www.danskebank.co.uk

Public Key Infrastructure (PKI) Hardware Security Module (HSM) Terms and Conditions

Effective from 25 May 2018

Danske Bank

1 Introduction

These Terms and Conditions constitute the terms and conditions between You and the Bank for the provision of the Services (the "PKI Hardware Security Module (HSM) Terms and Conditions"). These PKI HSM Terms and Conditions supplement the Bank's General Terms and Conditions – Business Accounts (the "General Terms") and any defined terms in these PKI HSM Terms and Conditions will have the same meaning given in the General Terms unless stated otherwise. In the case of any conflict between the conditions set out in the General Terms and those in the PKI HSM Terms and Conditions, then the terms of these PKI HSM Terms and Conditions shall prevail in relation to Your use of the Service only.

2 Interpretation

2.1 In these PKI HSM Terms and Conditions:

"**Authorised Signatory**" means an agent, contractor or employee of the Customer, (and "Authorised Signatories" shall be construed accordingly) notified to the Bank in accordance with the Bank's procedures (as such are in place from time to time) in relation to the identification of those individuals permitted, under the mandate applicable to a particular account or product offered by the Bank, to authorise transactions to be carried out by or with the Bank;

"**Bank**" means Northern Bank Limited having its registered office address at Donegall Square West, Belfast (registered number R568), and includes the Bank's successors, assignees and transferees whomsoever. Danske Bank is a trading name of Northern Bank Limited. Northern Bank Limited is a member of the Danske Bank Group;

"**Business Day**" means a Monday, Tuesday, Wednesday, Thursday and Friday (excluding English Bank holidays) when the Bacs system is fully open and operational to provide services of the kind contemplated in these PKI HSM Terms and Conditions. Entries will only be debited or credited to Your settlement account on days when the Bank is open for Business;

"**Certificate**" means an electronic attestation, which is an X.509 v.3 compliant digitally signed data structure, and which immutably binds a Public Key to information uniquely identifying the possessor of the Private Key corresponding to such Public Key, including those issued to You in accordance with Your Agreement;

"**Certification Authority**" means the entity responsible for the certification of Public Keys, the issuance of Certificates, and the maintenance of Certificate status information;

"**Certificate Holder**" means an individual, whether an employee, agent or officer of the Customer, issued with a Certificate to be held on an HSM;

"**Certificate Policy**" means either of the Identity or Utility Certificate Policies issued by the Bank (which are incorporated into Your Agreement and are available to You on request, in accordance with clause 27) and which set out the policy constraints on the use of Certificates within that Certification Authority's public key infrastructure service;

"**Certificate Practice Statement**" or "CPS" means a document that describes the practices to be performed by a Certification Authority to implement certain policy requirements stated in its operating policies and other documents;

"**Confidential Information**" means, without limitation, all information (whether written or oral) concerning business, financial or technical information or activities of, or relating in any way to, the Customer, the Bank (including its Group Companies), IdenTrust or the Service and any other information that is marked as being, or otherwise indicated to be, confidential at or prior to the time of disclosure, or that might reasonably be considered to be confidential;

"**Customer**" means the entity which is named as such in the application form for the Service;

"**Digital Signature**" means the data appended to, or a cryptographic transformation of, data contained within a Digital Transmission to authenticate the source and integrity of the data and to preclude repudiation by the signer, and which is the unique digital identification of an entity that is created by the entity applying its Private Key to a Digital Transmission for the purpose of confirming the identity of that entity, and its association with the Digital Transmission to the recipient of the Digital Transmission, employing a Private Key, a corresponding Public Key, and a mathematical function known as a "message digest function," such that a person receiving or otherwise accessing the Digital Transmission, and the signer's Public Key, can assess:

(a) whether the transformation of the Digital Transmission into the message digest function was achieved using the Private Key that corresponds to the signer's Public Key; and

(b) whether the Digital Transmission has been altered since the transformation was made;

"**Digital Transmission**" means an instruction, message, file or other communication which is transmitted in electronic form, using the Service, and which is signed with a Digital Signature and which includes a Certificate;

"**General Terms**" means the Bank's General Terms and Conditions – Business Accounts as amended from time to time;

