Frequently Asked Questions (FAQ)

1. What is ISO 20022 standard?

- ISO 20022 - Universal financial industry message scheme (which used to be also called "UNIFI") is the international standard that defines the ISO platform for the development of financial message standards. Its business modelling approach allows users and developers to represent financial business processes and underlying transactions in a formal but syntax-independent notation. These business transaction models are the "real" business standards. They can be converted into physical messages in the desired syntax. At the time ISO 20022 was developed, XML (eXtensible Mark-up Language) was already the preferred syntax for e-communication. Therefore, the first edition of ISO 20022 proposes a standardized XML-based syntax for messages. The standard was developed within the Technical Committee TC68 - Financial Services of ISO - the International Organization for Standardization.
- The Standard is issued by ISO Technical Committee 68 (TC68), which is responsible for Financial Services in ISO.
- The Standard is managed by Working Group 4 (WG4), a sub-group of TC68 whose charter is "the management of ISO 20022".
- The Standard defines a Repository Management Group who manages the content of the Repository.
- SWIFT is the Registration Authority for ISO 20022.

2. Why was ISO 20022 developed?

The need for ISO 20022 standard arose in the early 2000's with the widespread growth of Internet Protocol (IP) networking, the emergence of XML as the 'de facto' open technical standard for electronic communications and the appearance of a multitude of uncoordinated XML-based standardization initiatives, each having used their own "XML dialect". On top of offering a common way of using XML, the new standard shields investments from future syntax changes by proposing a common business modelling methodology (using UML - Universal Modelling Language) to capture, analyze and syntax-independently describe the business processes of potential users and their information needs.

3. What are the parts of ISO 20022 message?

The ISO 20022 Business Message consists of two parts:

(1) ISO 20022 Business Application Header
(2) ISO 20022 Messages

4. What are the ISO messages defined in this document?

i) head.001.001.01 Business- Application Header
ii) pacs.008.001.03 FIToFICustomerCreditTransferV03 : for Customer Credit transfer.
iii) pacs.009.001.03 - FinancialInstitutionCreditTransferV03 : for Interbank transfer, for defining the MNSB request & defining the Own account transfer in NG-RTGS.
iv) camt.054.001.03 BankToCustomerDebitCreditNotificationV03: for Customer Credit Debit Notification.
v) pacs.002.001.04, FIToFIPaymentStatusReportV04 : for MNSB Response & Own Account Transfer Response in NG-RTGS.
vi) pacs.004.001.03 PaymentReturnV03: to undo a payment previously settled.
vii) camt.053 BankToCustomerStatement end-of-day NG-RTGS statements to the Participants
viii) camt.998.001.02 to transmit various free format information to the Participants
ix) MX admi.004.001.01 SystemEventNotificationV01: to notify the occurrence of an event in a central system.

5. What is the Business Application Header?

The Business Application Header is a header that has been defined by the ISO 20022 community that form part of an ISO 20022 business message. Specifically, the BAH is an ISO20022 message definition (head.001.001.01) which can be combined with any other ISO20022 message definition to form a business message. It gathers together, in one place, data about the message, such as which organisation has sent the business message, which organisation should be receiving it, the identity of the message itself, a reference for the message and so on.

6. Whether all messages will have BAH?

All messages listed above will have the BAH attached to it.

7. What is the purpose of the BAH?

The purpose of the BAH is to provide a consistent and predictable way for this data to be conveyed with the message, regardless of implementation factors such as the choice of network. This does not prevent such data being conveyed either within the ISO 20022 message definition itself, or as part of a network header.

8. What's in the BAH?

The BAH consist of 9 building blocks

From: This mandatory field contain the details about the organisation that sent the message.
In NG-RTGS the inward messages will always be originated from RBI because of the 'V' topology, hence this field will always have the IFSC of RTGS for all inward messages to the bank.
To: This mandatory field contains the details about the organisation that should receive the message.
In NG-RTGS the outward messages will always directed to RBI because of the 'V' topology, hence this field will always have the IFSC of RTGS for all outward messages from the bank.
Business Message Identifier: a unique identifier for this particular message instance, as defined by the sending application or system;
Message Definition Identifier: the identity of the message definition
BusinessService: To identify the Business service.
Creation Date: the creation date (and time) for the data in the BAH;
Copy Duplicate and Possible Duplicate: fields to aid the identification of duplicate data;
Signature: Contains the digital signature of the Business Entity authorized to sign this Business Message.
Related: Specifies the Business Application Header of the Business Message to which this Business Message relates. Can be used when replying to a query; can also be used when cancelling or amending.

9. What is the member identification used in BAH?

Member identification is a mandatory field. The existing 11 character IFSC (Indian Financial System Code) is used as Member Identification. It is formed as below

Character position	Information	Remarks
First four characters	Bank code	Four Characters of bank Code
Fifth character	Zero	Reserved for future use
Last six characters	Branch code	Banks to use their existing codes with no white spaces(zeroes prefixed)

10. What is the BusinessMessageIdentifier in BAH?

 It is a mandatory field which uniquely identifies the message. It is defined as 22 character unique number as given below:
XXXX – Sender IFSC [4] first four characters of the IFSC
YYYYMMDD – creation date [8]
X – channel identification [1]
Nnnnnnnnn Sequence Number [9]

The Channel Identifier (X) may be used to identify channels such as Internet banking, Cash Management, Treasury, ATM, etc.

The values suggested are:

Channel ID	Values
NG-RTGS	9
Internet Banking	1
Cash Management	2
Treasury	3
ATM	4
Other	5

11. What is MessageDefinitionIdentifier?

It is a mandatory field which defines the name of the Business Message as published on the ISO 20022 website.
E.g. pacs.008.001.03

12. What is BusinessService?

It is a mandatory field specifying the business service agreed between the two MessagingEndPoints under which rules this Business Message is exchanged. It comprises a fixed value of "RTGS", and in the case of BAH for pacs.008 and pacs.009 the fixed value of "RTGS" must be followed by the local instrument name, i.e.
for RTGS, BAH for pacs.008: 'RTGSFIToFICustomerCredit'.
For RTGS, BAH for pacs.004; 'RTGSPaymentReturn'

For RTGS, BAH for pacs.009:-'RTGSFIToFICredit' or -'RTGSOwnAccTtransfer' or -'RTGSNetSettlement**XX**z**NN**'

Where 'XX' is the clearing type which may take values 'GC', 'IB', 'FX', MC, SE, OT & so on.

'z' is the indicator which may take values C –Original, R-Return, L-Last Return.
"NN" is the return serial.

 "GC" stands for guaranteed settlement of Securities and CBLO segment.
"IB" stands for guaranteed settlement of FOREX segment.
"FX" stands for non guaranteed settlement.
"MC" Stands for MICR Clearing
"SE" stands for non-guaranteed MNSB
"OT" stands for Other MNSB

13. How to define CreationDate?

It is a mandatory field which is defined as the Date and time when this Business Message (header) was created. The format is yyyy-mm-ddThh:mm:ss. Time upto second is recorded.

14. How CopyDuplicate is used in BAH?

It indicates whether the message is a Copy, a Duplicate or a copy of a duplicate of a previously sent ISO
20022 Message **DUPL** Duplicate(Message is for information/ confirmation purposes. It is a duplicate of a message previously sent).
Valid Values are:
CODU
COPY
DUPL

15. What is stored in Signature field?

It contains the digital signature of the Business Entity authorised to sign this Business Message (payload). The **Sgntr** block contains the following elements.

Message item	XML Tag
SHA2 Signatures	*<XML Sgntrs>*

16. How the end-to-end security is ensured in NG-RTGS transactions?

The RequestPayload will be used as single message tag which will contain both BAH along with signed and encrypted Business Message. The signature is attached in the BAH in <XML Sgntrs> tag before transmitting the message to NG-RTGS system by the bank. Further, the business message will be encrypted before it is transmitted over the Wide Area Network (WAN).

17. Can the bank use Straight Through Processing (STP) between CBS and NG-RTGS?

The banks can use STP between CBS and NG-RTGS in two possible ways
The STP between the CBS and NG-RTGS is faciliated by either the SFMS thick client or by the implementation of the web-service API provided it is PKI enabled. For the API option the requirements on the bank's CBS are:
-   Implementation of a client for the API (or purchase an equivalent commercial product) and integration of the client with the CBS

- Owning a valid certificate to be able to connect to the NG-RTGS. For the thick client the SFMS infrastructure (updated with the latest patch for the MI client as provided by IDRBT) may be upgraded with proper sizing if required.

18. When the field 'Related' can be used?

The Related field can be used while replying to a query; can also be used when canceling or amending a transaction. This field must be present when CopyDuplicate field is present.

19. How a FIToFICustomerCreditTransfer message is defined?

FinancialInstitutionToFinancialInstitutionCustomerCreditTransfer message is sent by the debtor agent to the creditor agent, directly or through other agents and/or a payment clearing and settlement system. It is used to move funds from a debtor account to a creditor. The FIToFICustomerCreditTransfer message is composed of two building blocks (i) Group Header (ii) Credit Transfer Transaction Information.

(i)   Group Header: This building block is mandatory and present once. It contains elements such as MessageIdentification and CreationDateAndTime.

(ii)   Credit Transfer Information: This building block is mandatory and for RTGS it will be present only once. It contains elements related to the debit and credit side of the transaction such as Creditor, CreditorAgent, Debtor and DebtorAgent.

20. What is MessageIdentification?

It is a mandatory field and is same as the BusinessMessageIdentifier defined in the BAH above.

