messaging standards were perceived to be complicated, while a less complicated messaging standard was required. Because UPI in India is an in-house standard, it was expected to deliver efficiency, ease of understanding, and accommodation of new requirements as major benefits over the standardized messages. The process of accommodating new requirements can be compared to the change request process of ISO 20022, which is a lengthy and, generally, an annual affair. This is not the case with proprietary formats. The other two perceived benefits are subjective and vary between different users. UPI in India has integrated with different domestic products, such as NETC for toll collection. The major challenges faced while integrating UPI with other systems were technical—for example, bandwidth needed to be upgraded at both NPCI's and the banks' end. In addition, the banks had to introduce an integration layer for transmitting the UPI messages (in proprietary format) to the core banking system. Implementation of UPI also required rigorous technical training of the parties involved, along with customer education. NPCI was of the view that all the implementations across the world would not be on a single messaging standard or even on a single version of a messaging standard. So if there were cross-border payment integrations where the two parties were on different versions, then they would require a central translator or convertor to make the messages understandable to both parties. Due to this hinderance, they preferred proprietary messages, as the translators would be required in both cases, whereas, with proprietary messages, they could reap the benefits of flexibility and better efficiency. Today UPI in India is integrated with Singapore; merchants registered with NETS (Singapore) can accept UPI payments from users in India registered on the UPI platform. UPI has also recently integrated with Bhutan and the United Arab Emirates, and conversations with different countries about integrating their FPS are ongoing.

CASE STUDY 3 SPEI IN MEXICO

SPEI in Mexico was introduced in 2004, long before ISO 20022 was introduced. The only prevalent standard was ISO 8583 for card-based payments, which had different implementations in two similar systems, Mastercard and Visa. The central system felt a need to bring out a system in which data is represented efficiently and elegantly while focusing on achieving higher efficiency rates. The implementors perceived speed, size of the message, and efficiency as the benefits of choosing a proprietary messaging standard over the others. In 2015, they analyzed ISO 20022 and found that an ISO 20022 message was seven times heavier in byte size than a similar proprietary message used by SPEI in Mexico. SPEI in Mexico has not integrated with other payment systems in the domestic market but has given credit cards as an option to be used as a proxy ID. The decision to include a credit card is left to the issuer banks, and they can decide to include the same. Currently SPEI is not integrated with another FPS, but it plans to integrate soon with other systems across the world. The implementors at SPEI in Mexico are of the view that all the implementations across the world would not be on a single messaging standard or even on a single version of a messaging standard. So if there were cross-border payment integrations where the two parties were on different versions, then they would require a central translator or convertor to make the messages understandable to both parties. SPEI in Mexico is planning to undertake a change where they would embed an ISO 20022 translator in the system that would increase interoperability.



5 CONCLUSION

5.1 DECISION FRAMEWORK

Any FPS implementation needs to be planned as a community effort. Decisions about the style, speed, and scope of the implementation of the messaging standard must be made after considering the widest set of stakeholders: direct participants, indirect participants, regulators, vendors, service providers, and consultants. Even where the overall business case is strong, it is important to understand that all participants may not feel the benefits and costs of the implementation equally.

The choice of an appropriate messaging standard is pivotal for the scheme to enable PSPs and others to develop services and innovations that are adaptable to the needs of end users. From an FPS perspective, a decision on messaging standards depends on one or more of the points below, which have ramifications from strategic, technical, operations, collaboration, and scheme-expansion perspectives.

1. Type of FPS Implementation

The various implementation approaches taken by FPS across the globe have been customized to the local context and benchmarked to some of the world's most popular live FPS schemes. The choice of an appropriate implementation approach is governed by the following factors:

- Interaction with other payment systems
- Regulatory push and urgency
- Evolving dynamics in the local payments industry and customer demographics
- Financial considerations
- Level of reliance on third-party organizations

Three broad implementation types are seen globally in the implementation of FPS. The type of FPS implementation can affect the decision of a messaging standard heavily, as it has a material impact on program structure and guidelines. For example, the FPS implementation NPP in Australia saw a large impact on program structure based on the new implementation of ISO 20022 from scratch. Also, beyond FPS, several high-value payment schemes in the European Union for Target 2 and CHAPS in the United Kingdom have ongoing multiyear programs to implement a common messaging framework.

- **Building FPS from scratch:** This implementation generally entails a long-term program in which a new system is built—that is, all the components to be implemented are built and deployed, and there is no reuse from other payment products. This type of implementation has been used by India and Australia and is best suited when the existing systems/infrastructure, if reused, would be incapable of providing the desired outcomes.
- **Migrating from one messaging standard to another:** In this implementation, a scheme migrates from one payment messaging standard to another to realize benefits that were impossible in the existing system—for example, the development of a common ISO 20022 messaging standard for the New Payment Architecture in the United Kingdom encompassing FPS, retail payment frameworks, and high-value payments with a key objective of increasing interoperability across the schemes, wherein all three schemes have a common settlement interface owned and operated by the central

bank, which provides a common ground for the implementation of settlement messages.