"**Group Companies**" means, in relation to a party to which the Bacstel-IP Services Customer Terms and Conditions apply, that company or other body corporate and all of its associates, subsidiary companies and holding companies and all other associates, subsidiary companies of any such holding company, for the time being within the meaning of the Companies Act 2006 (as amended from time to time);

"**Hardware**" means any physical hardware supplied by or on behalf of the Bank or its agent from time to time, in accordance with clause 19;

"**HSM**" means Hardware Security Module. HSM's allow service users to make submissions and access reports using an automated system where a person does not have to enter the PIN associated with the PKI credentials each time a submission is made or a report request is performed. The HSM holds the PKI credentials instead of them being held on a smartcard.

"**Identity Certificate**" means a Certificate issued by a Certification Authority to a Customer that can be used by the Customer in connection with digital identification and signature services;

"**IdenTrust**" means IdenTrust, Inc, a corporation established in the state of Delaware, USA, operating digital integrity or identity validation services (the "IdenTrust Service");

"**IdenTrust Marks**" means certain logos, designs, trademarks, service marks, names and symbols relating to the IdenTrust Service, or to IdenTrust itself, including without limitation the IdenTrust Global ID mark used on Certificates;

"**IdenTrust Participant**" means an entity that has entered into an agreement with IdenTrust for the provision of the IdenTrust Service, or an entity that offers the IdenTrust Service;

"**Insolvency Event**" means in relation to You (or for the purposes of an insolvency event, in relation to any of Your Group Companies, any of which will also be included in "You"), any of the following:

(a) that You are unable or admit You are unable to pay Your debts as they fall due within the meaning of Article 103 of the Insolvency (Northern Ireland) Order 1989 (the "Order") (other than by reason of the service of a written demand pursuant to Article 103(1)(a) of the Order where You contest such demand in good faith);

(b) an order is made by a court of competent jurisdiction, or a resolution is passed, for Your winding up;

(c) the presentation of a petition for Your winding up where such petition is not restrained from being advertised or is not dismissed within 28 days of its presentation;

(d) any individual comprising the Customer has a petition for a bankruptcy order presented against him;

(e) a seizure order, order appointing a receiver, attachment, sequestration, execution or other legal process is levied or enforced against all or a material part of Your property or assets and is not fully paid or discharged within 28 days unless and for so long as the same is being contested in good faith;

(f) any legal proceedings or other procedure or step is taken in relation to:

(i) a moratorium of any indebtedness, winding-up, dissolution, administration or reorganisation (by way of voluntary arrangement, scheme of arrangement or otherwise), other than a solvent liquidation or reorganisation; or

(ii) a composition, assignment or arrangement with any of Your creditors; or

(iii) a liquidator is appointed (other than in respect of a solvent

liquidation of Your business or undertaking), or a provisional liquidator, receiver, administrator, administrative receiver, compulsory manager or other similar officer is appointed in respect of or over all or a material part of Your undertaking or assets; or

(g) If any event analogous to (a) to (f) of this definition shall occur in any other jurisdiction to which You are subject;

"**KSM**" means Key Storage Mechanism and is the device that stores the Public and Private Keys associated with an HSM

"**OCSP** Responder" means an On-Line Certificate Status Protocol Responder operated by the Bank, an application used to obtain Certificate related information from a repository, or another on-line Certificate status protocol responder, used to verify Certificate status requests;

"**Personnel**" means the agents, contractors and employees of the Customer, or those of the Bank, as the context requires and will include Certificate Holders;

"**Private Key**" means the key within any asymmetric key pair generated by a public key infrastructure service for a person which is normally known only by that person, and which is one-half of a cryptographic key pair as drawn from the class of asymmetric key cryptographic functions used in the public key infrastructure service that an individual or entity (or, under these PKI HSM Terms and Conditions, a Certificate Holder) may apply to electronic transmissions, messages or records for identification and communication purposes, including to generate a Digital Signature to be placed on a Digital Transmission;

"**Public Key**" means the key of an entity's asymmetric key pair that can be made public. A Public Key is one-half of a cryptographic key pair as drawn from the class of asymmetric key cryptographic functions used in a public key infrastructure service that is uniquely related to the Private Key of an individual or entity issued with a Certificate (or in these PKI HSM Terms and Conditions, a Certificate Holder);