21. What is CreationDateTime and how it is different from the CreationDate defined in BAH?

CreationDateTime is the mandatory filed containing date and time at which this message was created and the CreationDate is the date and time at which the message header is created. The format of the date time is same throughout the message.
.

22. How the field NumberOfTransactions <NbOfTxs> is defined?

It provides the number of individual transactions contained in the message. The default value is 1 for Pacs.008 and Pacs.009 messages and ten(10) or more for NEFT. In some situations, viz. at the end of the batch or end of day, the number of NEFT transactions can be less than 10. In MNSB request this is defined as the number of participants in the batch. The datatype is numeric. It is a mandatory field.

23. What the field TotalInterbankSettlementAmount <TtlIntrBkSttlmAmt> used for?

This mandatory field gives the total amount of money moved between the instructing bank and the instructed bank.
Data Type: ActiveCurrencyAndAmount
This data type must be used with the following XML Attribute: Currency (Ccy) which is typed by ActiveCurrencyCode.
 Format: Amount
MinInclusive   0
TotalDigits   18
fractionDigits   2

Maximum digits = 18. Decimal mark excluded from count.

Note: The decimal separator is a dot.
ActiveCurrencyCode
ActiveCurrency
The currency code must be a valid active currency code of three (3) contiguous letters. For Indian Rupee the active currency code is INR
Example:
        <TtlIntrBkSttlmAmt Ccy='INR'>2345</TtlIntrBkSttlmAmt>

24. What is InterbankSettlementDate <IntrBkSttlmDt>?

It is a mandatory field providing the settlement date.
Data Type: ISODate

25. How SettlementInformation <SttlmInf> is defined?

This is a mandatory element defined as:
Definition: Specifies the details on how the settlement of the transaction(s) between the instructing bank and the instructed bank is completed.

26. How to define SettlementMethod <SttlmMtd>?

It is the method used to settle the (batch of) payment instructions with Data Type: Code It is a mandatory field.
One of the following SettlementMethod1Code values must be used:

Code	Name	Definition
CLRG	ClearingSystem	Settlement is done through a payment clearing system.
COVE	CoverMethod	Settlement is done through a cover payment.
INDA	InstructedAgent	Settlement is done by the agent instructed to execute a payment instruction.
INGA	InstructingAgent	Settlement is done by the agent instructing and forwarding the payment to the next party in the payment chain.

For the NG-RTGS system the default value is CLRG.

27. How to interpret InstructingAgent?

It is the agent that instructs the next party in the chain to carry out the (set of) instruction(s). It is mandatory in RTGS implementation.
The value for this Field tag 'InstructingAgent' should be the IFSC code of the Head office of the Sending bank.

28. What is FinancialInstitutionIdentification field used for?

This is a mandatory field which provides the identification of the Financial Institute referred to.

---

29. What details to be entered in ClearingSystemMemberIdentification field?

This mandatory field is used to enter the details of the participating bank. The mandatory sub-field MemberIdentification is used to provide IFSC of the concern participant. In case of InstructingAgent this field contains the IFSC of sending bank, while for the InstructedAgent this field contain the IFSC of the receiving bank.

30. What is InstructedAgent?

This mandatory field gives information about agent that is instructed by the previous party in the chain to carry out the (set of) instruction(s). It is defined by using FinancialInstitutionIdentification- ClearingSystemMemberIdentification- MemberIdentification. It is mandatory in RTGS implementation.
In case of Own Account Transfer this field provides the RBI IFSC.
The value for this Field tag 'InstructedAgent' should be the IFSC code of the Head office of the Receiving Bank.

31. How to use the field CreditTransferTransactionInformation ?

It is mandatory and is a set of elements providing information on individual transactions. Only one occurrence allowed for Customer Payment in RTGS system and 10 or more for NEFT. In case of Pacs.009 used for MNSB request multipal occurrence based on number of participants is allowed.
    The elements are: PaymentIdentification <PmtId>, PaymentTypeInformation <PmtTpInf>, ChargesInformation <ChrgsInf>, Debtor <Dbtr>, DebtorAccount, <DbtrAcct>, DebtorAgent <DbtrAgt>, Purpose <Purp>, ..., RemittanceInformation <RmtInf>.

32. How to use PaymentIdentification <PmtId> field?

It is a mandatory field giving set of elements used to reference a payment instruction.
Type: *This message item is composed of the following **PaymentIdentification** element(s):*

Message Item	<XML Tag>	Mult.	Represent./ Type
InstructionIdentification	<InstrId>	[0..1]	Text
EndToEndIdentification	<EndToEndId>	[1..1]	Text
TransactionIdentification	<TxId>	[1..1]	Text

i)   **InstructionIdentification <InstrId>**

Presence: [0..1]
Definition: Unique identification, as assigned by an instructing party for an instructed party, to unambiguously identify the instruction.
Usage: The instruction identification is a point to point reference that can be used between the instructing party and the instructed party to refer to the individual instruction. It can be included in several messages related to the instruction.
Data Type: Max35Text
Format: maxLength: 35
       minLength: 1

During the transition of existing member systems to the new ISO message formats, it is used for supplementary identification, such as the legacy transaction reference number (R41/R42.2020).

ii)   **EndToEndIdentification <EndToEndId>**

Presence: [1..1]
Definition: Unique identification, as assigned by the initiating party, to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain.
Usage: The end-to-end identification can be used for reconciliation or to link tasks relating to the transaction.
It can be included in several messages related to the transaction.
Usage: In case there are technical limitations to pass on multiple references, the end-to-end identification must be passed on throughout the entire end-to-end chain.
During the transition of existing member systems to the new ISO message formats, the EndToEndId should follow the 16 digits UTR pattern of the existing RTGS system, identified with the 6 character codeword prefix "/XUTR/". The existing UTR format is:

- Participant System ID (First four Characters of sending Bank's IFSC Code)
- Service Tag (One Character) Example : "H" for host
- Unique-ID comprising of Date (Julian date YYDDD) & Sequence Number (6 digits numeric)

iii)   **TransactionIdentification <TxId>** This is a mandatory field.
Definition: Unique identification, as assigned by the first instructing agent, to unambiguously identify the transaction that is passed on, unchanged, throughout the entire interbank chain.
Usage: The transaction identification can be used for reconciliation, tracking or to link tasks relating to the transaction on the interbank level.
Usage: The instructing agent has to make sure that the transaction identification is unique for a pre-agreed period.
Data Type: Max35Text
Format: maxLength: 35
         minLength: 1

In our case it is the Unique Transaction Reference (UTR) which would be of 22 characters
Format is:
XXXX- Sender IFSC   [4]
X-Payment System   [1]
X-Channel   [1]
YYYYMMDD-Date   [8]
nnnnnnnn- Sequence Number   [8]

Codes for Payment System (X) are:
R->RTGS
N->NEFT
A-> ACH

The Channel Identifier (X) may be used to identify channels such as Internet banking, Cash Management, Treasury, ATM, etc.

The values suggested are:

Channel ID	Values
NG-RTGS	9
Internet Banking	1
Cash	2

Management	
Treasury	3
ATM	4
Other	5

33. What data is to be provided in PaymentTypeInformation <PmtTpInf>?

This mandatory field contains set of elements used to further specify the type of transaction.
Type: *This message item is composed of the following **PaymentTypeInformation** element(s):*

Message Item and <XML Tag>	Mult.	Represent/ Type
InstructionPriority <InstrPrty>	[1..1]	Code
ServiceLevel <SvcLvl>	[0..1]	
LocalInstrument <LclInstrm>	[1..1]	
CategoryPurpose <CtgyPurp>	[1..1]	

i)   **InstructionPriority <InstrPrty>**

Presence: [1..1]
Definition: Indicator of the urgency or order of importance that the instructing party would like the instructed party to apply to the processing of the instruction.
Data Type: Code
The default priority assigned to every message is HIGH.

Code	Name	Definition
HIGH	High	Priority level is high .
NORM	Normal	Priority level is normal.

ii)   **ServiceLevel <SvcLvl>**

Presence: [0..1]
Definition: Agreement under which or rules under which the transaction should be processed.
Type: *This message item is composed of one of the following **ServiceLevel Choice** element(s):*

Index	Message Item	<XML Tag>	Mult.	Represent./ Type
2.11	Proprietary	<Prtry>	[1..1]	*Text*

Proprietary <Prtry>

Presence: [1..1]
Definition: Specifies a pre-agreed service or level of service between the parties, as a proprietary code. For RTGS processing priority is in range 00 – 99. This field also contain the Transaction Type code (TTC) along with the priority value. TTC values will be used to differentiate the transactions within the same type of transaction. e.g. in the pacs.009 transaction message the MNSB Own account transfer and Interbank transaction will have different TTC values.

Use: To be used for managing queues by sending bank before settlement.
Data Type: Max35Text
Format: maxLength: 35: For RTGS lower the number highest will be the priority.
For Banks priority range is from 11 to 99. Priority from 00 to 10 is reserved for RBI.
<SvcLvl>
  <Prtry>
     [TTC=**xxxx**],[PRI=**xx**]
  </Prtry>
</SvcLvl>

List of *Transaction Type values (*TTC) & Priority for RTGS System

TTC Value	Transaction Type	Priority Range	Default Priority	IDL Facility	Members Eligible

1000	Customer	11-99	35	Yes	A
1400	Inter-bank	11-99	35	Yes	A, B
1800	Own Account	11-99	35	No	A, B, D
3000	MNSB	11-99	11	Yes (for members)	C, D
3200	Inter-bank	11-99	35	No	D
3500	Customer	0-10	5	No	RBI
3600	Inter-bank	0-10	5	No	RBI
3700	MNSB	0-10	5	Yes (for members)	RBI
4000	Customer	11-99	45	No	D

Where A, B, C, D are RTGS membership types as mentioned in RTGS Business Operating Guidelines.

