Bank of England

RTGS Rules

V2.0 – April 2025

We first published a version of the RTGS Rules in March 2025. In April 2025, we published this version with minor updates for TS3.

The purpose of the RTGS rules is to set out – in plain language – our expectations of RTGS participants (in our capacity as the operator of RTGS and, where applicable, CHAPS) and actions we may take if we have concerns regarding an RTGS participant in line with the RTGS legal documentation.

For CHAPS Direct Participants, in particular, many of the relevant expectations are already covered either in the existing RTGS documentation or the CHAPS Reference Manual. CHAPS Direct Participants continue to be subject to our participant assurance model.

For other RTGS participants, some of the expectations are already contained in existing RTGS documentation but it is not always easy to extract key points. We are not putting in place formal assurance arrangements for non-CHAPS RTGS participants at this time. But this is something we may consider in the future on a proportionate basis, for example, for payment systems settling in RTGS, linked to our February 2024 discussion paper on **Reviewing access to RTGS accounts for settlement**. We may, however, adopt this approach on a reactive basis where we have identified concerns with an RTGS participant.

The RTGS rules should be read alongside our **access policy for RTGS settlement accounts and services**.

Introduction

1. These RTGS Rules (as defined in the RTGS Terms & Conditions) are rules and requirements published, or otherwise made available, by the Bank from time to time relating to the RTGS service.

2. The RTGS Rules set out the eligibility / access criteria for accounts in RTGS and the provision of settlement services, and elaborate on the requirements set out in the RTGS and CHAPS contractual documentation which RTGS users are subject to, namely:

    - requirements for RTGS account holders, including CHAPS Direct Participants, non-bank Payment Service Providers (authorised payments and e-money firms) and omnibus account holders; and

    - requirements for payment system operators who operate a payment system that settles in RTGS.

3. This document also provides more detail – in plain language – on the Bank's expectations and action the Bank may take if it has concerns regarding an RTGS Participant in line with the RTGS legal documentation.

4. In **Annex 1** we have set out a brief explanation of some of the key terms used in this document. For the avoidance of doubt these are provided for guidance only and are not intended to override or modify any existing definitions across the suite of RTGS legal documentation.

Applicability

5. Some of the RTGS Rules apply to all RTGS Participants; others only apply to certain types of RTGS Participants such as organisations who operate a payment system that settles in RTGS.

6. These RTGS Rules should be read together with the other parts of the RTGS and CHAPS legal documentation including:

    - for payment system operators who operate a payment system that settles in RTGS, the Settlement Service Provider Agreement (or in the case of the CREST system, the DvP Services Agreement);

    - for CHAPS Direct Participants, the CHAPS Participation Agreement pursuant to which a CHAPS Direct Participant is bound by the CHAPS Reference Manual;

- for participants in the **Sterling Monetary Framework** (SMF), the Sterling Monetary Framework Terms and Conditions and the Sterling Monetary Framework Operating Procedures; and / or

- for RTGS account holders, a mandate letter pursuant to which the account holder agrees to be bound by the RTGS Terms and Conditions, any relevant annexes to the Terms and Conditions and any Specified Document under the Terms and Conditions.

7. For the avoidance of doubt, in the event of a conflict between any of the documents listed above and the RTGS Rules, each of the documents above will prevail.

Eligibility criteria

8. The key criteria for an institution to be eligible for RTGS services are summarised below. An institution must be able to meet the contractual requirements for the service it is seeking, for example access to an account in RTGS, access to CHAPS or provision of settlement services by the Bank. The Bank may, in its absolute discretion, waive, add to or vary any or all of the criteria in relation to any institution or institutions.

Eligibility criteria for the Bank to act as settlement service provider to a payment system

9. Any payment system operator can apply for the Bank to act as their settlement service provider for settling payment obligations.

10. The risk reduction benefits of the Bank acting as settlement service provider to the payment system and the wider payments landscape (and therefore the financial stability benefits) must (in the Bank's view) outweigh the costs and risks borne by the Bank and the wider system. In considering the benefits, costs and risks attached to an application the Bank will consider the following criteria:

    - The value and volume of transactions of the system.

    - The nature of the transactions processed through the system.

    - The number of directly settling system participants eligible for a Bank settlement account.