- **Leveraging existing systems:** In this type of implementation, a system is built over another system or as an extension of the existing system. This implementation is beneficial as it saves cost, gives a faster return on investment, and has lower risk with less operational disruption, but leveraging existing systems may limit the scope of the new system. A classic example of leveraging existing systems is TIPS, which is built as an extension of Target 2.

The following are two major approaches for implementing any of the above-mentioned categories:

1. *Big Bang:* This approach entails a single program in which there is one major rollout of the desired payment system—that is, all the desired functionalities are delivered in one go. This approach costs less than a phased rollout, as the operating expenses are lower, but higher risk is attributed to a single-step implementation.
2. *Phased rollout:* Under this approach, the program is divided into phases, and each phase is an incremental improvement over the previous phase. For example, in a phased rollout, a scheme may implement the FPS in a way that allows them only to accept the payments (receive), while participants would need to use other existing payment methods to send payment.

When leveraging existing systems or migrating from one standard to another, extra caution is needed so as not to disturb the existing system. The following major points should be considered before envisaging such implementations:

- Identify affected systems, rules, channels, processes, and touchpoints.
- Determine the level of impact on the touchpoints, systems, and channels, and explore their readiness to accept the change.
- Plan the incremental change and prioritize based on the impact of the change on the overall system, timeline of change, and operational considerations.
- Emphasize minimizing the impact on customers.
- Map system parameters such as efficiency, speed, turnaround time, and other expected outcomes to the actual outcomes.

2. Experience and Participant Readiness

Before any FPS implementations, the scheme undertakes elaborate consultative sessions to look at the best practices both globally and locally that can be adopted or from which inference can be drawn. One of the key aspects of these consultative sessions is the selection of an appropriate messaging standard.

It has been observed with various global FPS implementations that local experience with the chosen messaging standard is a deciding factor in choosing a specific messaging standard. Having prior experience with messaging standards has the following benefits:

- Predictability in implementation milestones
- Lessons learned from similar implementations to further streamline scheme delivery
- More accurate cost projections
- Ready-made libraries of technical message definitions for baselining

In addition to experience with similar implementations in other schemes, the readiness of the participants is one of the key components that influences the scheme's decision on an appropriate messaging framework. Participants in the FPS schemes, especially the traditional financial institutions, have varied experience across multiple geographies, including experience and components within the participant's payment service architecture, that can handle various messaging standards. If scheme participants have a high degree of readiness, participants can start deriving the full level of business benefits from the mandated messaging standard and move beyond just compliance.

Also, the amount of time taken by the industry to streamline communication based on messaging standards and build upon the mandated messaging standards will help develop innovative use cases that will help translate into newer payment services built on top of the FPS infrastructure—for example, embedding QR codes within payloads to help corporate customers to derive and automatically capture payment-specific details such as invoice details, amount details, tax information, and use them in corporate-specific systems such as enterprise resource planning, terminal management systems.

However, the experience of participants with a specific messaging standard in one domain/geography doesn't guarantee a replication in the FPS architecture, but the experience certainly makes the process more streamlined, and the scheme can also draw inferences during the collaboration.

3. Time to Market

The development of FPS frameworks are timed-bound implementations that are undertaken and planned to be delivered within a specific time for a variety of reasons.

Given the various technical and functional components of an FPS, messaging standards are the key drivers in determining if the scheme can be delivered within the specified time frame and if it is able to accelerate successful delivery due to reasons such as technical integrations, collaboration, embedding business processes into messaging standards.

One of the reasons for a need to accelerate the time to market, as seen in global FPS implementations, is the emergence of a fragmented marketplace in which multiple closed loops and privately owned FPS are established in the country with no basis for underlying interoperability, and each payment scheme offers only a limited use case.

4. Cost

Any implementation of a messaging standard is a complex program that needs to be treated like another long-term strategic program and requires certain principles to be adhered to, so that delivery can be completed successfully. One of the most important principles is the aspect that the cost and budget allocated to the overall program will span the transformation of technology components, resource budgets.

The scheme needs to plan accordingly and consider the practical aspects of the implementation of a messaging standard for delivering the messaging standard correctly, on time, and at an acceptable cost to all stakeholders. The following factors will affect the cost of implementation:

- The availability of the resource skill set needed to implement the messaging standard in the region would affect cost. Also, the greater the complexity of the messaging standard chosen, the higher the cost, due to the specialized resources required.
- The strategy chosen by the scheme would also affect cost. For example, choosing a tactical solution in the form of central translators would require a one-time set-up cost, but avoiding a complete overhaul of technical components would bring savings.
- Generally, the longer the implementation timeline, the higher the costs, due to higher resource costs, large-scale transformations.