Membership Type	Broad Category
Type A	Regular Participant
Type B	Restricted Participant
Type C	Clearing House
Type D	Regular or Restricted Participant

iii)   **LocalInstrument <LclInstrm>**

Presence: [1..1]
Definition: User community specific instrument.
Usage: This element is used to specify a local instrument, local clearing option and/or further qualify the service or service level.
Type: *This message item is composed of one of the following **LocalInstrument2Choice** element(s):*

Index	Message Item	<XML Tag>	Mult.	Represent./ Type
2.14	Proprietary	<Prtry>	[1..1]	*Text*

Proprietary <Prtry>
Presence: [1..1]
Definition: Specifies the local instrument, as a proprietary code.
Type of local instrument.
For RTGS pacs.008 use:
-- 'RTGSFIToFICustomerCredit'
For RTGS, pacs.009 use:
-- 'RTGSFIToFICredit'
-- 'RTGSOwnAccTransfer'
 -- 'RTGSNetSettlementXXzNN'
For Return Payment use:
-- 'RTGSPaymentReturn'

Data Type: Max35Text
Format: maxLength: 35

iv)   **CategoryPurpose <CtgyPurp>**

Presence: [1..1]
Definition: Specifies the high level purpose of the instruction based on a set of pre-defined categories. Purpose of the Instrument.
Payment purpose must be a value listed in ISO category purpose code
Type: *This message item is composed of one of the following **CategoryPurpose Choice** element(s):*

Index	Message Item	<XML Tag>	Mult.	Represent./ Type

2.16	Code	<Cd>	[1..1]	Code

Code <Cd>
Presence: [1..1]
Definition: Category purpose, as published in an external category purpose code list.
Data Type: ExternalCategoryPurpose1Code
Format: maxLength: 4
           minLength: 1
Default value: CASH

FROM ISO 20022External Code list

The following codes are available.
CASH: CashManagementTransfer
CORT: TradeSettlementPayment
DIVI : Dividend
GOVT: GovernmentPayment
HEDG: Hedging
INTC : IntraCompanyPayment
INTE : Interest
LOAN: Loan
PENS: PensionPayment
SALA: SalaryPayment
SECU: Securities
SSBE: SocialSecurityBenefit
SUPP: SupplierPayment
TAXS: TaxPayment
TRAD: Trade
TREA: TreasuryPayment
VATX: ValueAddedTaxPayment
WHLD: WithHolding

The generic code for the normal funds transfer may be 'CASH'.
Example: <CtgyPurp><Cd>CASH</Cd></CtgyPurp>

34. How the funds are pushed and sweep back at the time of SOD (Start of Day) and EOD (End of Day) respectively?
The message format used for balance sweeping is Pacs.009 MNSB transaction?

a) For SOD:
- one debit against the settlement account of RBI in amount equal to the sum of all credits
- multiple credits against the settlement accounts of the Participants that have their balances initialized

b) For EOD:
- multiple debits against the settlement accounts of all Participants with a non-zero balance in NG-RTGS
- one credit against the settlement account of RBI in amount equal to the sum of all debits

Distinct TTC values are used for these two transactions
For SOD the TTC value is 5050 whereas for EOD the TTC is 5051

35. What data is to be entered in InterbankSettlementAmount field?

This mandatory field is used to provide details about the amount of money moved between the instructing agent and instructed agent. Settlement amount + currency. Datatype is amount.

36. What is meant by ChargeBearer field?

It is a mandatory field providing details about the party bearing the transaction charges. Data type is code. It is defined as
DEBT→ charges borne by Debtor
CRED→ charges borne by Creditor
SHAR-→charges are shared
SLEV→ following service level.
As per the current RBI policy the charges are borne by the Debtor.

37. What is ChargesInformation?

This optional field specifies which party will bear the charges associated with the processing of the payment transaction.
If *ChargeBearer* contains DEBT, then all transaction charges are to be borne by the debtor.
At present scenario, the charges are borne by the Debtor.
If *ChargeBearer* contains CRED, then at least one occurrence of *ChargesInformation* must be present.
If *ChargeBearer* contains SHAR, then in a credit transfer context, means that transaction charges on the sender
side are to be borne by the debtor, transaction charges on the receiver side are to be borne by the creditor. In a direct debit context, means that transaction charges on the sender side are to be borne by the creditor,
If *ChargeBearer* contains SLEV, then Charges are to be applied following the rules agreed in the service level and/or scheme).

38. How to use the Amount field?

This mandatory field stores the transaction charges to be paid by the charge bearer. The data type is amount.

39. How to use the field Agent?
It is the agent that takes the transaction charges or to which the transaction charges are due. This is a mandatory field.

40. What details are provided for debtor?

Providing debtor details is mandatory in RTGS. Under this element the following data is provided:
Name: ordering customer's name is mandatory.
Postal Address: ordering customer's postal address. This contains a sub-element named AddressLine which can be used for adding the address in free format. The number of occurrences is restricted to 4 in RTGS implementation.

41. How to use the DebtorAccount field?

This mandatory field provides the identification of the account of the debtor to which a debit entry will be made as a result of the transaction. It consists of the following sub elements
Identification: Mandatory field having a sub field named 'Other' in which a field named 'Identification' will have the debtor's account number.

42. What is DebtorAgent?

This is a mandatory field providing the details about the Ordering Institute. For RTGS participant the IFSC is provided while for non participant name and other identification with address is provided.

This may be the IFSC code of the InstructingAgent or Branch or Sub-member of the InstructingAgent. The system will validate first 4 characters of IFSC code of the DebtorAgent with that of InstructingAgent.

43. What is CreditorAgent?

This is a mandatory field providing the details about the Beneficiary Institute. For RTGS participant the IFSC is provided while for non participant name and other identification with address is provided.

This may be the IFSC code of the InstructedAgent or Branch or Sub-member of the InstructedAgent. The system will validate first 4 characters of IFSC code of the CreditorAgent with that of InstructedAgent.

44. Where to give the beneficiary customer details?

The beneficiary Customer details are given in the Creditor field. This is a mandatory field consisting of
Name – Beneficiary customer name
Postal Address – beneficiary customer address

45. How to give the creditor account details?

The CreditorAccount field is used to provide the creditor's account details. This mandatory field is used for identification of the account of the creditor to which a credit entry will be posted as a result of the payment transaction.

46. What information is provided in InstructionFoCreditorAgent field?

Further Information related to the processing of the payment instruction, provided by the initiating party, and intended for the creditor agent is given in this optional field.
 It has following subfields:

(i)   Code <Cd>

(ii)   InstructionInformation <InstrInf>

47. How to use the code field <Cd>?

The coded information related to the processing of the payment instrument, provided by the initiating party is given in this field. The following codes are used:

PHOB = Phone Beneficiary
TELB=Telecom
CHQB= PayCreditorByCheque
HOLD= HoldCashForCreditor

48. How to use InstructionInformation field <InstrInf>?

Further information complementing the coded instruction or instruction to the next agent that is bilaterally agreed or specific to a user community. It is of Datatype Max140Text.

49. Where to give the sender to receiver information?

This information is given in RemittanceInformation field. The sub field Unstructured is used to give the remittance information of 4 lines of 140 characters each.

50. How to use the field Notification?

This field notifies the debit and credit entries for the account. This block is composed of the following elements:
Identification: Unique identification, as assigned by the account servicer to unambiguously identify the account notification.
CreationDatetime: ISO date time
Account: Unambiguous identification of the account to which credit and debit entries are made.
Entry: Set of elements used to specify an entry in the debit credit notification. At least one reference must be provided to identify the entry and its underlying transaction(s).

51. What is TransactionInformationAndStatus <TxInfAndSts>?

It is related to pacs.002.001.04, FIToFIPaymentStatusReport. It is the Information concerning the original transactions, to which the status report message referred to.

52. How to use the field OriginalGroupInformationAndStatus?

This field provides the original group information concerning the group of transactions, to which the status report message refers to. It has the following sub fields
OriginalMessageIdentification <OrgnlMsgId>: Mandatary field for point to point reference, as assigned by the original instructing party, to unambiguously identify the original message.

OriginalMessageNameIdentification <OrgnlMsgNmId>: This mandatory field specifies the original message name identifier to which the message refers.

OriginalCreationDateAndTime <OrgnlCreDtTm> This mandatory field provides Date & time at which the original message was created.

GroupStatus <GrpSts> Madatory field which specifies the status of a group of transactions.
        Status code- CSC/ACSP/ACTC/ACPT/PDNG/RCVD/RJCT/ACCR /ACWC.

ACSC: AcceptedSettlementCompleted
ACSP: AcceptedSettlementInProcess
ACTC: AcceptedTechnicalValidation
ACCR: AcceptedCancellationRequest
ACPT: Accepted
ACWC: AcceptedWithChange
PDNG: Pending
RCVD: Received
RJCT: Rejected

For details on status code, pl refer to para 2.6 of documentation "Payment Clearing & Settlement – Maintenance 2012 by ISO".

53. What is StatusReasonInformation field?

This optional field provides detailed information on the status reason. (Reason for success / failure).

54. How to use the field Reason?

This mandatory field in Payment Status Report provides the reason for the status report. Reason for the status, in a proprietary form is added in the subfield 'Proprietary' (Actual reason code and reason description)

55. How the messages will flow from bank's CBS to the thick client?

The RTGS message will flow in the same manner as the SFMS messages except that The RequestPayload will be used as single message tag which will contain both BAH along with signed and encrypted Business Message. The signature is attached in the BAH in <XML Sgntrs> tag before transmitting the message to NG-RTGS system by the bank. Further, the business message will be encrypted before it is transmitted over the Wide Area Network (WAN).