Eligibility criteria for RTGS accounts (excluding omnibus accounts)

11. The institutions who may apply to hold an account in RTGS are:

- PRA-authorised/regulated UK incorporated, and UK subsidiaries or branches of non-UK incorporated, banks, building societies and investment firms (designated by the PRA for prudential supervision) that are participants in the SMF;

- Institutions who are part of a wider banking group who already hold an RTGS account (typically a reserves account);

- Central counterparties (CCPs) operating in UK markets which are either authorised or recognised under European Market Infrastructure Regulation (EMIR) in the United Kingdom, and are participants in the SMF;

- International Central Securities Depository (ICSDs) that are participants in the SMF;

- Financial Conduct Authority (FCA) authorised non-bank PSPs that meet amongst other things the requirements set out in the RTGS Terms and Conditions; or

- other financial market infrastructures where the Bank has determined at its discretion there is a credible financial stability case.

12. The decision to grant access to an RTGS account is made at the Bank's discretion. An institution who holds one or more RTGS accounts must have the operational capacity to participate in and efficiently settle transactions in RTGS.

13. Settlement accounts are the accounts typically used to settle an RTGS account holder's obligations in payment systems. Reserves accounts are only provided to SMF participants. Reserve Account holders can then use their reserves account as a settlement account in payment systems. Prefunding accounts are only provided to settlement participants in certain net settlement systems which require participants to pre-fund their settlement obligations in the system.

Omnibus account eligibility criteria

14. Institutions applying to hold an omnibus account must meet the following key requirements:

- the institution must be an operator of a payment system recognised by HM Treasury under the Banking Act 2009;

- the payment system must be designated under **Settlement Finality Regulations (SFR)** once operational;

- the payment system operator holding the account must ensure its participants have a strong legal claim on the underlying funds in the account by holding the funds in the account on trust on behalf of its participants;

- only participants in the SMF are permitted to hold an entitlement in the omnibus account; and

- the sterling balance in the relevant payment system must always be fully (1-1) funded with monies in the omnibus account.

CHAPS Participation

15. Institutions applying for direct access to CHAPS must additionally meet the eligibility criteria and requirements of the **CHAPS Reference Manual (CRM)**.

Assessment of applications

16. When considering an application for any of the RTGS Services set out above, the Bank will balance the benefits of granting access against the costs and risks borne by the Bank and the wider system. Further detail on the risk assessment process is set out in the **access policy for RTGS settlement accounts and services**.

Compliance with eligibility criteria

17. RTGS participants must comply at all times with the eligibility criteria for the RTGS services used, relevant contractual requirements (including these RTGS Rules) and any RTGS operational documents.

18. The RTGS legal documentation imposes obligations on RTGS participants to proactively disclose to the Bank, without undue delay, any material changes which may affect the RTGS participant. This obligation could be triggered for example if the RTGS participant:

- is at risk of not meeting our eligibility criteria, our requirements or rules (including these RTGS Rules) as required;

- is at risk of no longer meeting regulatory requirements – especially those that would mean it was no longer eligible for access to RTGS/CHAPS;

- or its regulator, is considering/has taken any measures, directions or other requirements; or is considering/has made a variation or withdrawal of regulatory permissions or authorisation or, for financial market infrastructures (including operators of payment systems), a variation or withdrawal of

recognition or designation by HM Treasury for regulation by the Bank or the Payment Systems Regulator.

19. The RTGS legal documentation identifies the actions that the Bank may take if an RTGS participant breaches its terms and/or the eligibility or access criteria or if ongoing requirements are no longer met and/or the Bank requires any steps to be taken for the protection of CHAPS, RTGS or the financial system. For example, steps we may take as part of our exercise of our contractual rights include amongst other things:

    - asking you when and how you intend to return to compliance;
    - applying fees and/or administrative charges where applicable;
    - refraining from providing the RTGS participant access to RTGS additional services (including – if applicable – in relation to who you provide settlement services for);
    - restricting account balances and/or transactions across the account (for example, in relation to volume, value, nature of transactions);
    - engaging with the relevant regulator; and
    - if the Bank considers it necessary, varying, suspending or terminating access to RTGS.

Transparency

20. As part of ongoing legal obligations under the RTGS legal documentation to provide information to the Bank, RTGS participants are expected to deal with the Bank, as the operator of RTGS and CHAPS, in an open, honest timely, and co-operative way. This includes disclosing information that is relevant to its use of RTGS, or its participants in the case of payment system operators.

