Connectivity - Key Information

Table of contents

1. API - Key Information Page 2

2. HSBC Connect - Key Information Page 4

3. HSBCnet - Key Information Page 6

 HSBC Group © All rights reserved.

API - Key Information

Application Programming Interface (API) means an interface for two systems to communicate. With the power of our APIs, we can accelerate your digital transformation ambitions by connecting financial services directly into your business operations and help you unlock the potential of your business.

1 Key Features

(a) **Transform operations with real-time connectivity:** Our APIs can help you transform your operations by delivering real-time connectivity between the Bank and your business. Achieve enhanced efficiency and timeliness on your transaction banking practices using our broad suite of APIs which include payments, collections, account information, trade and security services and more.

(b) **Digital-first innovation:** Our APIs reflect our digital-first approach; our innovative services are built to embrace a fast-changing future and deliver a full suite of interconnected solutions

(c) **Robust Security:** All our APIs are designed to follow industry-standard security controls to protect your data and support secure connectivity.

(d) **System Integration:** Align with your in-house eco-systems.

(e) **Discovery and Testing:** Explore the latest version of our technical documentation and various developer tools to support your API development on our developer portal (https://develop.hsbc.com - a developer-centric portal that is simple, agile, and future-proof) that empowers clients to achieve faster integration and reduced friction. Users can also test supported APIs in our sandbox environment by completing registration and creating credentials.

(f) **Connected Banking Partnership:** Connected Banking partnerships allow you to access our products and services directly from your existing Enterprise Resource Planning or Treasury Management systems leveraging our corporate APIs, simplifying how you can establish connectivity between our systems and yours as well as improving your day-to-day financial accounting experience.

2 Security

The security and integrity of APIs is crucial. Each API product will have its mandatory security requirements that are aligned with industry requirements and governed by strict internal policies. We follow the security protocols below to help protect API connectivity and data:

(a) **Transport Layer Security ("TLS"):** We protect the connection between your organisation and the Bank by using HTTPS, which encrypts data sent over the internet. When you connect, we provide an SSL/TLS digital certificate. This helps your systems confirm they are talking to the Bank and sets up a secure, encrypted session to keep information private while it's being transmitted.

To avoid connection issues, please check the certificate is valid (not expired) and trusted (issued by a recognised Certificate Authority). Please ensure your organisation's list of trusted Certificate Authorities is kept up to date before attempting connectivity to our APIs service.

(b) **Message Encryption & Signature:** Alongside TLS, we apply Message (Data) Security to protect information exchanged during an API session. Message Level Encryption strengthens protection of API payloads using public-key cryptography (asymmetric encryption).

Asymmetric encryption uses a key pair:

(i) Public key: shared via a trusted certificate and used to encrypt

(ii) Private key: kept confidential and used to decrypt data

Data encrypted with a public key can only be decrypted with the matching private key, supporting encryption, decryption, and digital signature verification. Our APIs use this model. To enable message encryption, you and the Bank must exchange public key certificates, using a separate key pair from the one used for TLS. During onboarding, provide your public key certificate to your Bank contact for setup.

(c) **Key Renewals**

(i) We support public key with a validity period. Automated renewal reminders are issued ahead of expiry to ensure keys are renewed on time and connectivity is maintained.

(ii) Public keys you manage also have a validity period and will need to be renewed before they expire to avoid service disruption.

(d) **Digital Signature** provides you and the Bank assurance of the origin, identity, and status of the message as well as acknowledges informed consent by the signer.

 HSBC Group © All rights reserved.

3 Need More Information?

Explore further details at developer portal (https://develop.hsbc.com). For queries or more information you can contact your Bank representative.

HSBC Connect - Key Information

HSBC Connect is an automated, flexible and secure host-to-host channel that enables direct connectivity between your organisation and the Bank. It supports clients in processing high volumes of payables and receivables and managing financial data at scale through end-to-end integration with Enterprise Resource Planning/Treasury Management System ("**ERP/TMS**") platforms. HSBC Connect is designed to support centralised payment operations, automated reconciliation services, and a high level of straight-through processing.

1 Key Features

(a) **Direct host-to-host connectivity:** A single interface providing end-to-end integration between your ERP/TMS and our payment processing and account reporting systems.

(b) **High-volume processing:** Secure submission of large volumes of payment and collection instructions, with the Bank returning confirmations, reports, statements and other reporting data to your ERP/TMS.

(c) **Global coverage:** One interface supporting connectivity across more than 50 countries in the Americas, Asia-Pacific, Europe and the Middle East.

(d) **Format support and routing:** Supports key industry formats including ISO 20022 XML and local in-country formats. Clients can submit data in a single format and we will validate, sort and route it for processing.

(e) **Operational efficiency:** Reduced operational effort through streamlined processing, less time spent on file-format maintenance, and simplified bank connectivity.

(f) **Fraud risk mitigation:** Increased automation and reduced manual handling can help lower fraud and user error risk.

(g) **Enhanced security:** Supports industry-standard protocols including SFTP, HTTPS/SOAP and AS2. PGP file encryption and digital signature are also supported as an optional enhanced capability.