One of the costliest propositions for implementing a messaging standard is the ramification on the following existing technical components used by the scheme and the participants:

- Legacy integration interfaces
- Data warehouses
- Physical data centers
- Payment-processing hubs
- Liquidity management
- Contingent data-recovery centers
- Any new technology implementation, such as hosting payment solutions in the cloud
- Security infrastructure

For example, the ISO 20022 implementation for cross-border payments has necessitated the overhaul of the legacy framework of both the scheme and participants in areas of payment hubs, data warehousing, gateway routing. Given the context, the types of participants in the FPS and their financial capability to deliver these costly implementations are important points to be considered by the scheme when deciding on a messaging framework.

5.2 KEY TAKEAWAYS

1. ISO 8583

ISO 8583 was originally published by ISO in 1987 and since has been predominantly used in card-originated transactions. Some of the early FPS implementations are using ISO 8583 messaging formats and are still operational. ISO 8583 relies on an unstructured free-text format and is smaller in size than other standards, which makes it the standard of choice where limited bandwidth, storage, or processing capabilities are the factors under consideration. ISO 8583 has a predefined data element for PIN and reserved-data elements that can be used to carry details of various factors used for customer authentication. In addition, ISO 8583 defines various message types that can be used to implement different use cases, although certain use cases, such as request to pay, cannot be implemented with the available message types.

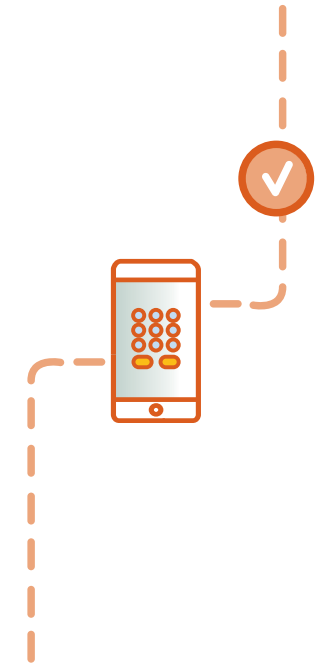
2. ISO 20022

ISO 20022 was first introduced by ISO in 2004 and is considered as the global standard for the exchange of electronic messages between financial institutions, both for payment as well as nonpayment transactions. The widespread adoption of ISO 20022 is attributed to the standardization of the message, interoperability, the availability of a large number of fields for carrying transaction information, and better STP rates. ISO 20022 is very detailed and has different message types that can be used to implement various use cases. This also means that the message is bigger in size than other standards and schema maintenance is difficult, as it takes a holistic picture of all the participants, rather than a single interest. To implement customer authentication, predefined

fields can be used to carry the authentication details. In addition, ISO 20022 has defined a real-time payments group to document a consistent and harmonized view of ISO 20022 message components, business processes, elements, and data content with respect to FPS in different market implementations.

3. Proprietary

Proprietary payment messages are a unique message format defined by a country/region/monetary authority for facilitating payments. This messaging format is generally localized and best suited for serving niche requirements. Proprietary messages offer high levels of customization, and schema maintenance activities, whenever necessary, can be done based on a single interest, which is not possible in the other two formats. This also means that proprietary messages are less standardized and less interoperable than other standards. Most of the customer-authentication implementations for fast payments have been done using a proprietary format, as it provides the flexibility to design the standard to embed solutions supporting different factors at various levels of authentication. In addition, the standard can be designed in a way to match the local infrastructure capabilities to achieve the required level of system performance.



6 ACKNOWLEDGMENTS

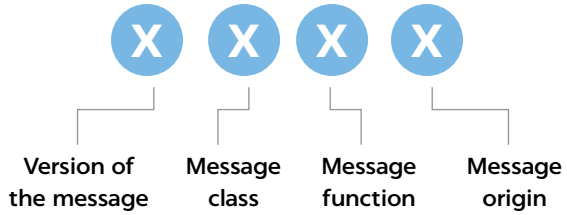
Organization	Contributor
PwC India	PwC India
World Bank	Harish Natarajan
	Nilima Ramteke
	Holti Banka

7 APPENDICES

APPENDIX A: STRUCTURE OF ISO 8583 MESSAGE

Each ISO 8583 message is identified by a message type indicator (MTI). The significance and usage of each digit is as shown in figure A1.

FIGURE A1 Significance of Digits in MTI



The first digit denoting the version of the message can be understood as shown in table A1.

TABLE A1 ISO 8583 MTI: Meaning of First Digit

MESSAGE TYPE INDICATOR	MEANING
0XXX	ISO 8583:1987
1XXX	ISO 8583:1993
2XXX	ISO 8583:2003
3XXX 4XXX 5XXX 6XXX 7XXX	ISO reserved
8XXX	Reserved for national use
9XXX	Reserved for private use

Source: Payment Systems Blog[12]

As shown in table A2, the second digit shows the message class.