21. RTGS participants should proactively share, without undue delay, information such as:

    - details of any proposed major organisational and business changes including major changes of control or ownership;
    - details of any breach by the RTGS participant of the RTGS legal documentation, including potential resolution, solvent wind-down, and administration events (i.e. going, or gone-concern);

- drafts of any press release or public announcement it plans to make in connection with its use, or access to, RTGS;

- proposals to make any changes to the primarily use, or purpose, of an account, or variations or extensions to services supported by the account or settlement services (such as those set out set out in **Annex 2 for net settlement system operators**). Any such changes must be approved by the Bank, as the operator of RTGS; or

- any other information required under the RTGS legal documentation.

22. RTGS participants should also meet any other requests in a timely manner for new or updated information from the Bank, as the operator of RTGS/CHAPS. This may include updating previously held information or collecting new information that was not previously provided or that the RTGS participant did not possess at the time of request. The information may be used among other things:

    - to support the Bank's assessment of a participant's continued eligibility for RTGS/CHAPS services; or

    - to inform the Bank's ongoing risk assessment of the service provision to the RTGS participant, including in relation to incidents.

23. RTGS participants should – proactively or, if applicable, at the Bank's request – share information without undue delay relating to requests from regulators such as the Bank's FMI Directorate, PRA, FCA and the PSR that may relate to RTGS participation. For example, the FCA's supervisory assessment of authorised payment institutions and authorised e-money institutions holding accounts in RTGS (or seeking to hold accounts) should be proactively shared with the Bank by relevant participants.

24. **Annex 2** sets out transparency provisions which apply to net settlement system operators, whilst **Annex 3** sets out provisions relevant to omnibus account holders.

Confidentiality

25. RTGS participants are subject to confidentiality obligations under the RTGS legal documentation which require them to keep information provided to them about RTGS and/or CHAPS, including in relation to other current and prospective RTGS participants, confidential (other than in limited circumstances) in line with the Bank's classification schema. Many of these documents should only be shared within your organisation on a need-to-know basis, or with trusted suppliers.

26. The Bank's **Information Security Classification Scheme – External users** summarises the handling requirements and applies whether the information was shared electronically, verbally, in paper format or in any other way. The most common classification RTGS participants are likely to see is OFFICIAL – AMBER.

27. The Bank will keep confidential all information about an RTGS participant, including its activities or customers, where that information is by its nature confidential or reasonably determined to be confidential (including where the information is commercially or competitively sensitive). However, this does not prevent disclosure by the Bank in a range of allowable circumstances under the RTGS legal documentation, such as to the extent disclosure is required to fulfil its role as the operator of RTGS or CHAPS or for the purpose of enabling or assisting the Bank to discharge its functions as a monetary authority.

Account management

28. RTGS account holders should seek to maintain an account balance(s) that minimises the risk of disruption because of insufficient funds being available. In particular:

    - for settlement-only account holders, this should take into account requirements around maximum balances. RTGS account holders should engage with the Bank if they believe there is a reasonable case for a higher maximum balance;

    - sufficient funds should be available to meet your settlement obligations as they fall due to avoid disruption to timely settlement or invocation of contingency procedures;

    - for participants in net settlement systems that use prefunding, an appropriate level of prefunding should be maintained to minimise the risk of out-of-hours requests to adjust prefunding levels – as this may require manual intervention by the net settlement system operator and the Bank; and

    - for all fee-payers, you should have sufficient funds for the Bank to collect fees from your RTGS account, where applicable.

29. RTGS account holders should regularly reconcile their accounts and inform the Bank promptly in case of any discrepancy.

Access and contact management

30. Under the RTGS legal documentation, RTGS participants are responsible for keeping contacts, authorised persons lists, and access management permissions to systems in relation to RTGS/CHAPS up to date. In most cases this can be done on a self-service basis through RCEP and Sailpoint by your nominated Principal Users and, where applicable, your Swift Security Officers.

31. RTGS participants should provide nominated senior contacts that the Bank can reach out to for strategic engagement as well as escalation. Contacts required are:

    - for CHAPS Direct Participants, a “CHAPS senior DP rep”;
    - for payment system operators that settle in RTGS, a “FMI senior representative”;
    - for non-CHAPS account holders, an “A/C holder senior representative”.