(h) **Support model:** Regional and global support for Payment Factories, Treasury Centres and Shared Service Centres.

2 Structure

Profile Owner and Account Holders

2.1 Profile Owner

(a) The Profile Owner is the client entity that contracts with us for electronic channels that are established and administered under an HSBC Connect profile.

(b) The Profile Owner may act for itself and/or other legal entities, known as Account Holders, who agree to have their accounts and/or services added to the HSBC Connect profile.

(c) The Profile Owner is authorised to perform a wide range of activities for itself and the Account Holders in relation to accounts and services within scope (for example: viewing information; submitting instructions; creating instructions/arrangements including for payments; requesting certificates/reports; drawing down funds; concluding contracts).

(d) The Profile Owner is solely responsible for ensuring that permissions and limits align with mandates and internal policies/controls. We will not check this.

2.2 Account Holders

(a) An Account Holder is an entity with accounts and/or services accessed through the profile. Access to the HSBC Connect profile is controlled by the Profile Owner.

(b) Accounts/services may be added to the HSBC Connect profile by the Profile Owner and/or the Account Holder.

(c) Account Holders authorise the Profile Owner to act on their behalf through electronic channels the Profile Owner holds with us; actions taken by the Profile Owner are binding on Account Holders.

(d) This authority applies to current and future accounts/services notified to us by either party and covers current and future electronic channels the Profile Owner holds with the relevant Profile Bank, which is the Group member with which the Profile Owner holds the profile.

2.3 Interoperability between HSBC Connect and HSBCnet

The interoperability described below applies where HSBC Connect is configured to route instructions to HSBCnet for review/authorisation and to provide visibility within HSBCnet.

(a) Submission via HSBC Connect; review/authorisation in HSBCnet: Instructions submitted from HSBC Connect can be delivered into HSBCnet for users to review and authorise prior to processing.

 HSBC Group © All rights reserved.

(b) Visibility in HSBCnet: you can have visibility in HSBCnet of instructions submitted through HSBC Connect.

(c) HSBCnet transaction limits apply: where instructions are routed into HSBCnet for approval, HSBCnet transaction limits apply to those instructions.

(d) HSBCnet entitlements apply: HSBCnet user and service entitlements govern what users can view and what actions they can perform for HSBC Connect-submitted instructions that are visible/authorised in HSBCnet.

3 Security

The security and integrity of HSBC Connect connectivity and data exchange are critical. Mandatory security requirements are outlined in the Security Measures, applicable to each HSBC Connect profile provided by us. For more details, refer to the www.hsbcnet.com/online-security/security-measures.

4 Digital Certificate / Encryption Key validity and renewals

Digital certificates and encryption keys help secure both the connection to HSBC Connect and the files exchanged through the service. Digital certificates are primarily used to authenticate a client when establishing a secure connection. Encryption keys (for example, PGP keys) may be used to encrypt files and/or apply a digital signature, strengthening confidentiality and supporting integrity/non-repudiation controls.

To maintain secure connectivity and avoid service disruption, you should note that digital certificates/encryption keys have a validity period and must be renewed before expiry.

(a) We support the use of digital certificates/encryption keys with a defined validity period.

(b) You are responsible for monitoring validity and completing digital certificate/encryption key renewals in time to continue using HSBC Connect.

(c) If digital certificates/encryption keys expire and are not renewed, you will lose access to HSBC Connect, which may prevent you from submitting payments and receiving reports/confirmations/statements via HSBC Connect.

Note: We will provide reminders in advance of the expiry of digital certificates/encryption keys, however you remain responsible for completing renewals before expiry to avoid disruption.

5 Need More Information?

You can contact your Bank representative for queries or more information.

HSBCnet - Key Information

HSBCnet gives you a clear picture of your global banking all in one place, wherever and whenever you want it. We offer a comprehensive suite of flexible online financial solutions – all designed to help you increase productivity and manage your cash flow. With real-time global account access and customisable setup features, you stay in control of the finances at every level of your organisation.

1 Key Features

(a) **User-Friendly Interface:** Access a comprehensive suite of global cash management, trade, supply chain, securities, and global markets solutions through a single, easy-to-use platform.

(b) **Asset Tracking:** Monitor payments, receivables, liquidity, and asset values securely and globally.

(c) **Flexible Reporting:** Utilise adaptable tools to manage cash flow and supply chain requirements.

(d) **Robust Security:** Benefit from multi-level, end-to-end security features.

(e) **Customisable Workspace:** Tailor your workspace to support local languages and time zones.

(f) **Automatic Updates:** Enjoy centralised, automated enhancements without the need for manual software updates.

(g) **Ease of Use:** Navigate intuitively with online learning resources and local language support.

(h) **Mobile and Desktop Access:** Bank conveniently from the office, on the road, or abroad.

(i) **System Integration:** Align with your in-house Treasury Management and Enterprise Resource Planning Systems.