TABLE A2 ISO 8583 MTI: Meaning of Second Digit

MESSAGE TYPE INDICATOR	MEANING
X0XX	Reserved by ISO
X1XX	Authorization message
X2XX	Financial message
X3XX	File actions message
X4XX	Reversal and chargeback messages
X5XX	Reconciliation message
X6XX	Administrative message
X7XX	Fee collection message
X8XX	Network management message
X9XX	Reserved by ISO

Source: Payment Systems Blog[13]

As shown in table A3, the third digit shows the message function.

TABLE A3 ISO 8583 MTI: Meaning of Third Digit

MESSAGE TYPE INDICATOR	MEANING
XX0X	Reserved by ISO
XX1X	Authorization message
XX2X	Financial message
XX3X	File actions message
XX4X	Reversal and chargeback messages
XX5X	Reconciliation message
XX6X	Administrative message
XX7X	Fee collection message
XX8X	Network management message
XX9X	Reserved by ISO

As shown in table A4, the last digit is for the message origin.

TABLE A4 ISO 8583 MTI: Meaning of Fourth Digit

MESSAGE TYPE INDICATOR	MEANING
XXX0	Acquirer
XXX1	Acquirer repeat
XXX2	Issuer
XXX3	Issuer repeat
XXX4	Other
XXX5	Other repeat
XXX6 XXX7 XXX8 XXX9	Reserved by ISO

Source: Payment Systems Blog[14]

APPENDIX B: COMPARATIVE ANALYSIS: PARAMETER FIELD LENGTH

TABLE B1 Comparison of Field Length of Sample Fields

FIELD	ISO 8583	ISO 20022	PROPRIETARY (UPI)
Name fields (debtor/creditor/ultimate debtor/ultimate creditor)	40	140	99
Address	140	Department <Dept>—70 SubDepartment <SubDept>—70 StreetName <StrtNm>—70 BuildingNumber <BldgNb>—16 BuildingName <BldgNm>—35 Floor <Flr>—70 PostBox <PstBx>—16 Room <Room>—70 PostCode <PstCd>—16 TownName <TwnNm>—35 TownLocationName <TwnLctnNm>—35 DistrictName <DstrctNm>—35 CountrySubDivision <CtrySubDvsn>—35 Country <Ctry>—2 AddressLine <AdrLine>—70	255
Amount	14	18 with 5 fraction digits	14
Account number	34	34	255 (total length of IFSC, ACTYPE, ACNUM)
Institution identifiers	11	Multiple with maximum length of 35	20
Transaction identifiers	18	Multiple with maximum length of 35	35

APPENDIX C: COMPARATIVE ANALYSIS: PARAMETER REMITTANCE INFORMATION

ISO 8583

There is no predefined field for remittance information in ISO 8583 messages, but this information can be provided in fields reserved for national or private use (57–63 and 112–127), which have a field length of 999 characters. For example, banks in the United Kingdom specify two fields: Field 120: payment reference information (in most cases, this is a client reference or account number that allows the beneficiary to identify the sender or purpose of payment), and Field 121: remittance information.

ISO 20022

Remittance information can be provided in the following two places in an ISO message:

1. **Related Remittance Information [tag <RltdRmtInf>]**
   Provides remittance-related handling information for use in transaction processing by any agent in the chain. Related Remittance Information is further divided into the following two subtags/elements:

   a. Remittance Identification [tag <RmtId>]
      This unique identification is assigned by the initiating party to identify unambiguously remittance information that is sent separately from the payment instruction. It is 35 characters in length.

   b. Remittance Location Details [tag <RmtLctnDtls>]
      Remittance location details is further divided into the following:

      i. Method [tag <Mtd>]: This tag is list of predefined code sets.

      ii. Electronic Address [tag <ElctrncAdr>]: The electronic address to which an agent is to send the remittance information. This field has a length of 2,048 characters.

      iii. Postal Address [tag <PstlAdr>]: This field is the postal address to which an agent is to send the remittance information. It is further divided into the following two parts:

      - Name [tag <Nm>]: This field is 140 characters long.
      - Address [tag <Adr>]: This field has further address subtags/elements.