    Deputies may also be nominated to support cover arrangements.

32. Contact information, where appropriate, should include a) group mailboxes so that RTGS participants don’t miss out on important communications while key contacts are on leave and, where appropriate, b) a group phone number which is monitored 24/7 and/or mobile numbers that the Bank can reach in the event of an incident.

33. RTGS participants must maintain enough active RCEP and BERTI users to avoid a situation where it asks the Bank, as the operator of RTGS, to step in its behalf. Where passwords are issued by the Bank, these should be kept securely by RTGS participants. RTGS participants should also maintain enough Swift Security Officers and any Swift-related tokens should by handled securely.

34. RTGS participants should consider the roles granted to staff for RCEP, external Sailpoint, and BERTI. In particular, if a user has more than one role whether it is an appropriate combination of roles as well as whether sufficient segregation of roles is in place.

35. Organisations should carefully consider the appropriate arrangements for staff access to systems where there are multiple organisations with access to RTGS. Organisations should ensure that they understand the implications of group access, alignment with their internal authorisations, and provide appropriate authorisation to the Bank where Principal Users are permitted to manage individuals for more than one RTGS participant.

36. The Bank may periodically ask RTGS participants to undertake user reviews, including of dormant users.

Engaging with the RTGS and CHAPS services

37. RTGS participants should ensure their staff are familiar with relevant documentation for their roles including obligations, service descriptions, and training materials. This includes:

    - the RTGS Service Description;
    - the key RTGS legal documentation as set out the **Applicability** section; and
    - RTGS operational documentation as referred to in the RTGS legal documentation, including user guides and contingency documentation.

38. RTGS participants should ensure they have the necessary operational procedures in place for using the RTGS and CHAPS services, as applicable.

39. RTGS participants should participate in technical, familiarisation and contingency testing when asked to do so. This is important to reduce operational risks associated with technical changes.

System participant engagement

40. **Annex 2** sets out our expectations on how net settlement system operators should engage with their settlement participants. **Annex 3** summarises some of the key responsibilities of omnibus account holders in their engagement with participants.

Incidents

41. RTGS participants should inform the Bank promptly of any abnormal behaviour detected which it believes may indicate problems with RTGS itself.

42. RTGS participants should inform the Bank in a timely manner of any incidents that could impact RTGS or the stability or efficient operation of the financial system. For example, this might include connectivity issues that mean the Bank may need to manually input transfers on behalf of a net settlement system operator or an RTGS account holder. In particular:

    - for CHAPS Direct Participants, the CHAPS Reference Manual sets out notification timings for CHAPS Direct Participants; and

- payment system operators settling in RTGS should inform the Bank as soon as possible, and at most within 15 minutes of potential disruption to settlement.

43. RTGS participants should, if requested, share information with the Bank in relation to incidents. Information requested after the incident may include the cause of an incident and steps to be taken to reduce recurrence.

44. RTGS participants should be familiar with contingency solutions – including changes to settlement hours – that are applicable for them and have appropriate internal procedures for how they would need to interact with these. An RTGS Participant's procedures should reflect the Bank's preferred order of use where possible. For example, a CLS member should first ask the Bank to enable Party to Party Transfers in BERTI for it to manually input a CLS pay-in if possible, instead of asking the Bank to manually input the CLS pay-in on its behalf.

45. RTGS participants should engage with the Bank on the orderly resumption of transactions following an outage (to the participant, RTGS, or another service provider) in accordance with the RTGS legal documentation.

Changes

46. RTGS participants should raise a case via RCEP as early as practical about potential changes such as to BICs, LEIs, organisational structures, and legal names that may require technical changes in RTGS. This is particularly important for non-standard changes such as those associated with mergers and acquisition activity.

47. RTGS participants should pay attention to updates provided by the Bank to documentation and information about upcoming technical changes, including to messaging schemas.

48. RTGS participants should participate in testing related changes when requested to do so.

Technical access

49. RTGS participants should have in place appropriate technical connections to the RTGS service. For RTGS account holders this includes:

- RTGS extranet and RCEP via Microsoft Azure;

- SWIFT-based access to BERTI via SwiftNet Browse; and

- optional use of APIs.

50. RTGS participants should consider the appropriate level of resilience for connectivity options given the impact and risk from disruption. For some firms this may mean having multiple connections.