56. Is XML signature used for digitally signing the message?

XML signature are not needed and the messages will be signed with PKI based SHA2 signature.

57. In case we opt to route the RTGS Messages through SFMS, do we require PI Server?

SFMS will provide a patch for the existing SFMS application. Once this patch is installed on the SFMS gateway server the same server can act as the thick client Member Interface (MI) for NG-RTGS. PI server will not be needed in the NG-RTGS environment, however; the banks may decide about the up-keeping of the PI server depending upon the archival policy of the respective bank.

58. In case we don't require PI Server, whether HSM is required?

Currently the SFMS application is not using the HSM card for cryptography; however, IDRBT has planned to upgrade the SFMS application to facilitate the hardware based encryption. Hence, the HSM cards may be required in the new version of SFMS application.

59. If HSM also is not required, how can we sign the outgoing RTGS messages? Will it be using Class2 or Class 3 certificate?

It is expected from the banks to sign the messages in the CBS application itself. However, in the absence of CBS application being able to generate the ISO 20022 standard message formats and signed the same, the MI client will digitally sign and encrypt the message.
The messages will carry a class 2 signature if the bank is using maker checker concept and if the process is STP the bank should use class 3 server signatures to sign the outgoing messages.

60. If we can use Class2, whether we can use the same certificate as the one used for NEFT.

As explained above the class 2 signature can be used in the maker checker concept.

61. In the present situation, we are supposed to fetch the certificates of other banks periodically. How this can be done in NG-RTGS?

The certificate containing the public key of the signer will be embedded in the signer information of the digital signature, so that there is no need to distribute public keys separately. However, the banks will have to maintain the CRL list as published by IDRBT CA.

62. Whether there's any chance of a DR Drill for RTGS alone once the new system comes in to effect and we use SFMS to route the RTGS messages?

The DR drill will be conducted as per the RBI BCP policy.

63. Whether we will have SOD/EOD concept?

There will not be any EOD/SOD for Web API Services client as this will be based on a pull mechanism. Usual EOD/SOD will happen in the thick client provided by IDRBT.

64. How the Message archiving will be done in the new scenario in case we don't have SOD/EOD?

The Web API services will be granted throughout the day, even before SOD and after EOD. The bank may design the Web API Server client with or without the database. The management of the Web API Server client database if any, will be handled by the banks.

65. What are the specifications for Web API Services client?

Please refer to the Annex –I

66. As discussed, our Bank has RTGS Membership but we have not yet started the RTGS Participation. We would like to go for Next Gen RTGS. Kindly provide us some guidelines, information on the same. Also request you to add my name in future programme, session, training, workshop related to Next Gen RTGS also others technology which may be useful.

As we are maintaining the address details of all RTGS members, you would be receiving operation manuals and software and other details after you fulfil the membership criteria asked by the Bank. Regarding NG-RTGS, we would be sharing the information to all members of existing RTGS system. No separate request for NG-RTGS is required.

67. User manual containing the screenshots for various users like specifications team and fund management should be made available.

User manual will be made available to all participants.

68. In our case, the RTGS and NEFT applications inward / outward messages are settling through STP (Straight Trough Process) and the CBS is maintained by HO team. The NG-RTGS is web / browser based in that case how messages are routing to CBS and vice versa.

At any given point of time only one NG-RTGS client will be operating at the banks' end. If the messages are settling through STP mode then the browser based client can only be used for viewing the reports. No transaction can be initiated through it.

69. In PO module inward and outward generated or downloaded reports should be in readable format.

The inward and outward messages can be downloaded in XML format only. Report data is automatically saved on the NG-RTGS server, which can be downloaded as required by participants in PDF format or CSV files (used by Microsoft Excel).

70. Kindly share RTGS migration plan to enable us to request same with HO team.

Migration plan will be shared shortly.

71. Is there any PI equivalent acknowledgements in NG RTGS viz R90 message?

The MX admi.004.001.01 SystemEventNotification will be used in place of R90. The following event codes will be used in the response message

F20 – Acknowledgement Message
F25 – Negative Acknowledgement
F23 – Delivery Notification message
F22 – Non-delivery Warning message
F27 – Bank API Response Message

72. Will RBI send settlement notification (Pacs.002.001.04) for all customer (pacs.008.001.03) and interbank (pacs.009.001.03) payment messages i.e. Positive and Negative settlement notification?

RBI will send camt.054 message as debit and credit notification for all customer transactions and will send pacs.002 message for MNSB response and Own Account transfer response.

73. RBI settlement acknowledgement will be based on <EndToEndId> 16 digit or <MsgId> 22 digit?
The settlement acknowledgement will contain both the IDs <EndToEndId> and <TxId> transaction identification.

74. Is there any validation on the ISO message received from Banks performed at RBI system, if yes then what are the validations?

The message validation will be performed at RBI system for all fields defined in the message format. In case of thick client, the thick client will verify the ISO message before sending it to RBI. In case of Web based API services, the API client will verify the message before sending it to RBI.

75. Does NG RTGS allow Banks to warehouse transactions at RBI e.g. Future dated transactions

The facility of Future value dated transaction will be made available after the policy decision.

76. Can we send future date RTGS transactions after cut-off date?

Yes.

77. Will the future value dated transactions be rejected in SFMS or in NG-RTGS?

The value dates of all messages/transactions entered through thick or thin clients are validated by the NG-RTGS. Hence, It can be rejected by Thick or Thin client before settlement.

78. What is the security class certificate to be attached to NG RTGS ISO messages?

All messages will be signed by the banks before it reach the NG-RTGS system. If the bank is adopting maker checker concept the class II user certificates will be attached to the message and in case of STP the class 3 server certificates will be used.

79. What is the encryption method for ISO Messages?

The Member Interface (MI) will encrypt the message in the same manner as that of SFMS messages. Currently the messages will be encrypted using software based encryption; however, IDRBT will be upgrading the SFMS application for using hardware based encryption.

80. By when the mapping document of Rxx-MX will provided to the banks?

The mapping document is available on the RBI website.

81. By when all business rules would be ready in view of the revision in the message format document?

The business rules are published on the RBI website.

82. If a bank is sending XML transactions via SFMS application server, also can the bank User will be allowed login to Web browser and Create/approve OAT transactions ?

There would be three modes of access for accessing NG-RTGS application. i.e., Thick Client, Web API Server and Browser based Client. All these modes will be made available over INFINET for the present. As a part of BCP Strategy, in case INFINET is down, browser based client through Internet will be enabled for Banks. All these modes of Access will be PKI enabled. Banks need to define their primary terminal and Secondary terminal at the time of participating in NG-RTGS. Initiation of transactions would happen at Primary Access mode of the bank. Browser based clients would be provided to all the banks for querying the status of the transaction irrespective of their choice of access mode. However, at any point of time, banks would be allowed to initiate their financial transaction using only one access mode which will be declared by the banks and accordingly configured in the NG-RTGS application and would be used for the purpose of routing in normal case. Secondary mode of access will be allowed only in case failure of primary mode of access.

83. Can we have SFMS as the primary terminal and a web browser as standby terminal?

 Yes.

84. Whether an existing PI user's e-Token with a digital certificate can be used to access NG-RTGS system as well?

Yes. The Web API Server client will be fully STP based hence no user will be involved. In the browser based client and thick client for maker-checker process the e-tokens can be used. The existing e-tokens, if supported by the NG-RTGS application can be used.

85. For default Purpose code, earlier it was mentioned that 'OTHR' has been included in the list of code and can be used as a default code. However in the revised document, we can't locate OTHR code and also default code has been identified as 'CASH'. Kindly clarify?

The revised formats are frozen for the development. However, the codes may undergo addition/changes depending upon the same registered with the ISO Registration Authority.

86. If CBS is not in a position to capture the purpose code, how it can be incorporated? Whether it will always be cash?

CBS systems of the bank need to be suitably upgraded to capture purpose code. The Purpose Code "**CASH**" as default will be used till Bank migrate to ISO 20022 message formats.

87. For Web API Services interface between CBS and NG-RTGS system, can we know whether the interface will ride on MQ or https: connectivity?

The Web API interface will be based on HTTPS protocol only. For Connecting to NG-RTGS system Web API Server would be provided by NG-RTGS solution provider. However, building necessary interface from CBS of your banks to the Web API Server rests on the bank.

88. Earlier in the present system (PI System) RTGS and message hub used to lie at RBI. Now the message hub is lying at IDRBT or at RBI?
The message hub would reside at both the locations IDRBT and RBI. However, it does not matter to the user.

89. Return Payment Flow-Failures (Unsuccessful settlement) – In the current RTGS setup the returns are by the way of R42 message, but whereas in NG-RTGS returns are by way of R41 message. Which format is used currently?

A separate message format pacs.004.001.03 PaymentReturnV03 will be used for return payment in the NG-RTGS system.

90. What is the difference between Y topology & V topology?

RBI opted for V topology to implement NG-RTGS in multiple channels. In the Y topology the core RTGS application acts as the settlement engine and all other jobs are performed by the routing application (in our case IFTP). The IFTP was stripping the message and holding the information till the message is processed at RTGS system. All the communication from the banks with the RTGS happened only through the IFTP. In the V topology the full message as sent from the bank is received, processed and responded by the central RTGS system
RBI has opted for V topology to enable multiple channels in NG-RTGS.