2 Structure

Profile Owner and Account Holders

2.1 Profile Owner

(a) The Profile Owner is the client entity that contracts with HSBC for the HSBCnet services, which are set up and managed under an HSBCnet profile.

(b) The Profile Owner can act for itself and/or other legal entities, known as 'Account Holders,' who agree to have their accounts/ services added to the HSBCnet profile.

(c) The Profile Owner is authorised to carry on a wide range of activities relating to itself and the Account Holders, as well as to any accounts and services held by them. Examples of these activities include: viewing and receiving information; giving instructions; initiating applications; placing orders; creating instructions (including for trade, loans and payments) or arrangements; making changes (e.g. change of address); adding, changing or removing accounts and services; requesting a certificate or report in relation to accounts that may or may not be linked to HSBCnet; and drawing down funds and concluding contracts.

(d) The Profile Owner appoints and sets up the System Administrators and Users and is solely responsible for deciding what access Users have, including allocation of signing authorities and transaction limit rules within the HSBCnet profile.

(e) The Profile Owner is solely responsible for deciding whether the permissions and limits set up in HSBCnet reflect both its and each Account Holder's mandates and internal policies and controls. We will not check this.

2.2 Account Holders

(a) An Account Holder is an entity that has accounts and/or services that are accessed through HSBCnet. The Profile Owner controls access to the HSBCnet profile.

(b) Both the Profile Owner and the Account Holders can add their accounts or services to the Profile Owner's HSBCnet profile.

(c) Account Holders authorise the Profile Owner to view their information and to take a wide range of actions on their behalf through the electronic channels (including HSBCnet) that the Profile Owner has with us. Any actions taken by the Profile Owner are binding on Account Holders.

(d) When an Account Holder authorises a Profile Owner to act on its behalf through its electronic channels, this authority applies to all current and future accounts and services we are notified of by either party. It also covers all current and future electronic channels the Profile Owner holds with the relevant Profile Bank, which is the Group member with which the Profile Owner holds the profile.

3 Roles

3.1 System Administrators and Users

(a) The System Administrator has a key role, and the Profile Owner should carefully consider which individuals are to perform this role.

 HSBC Group © All rights reserved.

(b) The Profile Owner nominates the initial System Administrators, who are the first System Administrators that will be set up on the HSBCnet profile by us.

(c) System Administrators:

(i) can delegate authority to other System Administrators and Users, who may then sub-delegate that authority; and

(ii) have administration rights and can set up, suspend and remove Users and System Administrators, and manage their permissions.

(d) Depending on their permissions, System Administrators and Users can send instructions and carry out the activities explained above in the "Profile Owners" section.

(e) System Administrators and Users may agree online terms and conditions, including potentially before they can access accounts and services on HSBCnet. Additional terms may also apply for certain accounts or services on the HSBCnet profile.

4 Additional Considerations

(a) **Sole and Dual Controls:** Some access rights and permissions have the option of being set up on a sole or dual basis. To keep you better protected, we recommend you choosing dual control (sometimes known as 'maker/checker'). If you choose to take a control on a sole, rather than dual, basis, this means System Administrators and Users will be able to act on their own without reference to another user. Sole control will make it harder for you to manage activity on HSBCnet and could increase your risk of fraud or user error. We may add extra controls to help reduce this risk – we'll let you know in advance if we do this.

(b) **Administrative Controls:** You must advise the level of administrative controls that are to apply to the HSBCnet profile. There are two options available:

(i) **Dual Management Control:** requires at least two System Administrators to make and complete any administrative function on HSBCnet. When one System Administrator makes any administrative change, at least one additional System Administrator must approve the request, depending on your System Administrator setup. This is our recommended control.

(ii) **Sole Authorisation Control:** a single System Administrator can act and make changes in User and account management, with all System Administrator functions processed immediately.

(c) **Authentication:** When creating a payment, you may be required to authenticate the payment using your security device. This can be a physical security device (hard token) or mobile app (soft token).

(d) **Transaction Limits:** This feature can be set for payment services. Users can manage transactions up to these limits. Transaction limits can be viewed and decreased on HSBCnet. Increasing transaction limits may require additional documentation.

(e) **Auto-account registration:** If auto-account registration is enabled, any eligible accounts you or the Account Holder have now or open in the future will be linked to your HSBCnet profile. You are responsible for ensuring you are authorised to access any account linked in this way, and fees may apply.

(f) **Auto-entitlement:** Where it is available, this allows an Account Holder to authorise the Profile Bank to automatically add all present and future eligible accounts in their name to the Profile Owner's HSBCnet profile. Additional fees and/or tariffs may apply to the Profile Owner if this service is selected.

5 Security

The security and integrity of HSBCnet is crucial. Mandatory security requirements are outlined in the Security Measures, applicable to each HSBCnet profile provided by us. For more details, refer to www.hsbcnet.com/online-security/security-measures.

6 Need More Information?

Explore further details at www.hsbcnet.com/, including User Guides, Customer Support, and Product Information. Virtual assistance is available for queries, or you can contact your Bank representative for more information.

 HSBC Group © All rights reserved.