2. **Remittance information [tag <RmtInf>]**
   This is the information supplied to match an entry with the items that the transaction intends to settle—for example, commercial invoices for an accounts receivable system.
   The remittance information field is further divided into the following two parts:

   a. Structured
      Information supplied to match an entry with the items that the transaction intends to settle in a structured form. This field is further divided into the following parts:

      i. ReferredDocumentInformation [tag <RfrdDocInf>]: This field is further divided into multiple tags/elements for providing identification and content of the referred document.

      ii. ReferredDocumentAmount [tag <RfrdDocAmt>]: This field is further divided into multiple tags/elements for providing details on amounts of the referred document.

      iii. CreditorReferenceInformation [tag <CdtrRefInf>]: This field is further divided into multiple tags/elements to be used to provide reference information provided by the creditor to allow the identification of the underlying documents.

      iv. Invoicer [tag <Invcr>]: This field is further divided into multiple tags/elements to be used to identify the organization issuing the invoice in cases where it is different from the creditor or ultimate creditor.

      v. Invoicee [tag <Invcee>]: This field is further divided into multiple tags/elements to be used to identify the party to whom an invoice is issued when it is different from the debtor or ultimate debtor

      vi. TaxRemittance [tag <TaxRmt>]: This field is further divided into multiple tags/elements to be used to provide remittance information about a payment made for tax-related purposes.

      vii. GarnishmentRemittance [tag <GrnshmtRmt>]: This field is further divided into multiple tags/elements to be used to provide remittance information about a payment made for garnishment-related purposes.

viii. AdditionalRemittanceInformation [tag <AddtlRmtInf>]: This field is 140 characters long in free-text form for additional information, to complement the structured remittance information.

b. Unstructured
Information supplied to match an entry with the items that the transaction intends to settle in an unstructured form—that is, free text. This field has a length of 140 characters.

Proprietary message

In UPI, the remittance information is added in the "note" tag and "refId" tag.

1. "note" tag is 50 characters long. It is the description of the transaction and in free text format (which is printed on the passbook).
2. "refId" tag is an external reference number to identify the payment, such as a loan number, invoice number, and so forth. It is 35 alphanumeric characters long.

APPENDIX D: COMPARISON OF UTF-8 AND ASCII

PARAMETER	UTF-8	ASCII
Definition	UTF-8 is a universal character set. It is the IT standard that encodes, represents, and handles text for computers, telecommunication devices, and other equipment.	ASCII stands for American Standard Code for Information Interchange. It is the IT standard that encodes the characters for electronic communication only.
Function	UTF-8 represents a large number of characters, such as mathematical symbols, letters of different languages, historical scripts, and so on.	ASCII represents a specific number of characters, such as uppercase and lowercase letters of the English language, digits, and symbols.
Space utilization	UTF-8 supports many characters and occupies more space. It uses eight bits to present any character, and ASCII is a subordinate of Unicode.	ASCII supports only 128 characters and occupies less space by converting the characters to numbers and using seven bits to present any character.

APPENDIX E: SCOPE OF RTPG

The Real Time Payments Group (RTPG)[15] was formed to document a consistent and harmonized view of ISO 20022 message components, business processes, elements, and data content with respect to FPS in different market implementations. Table E1 presents the scope of messages.

TABLE E1 **Scope of RTPG of ISO 20022**

SERVICE	MESSAGES	MEANING
Interbank services	Recommended messages (pacs.008, pacs.002)	RTPG-recommended ISO 2022 messages between two banks for credit transfer and payment-status reporting
	Optional and implementation driven (pacs.004, pain.013/pain.014, camt.052/053/054, camt.056/029, remt.001/002)	Optional messages that can be used by the implementors or for which the alternatives are present. For example, pacs.004 is used for returns, while TCHRTP in the United States uses pacs.008 for returns with details of original transaction.
Payer	Optional and implementation driven (pain.001, pain.002, pain.013/pain.014, camt.052/053/054, camt.056/029, remt.001/002)	Optional messages between the payer and the channel/overlay services
Payee	Optional and implementation driven (pain.013/pain.014, camt.052/053/054, remt.001/002)	Optional messages between the channel/overlay and the payee
Settlement	Optional and implementation driven (pacs.009, pacs.010, pacs.002)	Optional messages between financial institutions for settlement

APPENDIX F: ISO 8583 MESSAGE LINKAGE

i. ISO 8583 Messages and Field Descriptions

TABLE F1 ISO 8583 Messages Used in Linkage between Transaction Flow, Processing Steps with Messaging Standards

MESSAGE	MESSAGE CATEGORY	FIELDS AVAILABLE		PRIVATE FIELDS REQUIREMENT
X200	Acquirer financial request	DE 2 DE 3 DE 18 DE 32 DE 41 DE 42 DE 43 DE 102	Primary account number Processing code Merchant category code Acquiring institution identification code Card acceptor terminal identification Card acceptor terminal code Card acceptor name/location Account identification 1	Fields missing for carrying debtor's and creditor's information, remittance information, and on-behalf-of transaction fields
X210	Acquirer financial response	DE 2 DE 3 DE 18 DE 32 DE 39 DE 41 DE 42 DE 43 DE 102	Primary account number Processing code Merchant category code Acquiring institution identification code Response code Card acceptor terminal identification Card acceptor terminal code Card acceptor name/location Account identification 1	Fields missing for carrying debtor's and creditor's information, remittance information, and settlement information