91. R-20/F-20 and R23/F23 remains same as NEFT?

Please refer to Q. 68.

92. Validation of IFSC-Some branches initially enabled only for NEFT then for RTGS. IFSC type is SFMS. Are you going to introduce some more IFSC's?

NEFT IFSC's are validated with NEFT IFSC's only.

93. Is there any new field which is there in xml and which is not there in earlier message formats?

Kindly see the mapping document as available on RBI website.

94. Every message received from NG-RTGS forwarded to core banking. Can we hold the messages at SFMS, if in case CBS is not able to process the messages?
SFMS will not hold the message, after initial validations it will pass on the message to the next node i.e. CBS.

95. Dash Board is available for all messages. Not differentiating between RTGS & NEFT messages?

Separate dashboard will be available for both the applications.

96. Is Dashboard provided for outward/ inward liquidity management?

Dashboard for inward/outward liquidity management is included in the browser-based GUI of NG-RTGS.

97. Regarding multiple application – Can we push transactions for multiple back offices for RTGS?

Multiple Back office applications can interface with CBS of the Bank and then in turn can interface with NGRTGS.

98. RTGS messages mandatorily signed at CBS at Block A or at Block 4?

Currently the signature is put in Block 5 however, in the NG-RTGS the signature will be put in the tag *<XML Sgntrs> in BAH.*

99. Is there any flag to put the regular signature in the Current R series message?

Structure is Block A, Block 4 and Block 5A. Block 5A contains signature.

100. If bank's application is not ready for ISO message then bank will send MT message to MI. MI will convert the message to ISO format then whether that signature is valid at bank end or not?

MI after receiving the signed MT message will validate that signature with content of data, if the validations are successful then it will generate xml message and sign with the server certificate of MI.

101. Details about the changes in MQ in new environment?

Guidelines will be given to configure MQ in new environment for the thick client. The Web API services will only use HTTPS protocol.

102. Plan of RBI for transmitting xml and text format in parallel?

NG-RTGS will only use ISO20022 standard message format for receiving and sending the messages. If converters are used at bank end then the bank has to send and accept R series message to and from the convertor.

103. Is RBI planning to use any converters?

IDRBT will be providing a patch for the SFMS application which will convert the R series messages into ISO 20022 standard message format. However, use of convertor is only for interim period till bank migrate to ISO 20022 formats and share its plan of migration with RBI.

104. Primary dealer (type B member) of existing RTGS system who do not have NEFT or SFMS. Whether existing RTGS will be discontinued or they need to move SFMS as a fresh?

These members can move to thin client as the transaction volume is not high.

105. Banks are having two servers one for SFMS and the other for RTGS and using same infinite network for incoming messages. All their messages will be directed through the same network or not?

It is technically feasible to use the same network however, a document will be provided after thorough testing.

106. What is the size of the ISO message?

The full ISO message size is 6KB - (full xml – (2K), business header – (0.8K) and signature – (3K))

107. At treasury level (Settlement Account) will there be any change at the bank end?

No. Liquidity Reservation facility is available in the application. Banks has to decide whether they want this facility or not.

108. Own Account transfer through E-kuber will be available or banks have to use NG-RTGS only?

Both applications will have OAT facilities. In case of transfer of funds from Settlement Account to the Current Account of the Bank, the Bank can initiate OAT transaction by using NG-RTGS application. However, for the reverse, it will be using E-Kuber provided by CBS of RBI.

110. How LAF will be conducted?

Currently LAF is settling in E-kuber. It will continue to settle in E-Kuber. A policy decision will be taken on the continuation of LAF in E-Kuber application. RBI will intimate the banks accordingly.

111. Message creation facility is available in PI system in the current RTGS application. Will such facility be available in NG-RTGS?

In NG- RTGS PO systems is available through which one can originate the transaction.

112. In PI banks have right to reject or cancel any transaction? Is this facility available in NG-RTGS?

Transaction level visibility will be available in the application. Further, there are two level authentications available for each transaction. The transaction can be cancelled before settlement.

113. Any transactions originated by branches can be cancelled in MI?

Transaction cancellation facility is available till the transaction is not settled.

114. Will there be any second level authorization for STP transactions at MI level?

For STP mode there is no need to authorize. However, an alert gets displayed for very high value transactions.

115. Can the Alert be configured?

Alerts are configured centrally and set by RBI. In NG-RTGS there will be visibility of bank's accounting position.

116. What will be the Logic for CBS to generate the signature?

CBS will digitally sign the ISO 20022 message in the *<XML Sgntrs> tag to provide authenticity and non-repudiation by the bank.*

117. Whether the digital signature has to be done by the banks at ground level or can it be done centrally?

Banks can take this policy decision, however, the NG-RTGS application accept a digitally signed ISO 20022 message only.
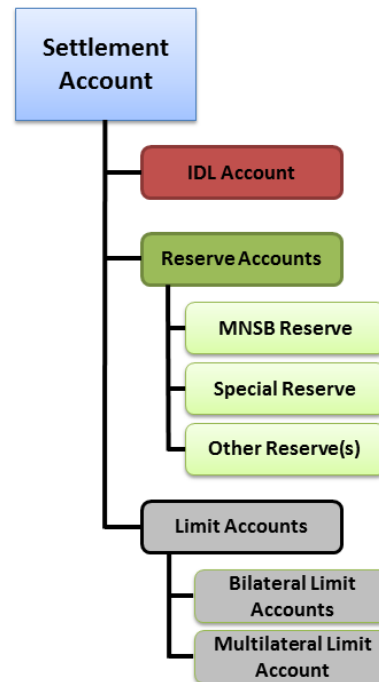
118. What is the Reverse Repo Code for IDL?

The reverse Repo Transaction Type code (TTC) for IDL is 5031.

119. RBI Accounts (Existing and Proposed settlement accounts)?

Each participant will have one Settlement Account in the NG-RTGS system. Participants may also use reserve accounts to put funds aside for specific purposes, as described in Figure below:

120. What is the equivalent ISO 20022 message for R09? (Notification after settlement)

 'camt.054.001.003' BankToCustomerDebitCreditNotification' will be used to send a debit notification to the sending bank. Except for MNSB transactions, no credit notification will be sent for successful transactions.

121. Is there any need to upgrade the existing infrastructure for NG-RTGS?

The banks which will be using MI thick client may take the policy decision depending upon their transaction volume and scalability of the SFMS infrastructure at their end.

122. Whether a bank has to purchase message broker application from IDRBT or they can choose from outside vendors?

No message broker solution is required for thick client.

123. What will be the cost involved for participating in NG-RTGS?

For using the PO client, zero cost will be incurred by the bank if they are having INFINET connection.

For using Web API services, the bank will have to build an interface for STPing the transactions to the central web API server.

For using MI thick client, the bank if required will upgrade the hardware as per the sizing requirement.

124. What will be the prerequisite for the existing SFMS for accommodating NG-RTGS?

Please refer to the patches released by IDRBT in its web site for accommodating the NGRTGS requirements in the SMFS infrastructure. These patches will be part of the SFMS AMC.

125. Different servers for RTGS and NEFT are suggested?

The solution will be provided and implementation is left to the bank.

126. Whether SFMS module patch will also take care of digital signature provided the banks take the signature from IDRBT or will that have to be incorporated at the separate level?

The SFMS module can take care of the digital signature however, RBI except the bank to sign the messages through their CBS application.

127. Whether network connection is a Broadband Connection or INFINET connection?

The IFINET connections will be used for network.

128. In NG-RTGS, where the database will be maintained?
The NG-RTGS application will have live data of last 7 days. However, the RBI Data warehouse CDBMS will store the older data.

129. Whether small banks do not require the MQ series and other things to connect to the NG-RTGS?

The small banks can connect through PO client which only needs an INFINET connection.

130. Whether the user administration of the PO will be with the Bank or RBI?

The PO user administration will reside with the banks.
For the PO, the user management will take place centrally in the PO application. Here, every user will have a profile and a password. Also, he/she will be required to have a certificate stored on an e-Token. The bank can assign a security officer who can manage the user profile for that bank, revoking or assign new functions to their users as found appropriate.

131. In case of thin client database will be at RBI end, but in case of thick client whether bank needs to mount the database locally?

The database holding the messages entered in PO and the rest of the information is central, at RBI. . The messages received by the NG-RTGS via the API will be stored in the same central database as the messages received directly from the thick client.

The existing SFMS infrastructure will be used for the thick client. Hence, the database for thick client will reside locally at bank end.

132. In the current scenario we are having production NR and DR. So in this case can we eliminate the NR factor over here?

This policy decision may be taken by the banks.

133. In the current scenario FINACLE is sending message to RBI through MQ. In NG-RTGS what will be the media?

The Messaging middle ware will be MQ for the thick client. Banks need to develop an interface to the Web API server.

134. Can we merge the existing database in NG-RTGS?

 No.

135. From end-to-end successful payment message, how many acknowledgement messages are we going to get?

Kindly see the message flow document.

136. If ISO validation failed in the message, then how it will be responded?

The invalid message cannot be submitted. The ISO validation will be performed by the thick client or Web API Services client.

137. Are there any options available to set a slab wise authorization labels?

User management will be available with the banks, through which they can set the authorization levels.

138. Do we have any similar features in PO & Thick client? Or is there any difference?

The thick client can directly be connected to the CBS application for STP. Further it will have its own database and the processing capacity will be high as compare to PO.
The transaction details needs to be keyed-in in the PO client, the STP facility will not be available here. The transaction response will be pushed to the thick client, where as the PO and API client will need to pull the response from RBI.
The reports will be only available from NG-RTGS browser access and not from the thick client.