Compliance

51. The Bank, as the operator of RTGS, may seek evidence and/or attestations from current and prospective RTGS participants regarding whether they are meeting the obligations set out in this document, and other documentation, in relation to RTGS.

Annex 1: Interpretation

- **CHAPS Direct Participant** is defined in the CHAPS Reference Manual. It is an organisation that meets the criteria for direct access to CHAPS and has been admitted as a CHAPS Direct Participant.

- **Net settlement system** refers to one of the payment systems for whom the Bank acts as settlement agent on a net settlement basis. A list of settlement instructions, which net to zero, are ordinarily submitted via Swift.

- **Net settlement system operator** refers to an organisation that is an operator of a net settlement system. A net settlement system operator enters into a Settlement Service Provider Agreement.

- **Net settlement system participant** refers to an organisation that is a settlement participant in a net settlement system. The organisation signs up to an RTGS mandate letter pursuant to which it becomes bound to the RTGS Terms and Conditions and an Annex to the RTGS Terms & Conditions which is specific to that payment system.

- **Omnibus account holder** is an RTGS account holder that holds an omnibus account in RTGS.

- **Omnibus account scheme participant** is an RTGS account holder that is also a participant in a payment system supported by an omnibus account held by the omnibus account holder.

- **RTGS account holder** is an organisation that holds one or more accounts in RTGS and has entered into the RTGS mandate letter pursuant to which it is bound by RTGS Terms & Conditions and relevant annexes.

- **RTGS participant** is any RTGS account holder or payment system operator that settles in RTGS including net settlement system operators and Euroclear UK and International as the operator of CREST.

- **RTGS services** include (i) the provision of accounts including reserves account, settlement accounts, omnibus accounts and prefunding accounts and (ii) the provision of settlement services including net settlement services and the DvP model used for CREST.

Annex 2: Provisions for net settlement system operators

Transparency/information sharing

Net settlement system operators should share information with the Bank to support amongst other things:

- the Bank in its assessment of the net settlement system operator's continued eligibility for RTGS services, including to inform its ongoing risk assessment of the service provision; and
- the allocation of shared RTGS costs across payment systems (i.e. gross payment values).

Change management

Net settlement system operators should engage with the Bank in a timely manner for any changes to settlement services required. This includes:

- changes to the timing or number of settlements; or
- onboarding or offboarding settlement participants.

Engagement with your settlement participants

Net settlement system operators are responsible for:

- managing your settlement participants, including the risks they (and through you) present to RTGS;
- liaising with settlement participants in the event of incidents disrupting, or concerns with the participant's compliance with requirements, that impact participants' effective participation in the scheme settlement; and
- determining how to split fees allocated to the payment system it operates across its settlement participants. The Bank will collect fees directly from the settlement participants as instructed by the operator.

Annex 3: Provisions for omnibus account holders

Omnibus account payment system participant engagement

Omnibus account holders are responsible for:

- liaising with its participants including in the event of incidents disrupting, or concerns that may impact participants' effective participation in the payment system it operates;
- apportioning and distributing interest received from the Bank or, in the case of negative interest rates, owed to the Bank across its participants according to the same formula as the Bank would have apportioned interest if those funds had been held on the omnibus account payment system participants' reserves accounts over the period; and
- determining how to split and take payment of their allocation of the RTGS costs across its participants.

Transparency/information sharing

Omnibus account holders should provide information in relation to:

- trust claim totals or flows of each omnibus account participant as required by the Bank to support it in compiling reserves information or in its continued risk assessment of provision of RTGS services;
- gross payment flows processed as required by the Bank to support it in determining the allocation of shared RTGS costs across payment systems; and
- proposed onboarding or offboarding of its settlement participants.

Annex 4: Settlement finality

Payment systems and other financial market infrastructures that have been designated under the **Settlement Finality Regulations (SFR)** can benefit from certain statutory protections against normal insolvency law. These protections mean that transfers (payments or securities transfers) which have been sent through the designated system can be treated as final, even if the sending settlement participant has become insolvent.

The RTGS system is not a payment system itself, and it is therefore not eligible to be designated under the SFR. Other statutory or contractual protections may however apply to payments settled in RTGS, as described in the following sections. For example, CHAPS payments, which are settled across accounts in RTGS, rely on the statutory protections conferred on CHAPS.