ii. Proxy Verification Flow

TABLE F2 ISO 8583 Messages and Important Fields for Proxy Verification Flow

STEPS	MESSAGE	IMPORTANT FIELDS/DATA ELEMENTS (DE)
1	FI specific	Debtor, creditor, proxy ID
2–3	X200	DE2, DE 3, DE 18, DE 32, DE 41, DE 42, DE 43, DE 102, and fields for carrying proxy ID details
4–5	X210	DE 39, echo fields from request message, response details to proxy verification
6	FI specific	Counterparty details, identifiers

iii. Successful/Rejected Transaction Flow

TABLE F3 ISO 8583 Messages and Important Fields for Successful/Rejected Transaction Flow

STEPS	MESSAGE	IMPORTANT FIELDS/DATA ELEMENTS (DE)
1	FI specific	Debtor, creditor, transaction details
2–3	X200	DE2, DE 3, DE 18, DE 32, DE 41, DE 42, DE 43, DE 102, and private fields for carrying debtor's information
4–5	X210	DE 39 and echo fields from request message
6	FI specific	Transaction information, counterparty details

APPENDIX G: ISO 20022 MESSAGE LINKAGE

i. ISO 20022 Messages and Field Descriptions

TABLE G1 **ISO 8583 Messages Used in Linkage between Transaction Flow, Processing Steps with Messaging Standards**

MESSAGE	MESSAGE CATEGORY	FIELDS AVAILABLE
acmt.023	Account management	<Assgnmt> - Assignment <MsgId> - Message Identification <CreDtTm> - Creation Date Time <Assgnr> - Assigner <Assgne> - Assignee <Vrfctn> - Verification <Id> - Identification <PtyAndAcctId> - Party and Account Identification <Acct> - Account <Othr> - Other <Id> - Identification
acmt.024	Account management	<Assgnmt> - Assignment <MsgId> - Message Identification <CreDtTm> - Creation Date Time <Assgnr> - Assigner <Assgne> - Assignee <Rpt> - Report <OrgnlId> - Original Identification <Vrfctn> - Verification <OrgnlPtyAndAcctId> - Original Party and Account Identification <Pty> - Party
pain.013	Payment initiation	<MsgId> - Message Identification <CreDtTm> - Creation Date Time <InitgPty> - Initiating Party <PmtInf> - Payment Information <PmtMtd> - Payment Method <ReqdExctnDt> - Requested Execution Date <Dbtr> - Debtor <DbtrAcct> - Debtor Account <DbtrAgt> - Debtor Agent <CdtTrfTx> - Credit Transfer Transaction <PmtId> - Payment Identification <Amt> - Amount <ChrgBr> - Charge Bearer <CdtrAgt> - Creditor Agent <Cdtr> - Creditor <CdtrAcct> - Creditor Account <RmtInf> - Remittance Information
pain.014	Payment initiation	<MsgId> - Message Identification <CreDtTm> - Creation Date Time <InitgPty> - Initiating Party <OrgnlGrpInfAndSts> - Original Group Information and Status <OrgnlMsgId> - Original Message Identification <OrgnlMsgNmId> - Original Message Name Identification <OrgnlPmtInfId> - Original Payment Information Identification <GrpSts> - Group Status <TxInfAndSts> - Transaction Information and Status
pacs.002	Payment clearing and settlement	<OrgnlMsgId> - Original Message Identification <OrgnlMsgNmId> - Original Message Name Identification <OrgnlCreDtTm> - Original Creation Date Time <GrpSts> - Group Status <TxInfAndSts> - Transaction Information and Status <TxSts> - Transaction Status <OrgnlTxRef> - Original Transaction Reference <ClrSysRef> - Clearing System Reference

MESSAGE	MESSAGE CATEGORY	FIELDS AVAILABLE
pacs.004	Payment clearing and settlement	<MsgId> - Message Identification <CreDtTm> - Creation Date Time <InitgPty> - Initiating Party <SttlmInf> - Settlement Information <TxInf> - Transaction Information <OrgnlInstrId> - Original Instruction Identification <OrgnlClrSysRef> - Original Clearing System Reference <OrgnlIntrBkSttlmAmt> - Original Interfinancial institution Settlement Amount <RtrdIntrBkSttlmAmt> - Returned Interfinancial institution Settlement Amount <Dbtr> - Debtor <DbtrAcct> - Debtor Account <DbtrAgt> - Debtor Agent <Cdtr> - Creditor <CdtrAgt> - Creditor Agent <CdtrAcct> - Creditor Account
pacs.008	Payment clearing and settlement	<MsgId> - Message Identification <CreDtTm> - Creation Date Time <InitgPty> - Initiating Party <CdtTrfTxInf> - Credit Transfer Transaction Information <Dbtr> - Debtor <DbtrAcct> - Debtor Account <DbtrAgt> - Debtor Agent <PmtId> - Payment Identification <Amt> - Amount <Cdtr> - Creditor <CdtrAgt> - Creditor Agent <CdtrAcct> - Creditor Account <RmtInf> - Remittance Information <IntrBkSttlmAmt> - Interfinancial institution Settlement Amount <ChrgBr> - Charge Bearer
remt.001	Remittance information	<MsgId> - Message Identification <CreDtTm> - Creation Date Time <InitgPty> - Initiating Party <RmtInf> - Remittance Information <Ustrd> - Unstructured <Strd> - Structured <OrgnlPmtInf> - Original Payment Information