139. In PO module can there be still any integration with CBS?

 No, the PO module is meant for manual entry in the application.

140. What is the file format to upload RTGS transaction at PO module?

The format is ISO 20022 only. Also, the messages must be signed.

141. Thick client v/s Web browser whether bank will have choice of using the system?

Yes.

142. Whether there is any need to convert the existing data to ISO XML format for future reference?

No, depending upon the data archival policy of the banks, the banks have to maintain and manage the PI server database for the required time period.

143. How performance of the system will improve in NG-RTGS?

The NG-RTGS system is designed to handle 10 lakh transactions in a day with a peak volume of 2.5 lakh transactions in an hour.

144. In the ISO message structure how does one know what are mandatory and optional fields?
In the ISO message formats the mandatory field has the ISO multi defined as **[1..n]** while for the optional field it is defined as **[0..n].**

145. Internet based message creation can we give it to client directly?

No. the access to the secured site will only be provided to banks.

146. Whether this entire architecture IPV6 Compliant?

Yes.

147. What type of client is to be selected?

NG-RTGS Access Guidelines:
  Category I: Top Banks covering 90 percent of RTGS Business or having more than 2000 RTGS transactions per day -**Thick Client - Compulsory**
  Category II: Mid-Sized Banks having RTGS transaction volume of more than 100 transactions per day and less than 2000

Transactions per day -**Web API Services Client**

 Category III: Small Banks having less than or equal to 100 RTGS transactions per day -**PO module access**
Category II and Category III banks can also opt for thick client depending on their expected RTGS transaction volume in future. Every Member Bank can opt for minimum two Modes of Access for NG-RTGS. Members who opt for Web API mode of Access need to integrate their Core Banking Solution with Web API.

148. Handling of NRE account currently in R41 we receive NRE 1 in 7495 field based on this field bank takes decision on processing.

In the message format there is field tag account type, this field will be used to take care of NRE transactions and a circular will be issued.

149. Are RTGS timings going to undergo changes for Customer and interbank will the special session at 7.00 pm for adverse clearing?

Initially, we shall go ahead with the existing business hours and timings may be revised in consultation with the stakeholders.

150. Proprietary field is expected to capture type of account in case of NRE and what are the expected values?

Please refer to Mapping document, where NRE details mentioned in 7495 is captured.

151. Can we handle credit card transactions?

No. NG-RTGS system will process transactions from one participant to another participant.

152. Can we have outward and inward narration?

Whatever is fed in by sender will be carried through.

153. Whether bank should continue processing on behalf of member banks?

Yes. Sub-membership will be continuing.

154. Which fallback system would be best?
  a) **Primary thick client (SFMS-MI) and secondary thin client (web based).**
  b) **Primary thick client (SFMS-MI) and secondary PO based.**

 a) Yes, but Web API need to integrate with CBS of the Bank.
 b) Yes, PO can act as fallback but with limited no. of transactions say 100 transactions per day.

Both Payment Originator (PO) and API Server reside in NG-RTGS.
The PO client does not provide end-to-end STP capabilities and hence it cannot handle significant volumes of payments efficiently.
On the other hand, the web-service client can offer all this but it has to be provided/developed by the bank.

155. What is the configuration of new SFMS server for NG-RTGS? (Hardware, Software & Operating System)?

The configuration of current SFMS server will suffice. Please refer to presentation slide on pre requisites.

156. Whether existing HSM needs to be deployed on new security applications?

Yes, SFMS server will initially use .pfx files.

157. Volume wise hardware sizing may be published on website?

Please refer to presentation slide on pre requisites.

158. List of fields which are necessarily to be sent from CBS may be published.

Please refer to Message formats and Mapping document.

159. List of options available in NG-RTGS for banks may be published.

List of options will be made available in User manuals/guidelines which will be shared to all Participants/members in NG-RTGS.

160. Throughput and sizing of different banks manages with their server-size available today can be a ready reckoner for server requirements.

Please refer to presentation slide on pre requisites.

161. If there is change in ISO format message, then will there be any change in NG-RTGS format?

Yes.

162. AML - In case if transaction is doubtful what will bank has to do with that transaction?

Banks may follow AML guidelines issued by RBI in this regard.

163. Is there any provision for authorization level like in PI (existing) for liquidity management?

Yes.

164. What are Liquidity management features?

PI refer to the training presentation slides which were demonstrated during workshops for NG-RTGS.

165. In case of Inward processing if some banks are on ISO and other banks are on SFMS series (R41, R42) then how transactions will be received by the bank?

Converter will be required at bank end using R41/R42 series messages for the interim period.

166. Initially R41/42 message as well as R09 and R90 (PI response) is to be provided by convertor. Negative response involved financial reversals.

Only one message camt.054 (debit notification) will be received by the sending participant after the successful settlement in NG-RTGS system and is converted to R43.

167. Payment status report specification.

It is shared during training of members.

168. How will the Return be identified as Related Reference if not present in ISO message?

Related Reference will be provided in Return message.

169. Are there any changes in the party A/c statement required?

No.

170. Presently 2 users are required to create/ authorize message from PI. One more user is required in IDRBT systems and HR issues are involved for addition staffing in operation?

Authorizer of RTGS message will be required if Bank sends unsigned messages and opts for non-STP mode in SFMS-MI. Bank opting for STP mode will have to send signed messages to SFMS-MI to save manpower.

171. Whether Sub-Members concept of existing RTGS system will be continued in NG-RTGS?

Yes.

172. Any return message should have 2020 reference number as part of 2006 Related Reference number field. Needs separate placeholder for the same in pacs.004?

Related reference field / tag will be provided.

173. Placeholder for 2020 field required in ISO 20022 Message formats to identify return payments.

Related reference field/tag will be provided.

174. Using same SFMS setup how the RTGS of bank and sponsored RRB can be handled when our Flexi CUBE and RRB using Finacle and RRB is not ready with the change?

Existing NEFT Branch server will be upgraded with SFMS-MI. Please discuss with IDRBT for further details.

175. Whether we can go for single server or separate servers are better?

It will be Banks' call depending on volume and availability of DR and Near DR set up at bank end for NEFT branch server. Both options will be available in any case.

176. DR Setup & sizing required in new scenario of NEFT & RTGS using SFMS platform.

Please refer to presentation slide on pre requisites.

177. How the IFSC issues being used for RTGS will be populated in SFMS for NG-RTGS?

The present SFMS procedure will be continued.

178. Please elaborate the scenario for single server SFMS and different servers for NEFT & RTGS.

This will be provided in the later patches and its banks' call to implement.

179. Whether different connectivity is required for NEFT & RTGS through SFMS?

No.

180. (Regeneration of message from SFMS server to CBS, when message appear lost.)Though not a feature as discussed, it is required for identification and processing.

As long as the inward message is in intermediary status, we will provide the feature.

181. Whether we require separate server /infrastructure for RTGS/NEFT?

Not required. Present SFMS server with latest patch for NG RTGS will serve for Thick Client in NG-RTGS.

182. Whether performance between Web-API & SFMS-MI will be comparable?

Yes, the performance is comparable; however, the volumes handled by the Web-API are significantly lower.

183. In web service how many threads can bank initiate?

Technically, more than one connection per bank can be used for sending messages to RTGS but in this case the system cannot guarantee the FIFO order for the submitted payments. Also, retrieving messages from the system works best with only one connection as the RTGS system cannot identify the requestors only certain messages.

184. Whether business rule is implemented based on IFSC, account number, currency in message to push the messages in different avenues?

In NG-RTGS, the IFSC information is used to identify the debit/credit parties. The account number is not used for the settlement process in RTGS. However, it could be mandatory for other systems. (e.g. CBS).

185. Server sizing document of SFMS thick client (separate setup) should be shared with bank.

Please refer to presentation slide on pre requisites.

186. In passbook, statement alerts of account which details like UTR no, transaction number should be provided.

Not in the scope of SFMS.

187. 'R' series messages sent without UMAC to SFMS convertor should get routed to RBI for settlement without authorization.

Message should be signed before it is sent to SFMS-MI else it would require authorization at SFMS-MI.

188. TTC default value to value to be shared with banks.

Pl refer to Question No. 33 for List of TTC Codes.

189. Permanently for next 3 months, if testing region is provided or banks to try out and when the test region accepts 'R' series messages and give responses in 'XML' the comfort level of banks would increase. The same can be please be explored.
Demo for the thick client: Clear demonstration of the fields entered in the verification and authorization screens will be required to distinguished data entered and repopulated data.

During Pilot testing, banks will be testing their messages using RBI's test server. Subsequently, after pilot testing gets over, banks will be testing their message using their own testing region.

190. Can bank use server certificate as UMAC for messages?

In PO module class-2 digital signing certificate will be used for signing whereas in case of SFMS-MI and Web-API Class-3 server certificates will be used for signing.

191. Can we issue user signing certificate in name of Bank/department?

No. Only certificates issued by IDRBT Certificate Authority (CA) are accepted by the NG-RTGS/PO systems for signing and login.

192. Can we search message with 16 digits UTR Number in SFMS?

Yes. 16 digits UTR number will be stored in EndToEnd Identification tag for the interim period till bank migrates to ISO 20022 message formats.

In PO, since bank is supposed to be ISO compliant it should use endtoend is tag for entering customer reference no only. Therefore in PO, /XUTR/ should not be pre-fixed at all. However, /XUTR/ is required to be appended in SFMS-MI converter to store the old UTR no in end-to-end id.

193. Need separate incoming queue & CBS receiver process for RTGS messages if NEFT & RTGS running in same server?

Please follow the existing SFMS guidelines. Please get in touch with help desk (ngrtgshelp@idrbt.ac.in).