CHAPS

The CHAPS payment system is designated under the SFR, and once a payment entered into the CHAPS system has reached a defined 'point of irrevocability', it can no longer be voided or reversed, even at the request of an insolvency practitioner. The **CHAPS Reference Manual** defines the points at which a payment is considered to have entered into the system, when it is treated as irrevocable as well as when it is treated as final. The CHAPS Reference Manual therefore transparently marks the point at which payments are protected against normal insolvency law.

Other designated systems settling in RTGS

Some of the other UK payment systems that settle across accounts in RTGS are also designated under the SFR. This includes Bacs; the cheque-based Image Clearing System; CLS; the embedded payment arrangements within CREST and LCH Limited; Faster Payments; the Sterling Fnality Payment System; and Visa Europe. Furthermore, UK central counterparties have also designed their sterling payment arrangements as to be settled through CHAPS and CREST, and such payment arrangements are themselves designated under the SFR: ICE Clear Europe; LCH Limited; LME Clear Limited and SIX x-clear. A list can be found on the Bank's website, at **https://www.bankofengland.co.uk/financial-stability/financial-market-infrastructure-supervision/who-are-we**

As a consequence, where a system is designated, the payment 'transfer orders' executed within that system (and settled across RTGS) benefit from the statutory protections given to that system under the SFR. Where, in the case of a UK central

counterparty, the payment leg of a transaction is settled as a CHAPS payment, it will also benefit from the CHAPS designation. For the avoidance of doubt however, payments made through net settlement payment systems are not settled as CHAPS payments.

Other transfers in RTGS

For non-designated arrangements (LINK, Mastercard, PEXA and settlement of positions from the Notes Circulation Scheme) and internal transfers within RTGS that do not originate from a designated system, statutory protections will not apply and protection is instead at a contractual level, for example, the RTGS Terms & Conditions, these RTGS Rules, and relevant documentation owned by the PSO.

Contractual definitions of settlement finality

Where statutory protections are not available, contractual arrangements may still provide a measure of certainty that payments cannot be unwound by the sending settlement participant after they have reached a certain processing point within a system (although contractual protections will not modify the application of insolvency law). This section sets out what we consider to be the key processing points for transfers in RTGS. Designated systems will have defined their own key processing points for transfers over their systems, which may differ from the RTGS processing points summarised below. In the event of any inconsistency, the definitions provided by the designated system operator will take precedence.

When RTGS is processing normally:

- The transfer **enters RTGS** when it has entered the Swift network and has been acknowledged by Swift or – for manual input into BERTI – when the transfer has been approved and the status changed to pending.
- The transfer **can't be revoked** after the point the settlement status in RTGS changes to 'settling'.
- The transfer is **applied to account balances** when the settlement status in RTGS changes to 'settled'.

The equivalent points are set out below for contingency operation.

Scenario	Enters RTGS	Can't be revoked	Applied to balances
Transfers when MIRS is active (or the transfer has already entered RTGS and can no	As above	The point at which the settlement status in MIRS changes to 'settled'	The point at which the settlement status in MIRS changes to 'settled'

Scenario	Enters RTGS	Can't be revoked	Applied to balances
longer be revoked before MIRS becomes active)			
Transfers that are manually entered into BERTI or MIRS	The point at which the Payment is approved in BERTI or (when MIRS is active) the point at which the payment has been accepted and changes to 'pending' in MIRS	As set out above or, when MIRS is active, the point at which the settlement status in MIRS changes to 'settled'	As set out above or, when MIRS is active, the point at which the settlement status in MIRS changes to 'settled'
Transfers input through a secure spreadsheet-based solution operated by the Bank (designed for use when RTGS and MIRS are otherwise unavailable)	The point at which the operator receives a message that a transfer has been 'submitted'	The point at which the operator receives a message that a transfer has been 'submitted'	The point at which the operator receives a message that a transfer has been 'successfully settled'

Bank of England

Annex 5: Swift RTGS access: code of conduct (STacoc)

Introduction

Sailpoint, BERTI and APIs are all parts of the RTGS service accessed via Swift. This annex sets out the requirements that apply to RTGS participants' use of Swift to connect to RTGS.

This annex should be read alongside relevant documentation provided by:

- the Bank in relation to the RTGS service, including the user guides covering access management and BERTI; and
- Swift including in relation to SwiftNet, and Swift Alliance including Swift WebAccess, Swift Cloud, as well as Swift Customer Security Program and the Swift Customer Security Controls Framework.