ii. Proxy Verification Flow

TABLE G2 **ISO 20022 Messages and Important Fields for Proxy Verification Flow**

STEPS	MESSAGE	IMPORTANT FIELDS
1	FI specific	Debtor, proxy ID
2–3	acmt.023	<Assgnmt>, <MsgId>, <CreDtTm>, <Assgnr>, <Assgne>, <Vrfctn>, <Id>, <PtyAndAcctId>, <Acct>, <Othr>, <Id>
4–5	acmt.024	<Assgnmt>, <MsgId>, <CreDtTm>, <Assgnr>, <Assgne>, <Rpt>, <OrgnlId>, <Vrfctn>, <OrgnlPtyAndAcctId>, <Pty>
6	FI specific	Identifiers, counterparty details

iii. Successful/Rejected Transaction Flow

TABLE G3 **ISO 20022 Messages and Important Fields for Successful/Rejected Transaction Flow**

STEPS	MESSAGE	IMPORTANT FIELDS
1	FI specific	Identifiers, debtor, creditor, transaction details
2–3	pacs.008	<MsgId>, <CreDtTm>, <InitgPty>, <CdtTrfTxInf>, <Dbtr>, <DbtrAcct>, <DbtrAgt>, <PmtId>, <Amt>, <Cdtr>, <CdtrAgt>, <CdtrAcct>, <RmtInf>, <IntrBkSttlmAmt>, <ChrgBr>
4	pacs.002	<OrgnlMsgId>, <OrgnlMsgNmId>, <OrgnlCreDtTm>, <GrpSts>, <TxInfAndSts>, <TxSts>, <OrgnlTxRef>
5	pacs.002	Fields of step 4 and <ClrSysRef>
6	FI specific	Creditor, Transaction details, Charges, Value Date, Identifiers

iv. Request-to-Pay Flow

TABLE G4 **ISO 20022 Messages and Important Fields for Request-to-Pay Flow**

STEPS	MESSAGE	IMPORTANT FIELDS
1	FI specific	Identifiers, debtor, creditor, requested transaction details including amount, reason
2–3	pain.013	<MsgId>, <CreDtTm>, <InitgPty>, <PmtInf>, <PmtMtd>, <ReqdExctnDt>, <Dbtr>, <DbtrAcct>, <DbtrAgt>, <CdtTrfTx>, <PmtId>, <Amt>, <ChrgBr>, <CdtrAgt>, <Cdtr>, <CdtrAcct>, <RmtInf>
4	FI specific	Requested transaction details, requestor details, amount details
5	FI specific	Response details
6–7	pain.014	<MsgId>, <CreDtTm>, <InitgPty>, <OrgnlGrpInfAndSts>, <OrgnlMsgId>, <OrgnlMsgNmId>, <OrgnlPmtInfId>, <GrpSts>, <TxInfAndSts>
8	FI specific	Response details

APPENDIX H: PROPRIETARY MESSAGE LINKAGE

i. Proxy Verification Flow

TABLE H1 **Proprietary Messages and Important Fields for Proxy Verification Flow**

STEPS	MESSAGE TYPE	IMPORTANT FIELDS
1	FI specific	Debtor, proxy ID
2–3	Implementation specific	Debtor, proxy ID, identifiers
4–5	Implementation specific	Identifiers, creditor, original transaction, proxy response
6	FI specific	Identifiers, counterparty details

ii. Successful/Rejected Transaction Flow

TABLE H2 **Proprietary Messages and Important Fields for Successful/Rejected Transaction Flow**

STEPS	MESSAGE TYPE	IMPORTANT FIELDS
1	FI specific	Identifiers, debtor, creditor, transaction details, on-behalf-of fields (optional)
2–3	Implementation specific	Identifiers, debtor, creditor, transaction details, on-behalf-of fields (optional), clearing specific fields
4–5	Implementation specific	Response code, response details, settlement information(optional)
6	FI specific	Transaction information, counterparty details

iii. Request-to-Pay Flow

TABLE H3 **Proprietary Messages and Important Fields for Request-to-Pay Flow**

STEPS	MESSAGE TYPE	IMPORTANT FIELDS
1	FI specific	Identifiers, debtor, creditor, requested transaction details including amount, remittance information
2–3	Implementation specific	Identifiers, debtor, creditor, requested transaction details, charge bearer, remittance information
4	FI specific	Requested transaction details, requestor details, amount details
5	FI specific	Response details
6–7	Implementation specific	Response code, response details, identifier, original request message details
8	FI specific	Response details

APPENDIX I: AUTHORIZATION <AUTHSTN> DETAILS

This tag is used for user identification or to check whether the initiating party is permitted to make the transaction from the specified account in the message by usage of any type of user key.