194. Can we use same Bank API of SFMS for NEFT as well as RTGS messages?

Yes, you can use for NG RTGS.

195. In getMessage() API, can we use query based on last message received ?

The getMessage() call accepts only one parameter (the id of a message). Based on that, NG-RTGS responds with the very next message received by the bank in NG-RTGS. This is the only option available for now.

196. How cut-off can be identified in SFMS at runtime?

SFMS has no cut-off time for the messages.

197. If CBS of Bank is ready to send XML format & other channel are sending in R-series then how such mixing of message format will be handled at SFMS?

NG-RTGS application will exchange ISO 20022 compliant messages with Banks, converter may be deployed by Banks themselves as per their requirements.

198. Will the signature be removed for inward message at SFMS?

No. The ISO message with signature will be given to bank.

199. Whether the field size of 6X35 in existing R-series message of current RTGS System can be continued since NG-RTGS is providing 4X35 only?

It will be 4X35 only.

200. Drop-down for static values while adding transactions should be provided.

Fixed codes are already available.

201. How to view ISO raw messages generated in MI?

Raw message can be seen in display format.

202. Audit trail of messages may be provided.

Yes, it is available.

203. SFMS application should accept outward transactions from multiple channels and send corresponding response to the channel that has been sent outward transaction.

This is based on registered app ID.

204. Request to provide features in SFMS to control outward RTGS transactions. (There are cases where PDC has asked to stop sending outward transactions by banks)

SFMS will not hold back any messages.

205. Instructing agent – For Proprietary field can we have a drop-down?

IFSC Search feature will be provided.

206. Whether RTGS R41/R42 header differs from NEFT formats?

Yes, but in future ISO formats for NEFT and RTGS will be same.

207. Clarification regarding DR setup for Bank.

Please follow you bank's policy.

208. Need to have 22 character transaction identification auto generated through system.

When messages are created simultaneously from CBS and SFMS front end, maintaining uniqueness is difficult.

209. In web browser terminal amount based authorization may be built. e.g. up to 1 crore one creator and authorizer and above 1 crore one creator and two authorizers.

PO module is for small banks only. Such authorization may be implemented by Banks themselves in their CBS system.

210. When the patch for NG-RTGS will be released by IDRBT?

The Patch has been released on IDRBT Site. Please visit the link http://www.idrbt.ac.in/sfmsupdates.html

211. What are the prerequisites for using SFMS thick client?

Please refer to presentation slide on pre requisites.

212. If bank submit R41 to SFMS, then it will be converted into XML. Please let us know what receipt bank will receive (R41 or XML)?

Bank will receive the receipt as per the SFMS-MI conversion parameter set by the receiving Bank.

213. How Digital signing will be handled in case of PO?

Class 2 digitally signed certificates will be issued to PO user which will be stored on the e-token of the user.

214. In case of wrong password entry, user should be described a password format.

The password complexity requirement will be made public by RBI and included in the user manuals.

215. What is the file upload format for pacs.008 and pacs.009 (PO module)?

The format will be the same as for the rest of messages: ISO 20022 with signature.

216. Whether IFSC can be different for instructed agent and creditor agent?

Yes, IFSC can be different for instructed agent and creditor agent.

217. PO inward should be available in a user friendly format such as inputting outward transactions, small banks using web PO would print the inward message and have the accounting entry post at their end, the XML inward will not help without them having an internal module.

The same details visible for the outward messages are going to be available for the inward messages. They can be also printed easily.

218. Two users simultaneously cannot login on same machine to PO module?

No, this is not allowed by design for security reasons.

219. In PO module at the time of manual message creation, field level validation is not present. (e.g. transaction identification)

The validation of transaction id will be switched on after all the specifications are completed. However, the system generates transaction ID automatically if it is left blank.

220. In PO module, RTGS priority code validation is not present. It should not allow entering value between 0-10.

The PO module can be used by RBI users as well. The 0-10 range is reserved for RBI operations. However, Priority range 11-99 is for available for other RTGS participants.

221. In future that if CBS system is signing the transaction then we may fall that messages in RTGS are in pending status due to insufficient funds. There should be an alert for the same.

There could be too many alerts in case large numbers of transactions are put in pending. Participants should periodically login to NG-RTGS and monitor their pending queue.

222. Can the PO be used in case of an emergency on a normal working day?(e.g. currently we can use PI system for input of messages in addition to those we do on CBS.)

Yes. Submission from PO is available at any time. However, if you want to receive the payments in PO, your Participant profile must be first updated by RBI.

223. Whether in PO, message download is limited to one message at a time?

Yes. For more throughputs, please use thick client or web-service client.

224. Local database issues in PO – clarification required.

There is no need for local database when using the PO system.

225. What is the provision for local database handling at bank's level?

There is no requirement to have a local database at the bank's end. The PO runs centrally at RBI and the web-service client is provided by the bank, on any configuration available in the market.

226. PO module is much better as a beginning but practically not better for handling 5000-10000 messages.

The PO was not designed for such large volumes. Banks should revert to thick client or web-service clients for large volumes.

227. Service level proprietary fields can be populated automatically.

Service level field contains the TTC and priority information. For RBI RTGS transactions default priority should be 10 unless it is entered differently. For customer transactions default priority should be 99 unless it is entered differently. In any case, RBI transactions can have priority range from 0-10 and transactions initiated by other members of RTGS will have priorities between 11-99.

228. Whether all response messages received will be converted to R-series messages?

There is no conversion service provided by the PO, nor by API. All messages are delivered in ISO format only.

229. Rejection logs to be displayed in front end.

The rejected transactions/messages can be queried by using the filtering criteria.

230. Whether SFMS will accept current RTGS header for conversion?

Yes.

231. getmessage() in API should be seamless instead of query based mechanism.

 The query-based approach is limited by the underlying technology. It cannot be changed.

232. Current NEFT system uses certificate class III with IFSC can we use same IFSC to route RTGS message or need to register new IFSC for RTGS?

Same IFSC will hold good.

233. Can we have the options of making payments on PO for any emergency payments?

Yes. Only when primary NG-RTGS thick client is down or PO is used as a Primary terminal only by small banks.

234. Do bank need to apply for any certificates afresh for NG-RTGS?

Ans: Users that need access to NG-RTGS and PO systems require new certificates.

235. Reserve account priority range may be fixed (11-99) and default value should not be 99.

The exact priority values will be communicated by RBI. If not used, the field can be left blank.

236. In Case securities are withdrawn from the IDL account, will the change in "available IDL balance" undergo a change? The short is the IDL balance "online" or balance at SOD? Clarify on reverse also.

The funds provided as IDL will be clearly visible in a subaccount of the settlement account. Also, any IDL operations (debits and credits) will be clearly associated with that sub-account.

237. Report on IDL balance utilized & reversed. Also if peak IDL utilization during day and total IDL available on that particular day should be provided in the report.

Ans: IDL reports were specified by RBI and it will be delivered by Montran/TCS.

238. Will there be a message/ pop-up for IDL utilization?

No.

239. Whether alert list will be received by banks?

Yes, list of alerts which will be received by banks have already being shared.

240. Can PO system be used as backup at least in pilot phase?

PO will act as backup but for limited number of RTGS transactions.

241. Download allowed multiple times. Second time a copy should be shown.

Download a message is possible any number of times. Every time, an identical copy of the messages is provided.

242. MI client H/w setup speaks for high volume.

Yes.

243. Will NG-RTGS run on ACK boxes?

NG-RTGS will run centrally, at RBI's mainframe server only.

244. If we continue using gateway what will happen?

SFMS Gateway removal is mandatory to participate in NG RTGS.

245. Can we have multiple polling in web services approach?

Repetitive polling is allowed, but not multiple clients simultaneously connected to the central site.

246. Will the admi.004.001.01 be provided with a BAH? The specification document mentions that a BAH is not required

Admi.004 message will be with BAH.

247. Based on the reason code provided by SFMS branch in the admi.4 notification what are the relevant action required to be considered by the banks?

    (a) F20 – Acknowledgement Message (Banker can flag)
    (b) F25 - Negative Acknowledgement (Banker has to check the status of the transaction through helpdesk)
    (c) F23 - Delivery Notification message (Banker can flag)
    (d) F22 - Non-delivery Warning message (Banker can flag)
    (e) F27- Bank API Response Message (Banker can flag)

248. Please confirm if pacs.2.1.4 payment statue notification will be sent by RBI only for failed payment request notification

Yes. pacs.002.001.04, FIToFIPaymentStatusReportV04 will be sent by RBI only for failed payment request notification. For successful settled payment request,camt.054.001.03 BankToCustomerDebitCreditNotificationV03 will be sent to Instructing agent.

249. On the web API what result code should be treated as PI NAK.

On web API, Return value = "1" – for invalid data (e.g. null argument) and "2" – internal server error (which should be reported).

250. On the web API what action should be taken by the bank for reason code '1'   ?

The participant should check the data and re-send the message using Function Call detailed in
http://rbidocs.rbi.org.in/rdocs/content/pdfs/API%20Web%20Service%20v1.0.pdf.

251. Will RBI keep a control of message id sent to bank on the web service gateway?

All the messages fetched by participant API are generated and maintained at NGRTGS. All outgoing messages will have unique message id generated by the NG-RTGS.

252. What is the SOD method in NGRTGS?

There is SOD operation at Central site only and no SOD operation is required at Participant site for NGRTGS. Messages can be submitted by Participants before SOD as they are kept in the input queues until the system opens for business.