CHAPS Direct Participants should also refer the **CHAPS Reference Manual** including section 20 – Swift network connectivity, sections 28 and 29 on security risks and sections 33, 34, and 35 on outsourcing and third party risk management.

In order to access BERTI:

- The RTGS Participant must be part of the relevant Swift Closed User Groups which are managed by the Bank.
- An individual user must be set up in RCEP and BERTI (via external Sailpoint) with one or more BERTI access roles and set up with a 'Distinguished Name' (DN). Access is on a federated basis i.e. Swift credentials managed by a participant's Swift Security Officer.

Participant responsibilities

Each RTGS participant is responsible for managing its relationship with Swift to access Sailpoint, BERTI and API services as well as logical and physical security arrangements. This may include specific hardware – including Hardware Security Modules (box-based and token-based) – and software, network connectivity, user tokens, support packages, and contractual documentation.

RTGS participants are also responsible for managing relationships with relevant third parties such as Swift service bureau and Swift network partners. RTGS participants may use a Swift Service Bureau if:

- Access uses a participants' corporate equipment i.e. not personal devices belonging to staff;
- A Virtual Private Network with strong encryption and two-factor authentication is used; and
- Connection is through locked-down equipment and any remote desktop/virtual connectivity is to a machine that sits securely with the Service Bureau's corporate premises.

RTGS participants must grant the Bank access its Swift Customer Security Programme self-attestation upon request.

Managing individual users

RTGS participants should follow the processes set out in the access management guides provided by the Bank in relation to RTGS.

Ordinarily, a user should only have one account for access to Sailpoint and BERTI. Exceptions to this are a) where a separate profile (and DN) is used for a Sailpoint Principal User and b) users who form part of a group, where a separate account is required for each RTGS participation.

At least one and up to ten DNs may be applied for each user. DNs should be segregated in line with the Swift Customer Security Program and the Swift Customer Security Controls Framework. Test DN should only be used for access to test services, Live DN should only be used for access to test services.

The Bank may periodically ask RTGS participants to undertake user reviews, including of dormant users. RTGS participants should have documented processes in place to complete these.

Resilience and security

Access to Sailpoint, BERTI and API should ordinarily be from corporate premises with:

- Certificates for Swift Alliance Web should be held in a box-based Hardware Security Module; and
- Individual user credentials should not be shared except for the trialling service.

Virtual users may be used for each Swift Alliance Gateway to support resilience.

To support resilience, remote access may be used if Swift Customer Security Program controls are met including:

- Access uses a participants' corporate equipment i.e. not personal devices;

- Strong encryption and two-factor authentication is used;
- Connection is through locked-down equipment and any remote desktop/virtual connectivity is to a machine that sits securely with the Service Bureau's corporate premise; and
- Remote access is not from public spaces e.g. hotel lobbies, train stations.

For CHAPS Direct Participants, resilience should be in place in line with the requirements set out in the CHAPS Reference Manual. It is also beneficial for resilience for different gateways to be used for Swift Interact – for messaging services – and Swift Alliance Web.

Non-CHAPS RTGS participants, should have at equipment at two different physical locations. Access is permitted via Alliance Web Platform, Swift Alliance Lite 2 and/or a Swift Service Bureau. Non-CHAPS RTGS participants may use the same equipment for participants that form part of the same banking group.

Lost or stolen Swift certificates

If a Swift certificate used in connection with access to RTGS is lost or stolen:

- Your Swift Security officer must immediately disable the lost or stolen certificates. In extremis, Swift can do this on your behalf.
- Your Sailpoint Principal Users can remove DN, and roles if deemed necessarily, in Sailpoint.
- You must promptly notify the Bank by calling the RTGS hotline, followed up by raising a case in RCEP.

In extremis, we can edit your users in Sailpoint.

Compliance

For CHAPS Direct Participants, compliance against the requirements set out in this Annex will be covered through the participant assurance arrangement set out in the **CHAPS Reference Manual** including through regulator completion of a compliance certificate.

For other RTGS participants with access to BERTI, the Bank may require completion of a security self-certification questionnaire – including as part of onboarding. The Bank reserves the right to undertake on-site compliance checks as part of this process.