1. **Code <Cd>**

   This tag represents authorization in a predefined coded format and can be used for sending the authentication confirmation. The codes are defined as follows:

   a. AUTH (Preauthorized file)

   b. FDET (File-level authorization details)

   c. FSUM (File-level authorization summary)

   d. ILEV (Instruction-level authorization)

2. **Proprietary <Prtry>**

   This tag specifies the authorization in a free-text format with a maximum length of 128 characters. This tag can be used to carry PINs, passwords, and other customer-authentication details after encrypting the data.

APPENDIX J: AUTHENTICATION <AUTHNTCN> TAG DETAILS

The Authentication <Authntcn> tag can carry the following details:

1. **Message Authentication Code <MsgAuthntcnCd>**

   Message Authentication Code is used for assuring nonrepudiation of messages. It is used for confirming that the stated sender has sent the message and that it has not been changed in the transportation of the message.

2. **Date <Dt>**

   This tag will contain date and time information on which the authentication is provided.

3. **Channel <Chanl>**

   This tag is a parent tag and represents the channel used to authenticate the transaction. This tag does not carry information but has the following subtags/elements:

   3.1 Code <Cd>

   The tag contains a list of predefined values for the channels used to authenticate the customer—that is, the channel used to authenticate the mandate. The list has the following:

   a. ATM
   b. CARD
   c. INBA (Internet banking)
   d. MOBI (Mobile)

   3.2 Proprietary <Prtry>

   Proprietary codes can be input in this tag to represent another form of customer authentication done apart from the predefined list of codes.

APPENDIX K: UPI: MOBILE BINDING PROCESS

The process of mobile binding is accomplished by the following steps:

1. **Telephony manager**

   This process is to collect the device ID and International Mobile Equipment Identity (IMEI) of the device on which the application is going to be used.

2. **Silent SMS process**

   In this process, a message is sent to verify the user's mobile number entered during the registration process.

3. **Get mobile number PSP server**

   This process has three input parameters—that is, device ID, IMEI, and SMS (which is sent to the server). The server responds back with the mobile number confirmation of user.

4. **Register user webservices**

   In this process, a call is made to the PSP server name used at the time of registration. If all the data sent is correct and matches the PSP records, either the PSP sends a successful message or an error message is displayed to the user.

5. **Log-in page**

   On a successful registration, the user is redirected to a log-in page, where, to add the bank account, a log-in pin is required that was set at the time of registration.

6. **Validate user webservice**

   Once the PIIN is entered, a validated user webservice is called. If the details are correct, the user is redirected to the main menu, from where the actual transactions can be made.

NOTES

1. IBM, https://www.ibm.com/docs/en/ftmswsfm324?topic=components-message-standards-message-definitions-message-domains
2. ISO, https://www.iso.org/obp/ui/#iso:std:iso:8583:-2:ed-1:v1:en
3. ISO, https://www.iso20022.org/iso-20022-message-definitions?business-domain=1
4. SWIFT, https://www.swift.com/standards/iso-20022
5. The details of the change requests submitted are available on the following portal: https://www.iso20022.org/development/status-iso-20022-submissions
6. BCS Consulting, https://www.bcsconsulting.com/blog/iso20022-interoperable-or-not-so-standard/
7. SWIFT, https://www.swift.com/standards/iso-20022
8. Financial Transaction Message Tools, http://www.fintrnmsgtool.com/iso-mti-code.html
9. ISO, https://www.iso20022.org/iso-20022-message-definitions?business-domain=1
10. Third-party providers rely on customer accounts of other financial institutions.
11. IRDBT, https://www.idrbt.ac.in/assets/publications/Reports/IPTS2018/K.Spandana.pdf
12. https://sites.google.com/site/paymentsystemsblog/iso8583-financial-transaction-message-format
13. https://sites.google.com/site/paymentsystemsblog/iso8583-financial-transaction-message-format
14. https://sites.google.com/site/paymentsystemsblog/iso8583-financial-transaction-message-format
15. More details on the RTPG scope and messages can be found at https://www.iso20022.org/catalogue-messages/additional-content-messages/iso-20022-real-time-payments-group-rtp


WORLD BANK GROUP