253. What is the type of message used for initiating starting position (SODBAL) in the RTGS settlement account? Will it be a valid camt.54 message? If yes then what will be the identifier for such message?

Once the system opens for business, the Participants will receive automatically a camt.054 notification message when their settlement account has its balance set by RBI. The message will contain the code word "SODBAL" in the Entry Details section (<NtryDtls>) of the message.
The Sequence path would be
Notification **<Ntfctn>**

Entry **\<Ntry\>**
    EntryDetails **\<NtryDtls\>**
        TransactionDetails **\<TxDtls\>**
            Purpose **\<Purp\>**
                Proprietary **\<Prtry\>**

The other codes will be

Codes	Meaning of the Codes
EODZERO	End of day Balance notification (camt.054) received by participants in form of code word "EODZERO" when funds transfer happens from respective NG-RTGS settlement accounts to respective Current Accounts of the banks maintained in RBI CBS System (E-Kuber) as part of NG-RTGS EOD operation by RBI
REPO	REPO notification (camt.054) received by participants when NG-RTGS triggers IDL successfully.
REVREPO	Reverse Repo notification (camt.054) received by participants when IDL taken by the bank gets reversed.
MNSB	Notification (camt.054) on account of MNSB settlement.
C2C	Customer Payment debit notification (camt.054) on account of Customer Payment
B2B	Interbank Payment debit notification (camt.054) on account of Interbank Payment
OAT	Own Account Transfer Payment notification (camt.054) on account of Own Account Transfer
RETURN	Return Payment on account of Return Payment

254. What is the EOD method in NGRTGS?

There is EOD operation at Central site only and no EOD operation is required at Participant site for NG-RTGS.

255. What it the type of message used for sending a final EOD balance sweep transaction? Will it be a valid camt.54 message? If yes then what will be the identifier for such message?

The system will generate a camt.054 to every Participant that had its balance moved from the settlement account to current account which is held in RBI CBS system(E-Kuber). The message will contain the code word "EODZERO" in the Entry Details section of the message.

256. What is the message type used for EOD report?

camt.053 which will be used to convey the end-of-day NG-RTGS statements to the Participants.

257. Will the admi.004.001.01 be provided with a BAH? The specification document mentions that a BAH is not required.

Please see answer to query No. 246.

258. Based on the reason code provided by SFMS branch in the admi.4 notification what are the relevant actions required to be considered by the banks?
    F20 – Acknowledgement Message
    F25 - Negative Acknowledgement
    F23 - Delivery Notification message
    F22 - Non-delivery Warning message
    F27- Bank API Response Message

Please contact ngrtgshelp@idrbt.ac.in for seeking clarification on the query.

259. What is the differentiating factor to identify a fresh camt.54 and response camt.54 (for pacs 8, 9, 4)?

The BAH field Tag ' BusinessService'   <BizSvc> of camt.054.001.03 BanktoCustomerDebitCreditNotificationV03 is always fresh signed message generated from NG-RTGS. Response to pacs.008/009 will be same pacs.008/009 with only change in 'from' and 'to' field in BAH. Appropriate camt.054 messages will be generated and sent by NG-RTGS application to participants. Further, BAH of each message will contain the appropriate information in its field Tag ' BusinessService'   <BizSvc>.

260. How will printing be handled in current case incoming are printed automatically?

Participants can download NGRTGS reports in pdf, excel, csv. Participants should print the same locally.

261. Elaborate on charge bearing field – refer question 36 in FAQ.

It is a mandatory field providing details about the party bearing the transaction charges. Data type is code. It is defined as
DEBT -> charges borne by Debtor

CRED -> charges borne by Creditor
SHAR -> charges are shared
SLEV - > following service level.
As per the current RBI policy the charges are borne by the Debtor.

262. How to retrieve the old messages in PI?

Participants are responsible for maintaining and managing their existing systems including database for retrieval of old messages in PI.

263. What would be archival policy and will the method to retrieve message when needed?

Participants are responsible for maintaining and managing their existing systems including database for retrieval of old messages in PI. The payments will be available for enquiring for 7 days in the NG-RTGS.

264. Will Converter comply to all the attributes of ISO standard messages?

No. Existing R series attributes will be mapped to ISO tags, but many attributes will be blank/masked/appended with default values as the same is/are not available in existing R series format. Also please contact ngrtgshelp@idrbt.ac.in for seeking clarification on the query.

265. In case of problem if two methods are used during a day then what will be the method to check on transactions?

 The database is centralized; hence transactions inputted through different channels update the common database. Transaction status can be enquired via browser.

266**. PO Application - Signature: Unable to approve the messages. Error:'Signature verification failure: No data received'.**

Please update your JRE 32-bit version which will solve the signature problem.

Please refer below link for your reference
http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.html

267. **PO Application Access: Not able to access PO & RTGS URL.**

Obtain the 10 series IP address from the participant, confirmed with CRF and opened the port for the same.

268. **PO Application – Login: Not able to login in PO and when enter User ID and password same login screen appearing(refreshing).**

Certificate Serial numbers in both NGRTGS and PO Users to be manually keyed in and password to be reset to default.

269. **PO Application Login: Not able to access URL for PO & RTGS . Error ' Page cannot be displayed' Telnet was successful.**

Please check with local network team and work on proxy settings.

270. **PO Application Access: User login and credentials needed to login to PO and RTGS.**

 UserName and Certificate Serial No received from bank to be updated in system.

270. **OAT transaction: The transaction failed @ RBI with following error and status as "Failed at RTGS".**

Use proper current account number in OAT.

271. **PO Application Functional: UserName and Certificate Serial No received from bank were updated in system. Appropriate login and password to be used shared.**

Maker can not approve your own transactions. At least one level of approval is required. Hence, log in as a checker and approve.

272. **PO Application Functional: Authorised outward transactions from PO is seen in approve status and same is not getting settled. Also we are getting a below message display 'Object needs to be approved one more time(s).'**

The approval count for the bank was set to 2 levels. Hence, the system was asking for second level of approval.

273. **PO Application Signature: Error message:' Authentication failed!' while approving Customer to Customer transaction.**

Update to Java (jre) 7 plus version.

274: **NG-RTGS Transaction Related: Return message getting rejected. Rejected with reason duplicate reference.**

Check for Incorrect Transaction id used in Return Payment.

275. **NG-RTGS – Login: "Forbidden Error' while accessing NG-RTGS system. User is unable to login in the start of day."**

Please clear the cache, cookies. Restart the terminal/PC and re-inserted the e-token.

276. **NG-RTGS – Transaction Related: Transaction from CBS with Bank's IFSC is getting failed at RBI. Pacs.002 message shows "Failed AT RTGS".**

This was rejected with reason invalid signature.

277. **Software Clarification on IE version: Is IE 8 ok or its is must to use IE 9?**

Need to upgrade to IE 9.

278. **NG-RTGS Transaction Related: No response is being received for messages sent to NG-RTGS**

It was a future dated message.

279. **In PO unable to maintain IFSC code**.

Under Maintenance Participant---> List we can view only maintained IFSC.

280. **NG-RTGS Functional: Unable to see option to deletion /recall functions.**

Unable to see option to deletion /recall functions.

281. PO Functional: Unable to see option to Alert /Event monitoring in PO.
The option to Alert /Event monitoring is not available in PO. However, it is available in NG-RTGS.

282. Outward pacs.008 message has been rejected with reason "/018 INVSIG".

Rejected due to invalid signature.

283. PO – Login: Error Forbidden.

 Please Insert token and retry to Login.

284. PO - Unable to approve the messages. Error: 'Signature verification failure: No data received.'

Please follow the below steps:
   1. Remove the e-token
   2. On IE, Tools -> internet options -> Delete -> temporary files, cookies, Form data, Passwords
       Tools ->internet options -> Content -> Certificates -> Remove all certificates
   3. Re-insert the e-token
   4. Update your JRE 32-bit version which will solve the signature problem.
   Please refer below link for your reference
   http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.html

285. PO – Access: Forbidden error while accessing the PO Module.

Please follow the below steps:
   1. Remove the e-token
   2. On IE, Tools -> internet options -> Delete -> temporary files, cookies, Form data, Passwords
       Tools ->internet options -> Content -> Certificates -> Remove all certificates
   3. Re-insert the e-token.

286. **General Query: Settlement to Invalid Current Account**

For Settlement A/c to invalid Current A/c

(i)Customer to Customer Payment: RBI-CBS will send a pacs002 reject message to NG-RTGS. Further pac.004 has to be initiated from RBI-CBS for Return payment.

(ii) Inter Bank payment: Current Account will be credited based on the IFSCs of the bank. This is because IFSC's are mapped to appropriate Current account numbers at RBI-CBS.

(iii) Own Account Transfer: Current Account will be credited based on the IFSCs of the bank. This is because IFSC's are mapped to appropriate Current account numbers at RBI-CBS. However, the sender institution must make sure the correct Settlement account is used in OAT.

286. How to receiving bank will ensure that RTGS payment is received by him for Customer & Interbank Payment?

In case of Customer & Interbank payment, once settlement happens in RTGS System, the recipient bank will receive full Customer (pacs.008) and Interbank (pacs.009) message respectively with RTGS signature signed by RTGS system.

287**. How to refer and select mode of access in NG-RTGS?**
 Please refer to answers to Query No. 82 & 147. Participants need to fill the Annex-I and forward to NG-RTGS Support Helpdesk email ID   ngrtgssupport@rbi.org.in .

288. **What are the technical requirements to meet access to NG-RTGS?**
Please fill up the format Annex-II.xlsx and forward to NG-RTGS Support Helpdesk ngrtgssupport@rbi.org.in.