"**Root Certificate Authority**" means IdenTrust or any other root Certificate authority used by the Bank from time to time;

"Service" means the IdenTrust compliant public key infrastructure service offered to You by the Bank for use in conjunction with Your account(s) or other facilities or products offered with or by the Bank, including the provision of Certificates issued to You or Your Certificate Holders;

"**Utility Certificate**" means a Certificate issued by an IdenTrust Participant to a Customer that can be used by a Customer to facilitate the confidentiality and integrity of Digital Transmissions, which shall be in the format specified by IdenTrust;

"**You**" and "**Yours**" refers to the Customer set out in the application form who apply to use the Service, and where more than one person comprises the Customer, "You" means all of them jointly and each of them severally, and shall include Your successors, assigns, and Personnel and, in relation to Your rights to use the Service, any other authorised user;

"**Your Agreement**" means the agreement (comprising the signed application form) to which these PKI HSM Terms and Conditions apply.

2.2 References to clauses and schedules are references to the clauses and schedules of these PKI HSM Terms and Conditions.

2.3 References to one gender include all genders and references to the singular shall include the plural and vice versa.

2.4 If there is any conflict between the terms of the main body of these PKI HSM Terms and Conditions and those contained in any Schedule or document referred to or any other terms and conditions of the Bank which apply to Your account(s) for which You will use the Service, to the extent of that conflict, the documents shall have the following order of precedence, except as otherwise provided in the Bank's other terms and conditions:

(a) these PKI HSM Terms and Conditions;
(b) the Schedules to these PKI HSM Terms and Conditions;
(c) the CPS or any Certificate Policy;
(d) the Bank's other terms and conditions.

3. Certificates

3.1 The Bank is responsible for the provision of the Service to You, but You acknowledge that the Bank may use another party to issue Certificates to You on behalf of the Bank, and perform the Bank's Certification Authority and registration authority functions. Unless the context otherwise requires references to the Bank also include a reference to any such other party.

3.2 The Bank may issue, or procure the issue of, Certificates to You as part of the Service, provided that You;

(a) are a non-consumer entity such as a company, corporation, limited liability company, association, government agency, partnership, limited liability partnership or sole trader; and
(b) have successfully met the Bank's "Know Your Customer" requirements; and
(c) have agreed to these PKI HSM Terms and Conditions.

4. The Service

4.1 You may use the Service;

(a) to encrypt and/or digitally sign a message, transaction or other electronic file; or
(b) when requesting confirmation of the status of a Certificate included in a Digital Transmission received by You as a valid Certificate.

4.2 You agree that any use of Certificates issued to You in connection with the Service will be subject to the following limitations:

(a) Certificates must not be used for the purposes of creating further Certificates.
(b) You may not use Certificates in breach of any of the obligations or restrictions imposed under these PKI HSM Terms and Conditions.
(c) You may not use Public or Private Keys, their storage mechanism, Certificates or the Service in relation to any transaction where You are not acting as principal, or agent for a principal disclosed to the Bank or for, or in connection with, any unlawful purpose.
(d) You may only use Certificates in conjunction with IdenTrust enabled applications or the IdenTrust Service.
(e) Certificate use must be consistent with the Certificate Policy associated with the particular Certificate being used, and must not be in breach of any of the obligations or restrictions established or imposed under the applicable Certificate Policy.
(f) You may not rely on the validity of a Certificate sent to You as part of a Digital Transmission, unless You have authenticated that Certificate by:
(i) confirming the validity of each intervening Certificate between that being sent to You and that issued by the Root Certificate Authority (and including confirming the validity of the Certificate issued by the Root Certificate Authority) for each Certificate so associated with a Digital Transmission, and confirming that the Certificate has not expired; and
(ii) undertaking a SHA-1 integrity check on any such Digital Transmission and each part thereof, against the Digital Signature applied to such Digital Transmission (or each part of it); and
(iii) submitting a validation request to the Certificate issuer in relation to the relevant Certificate and receiving confirmation of validation.
(g) You may not use Certificates in any circumstances or in any application that could lead directly to death, personal injury or damage to property, and the Bank shall not be liable for any claims arising from such use.

4.3 The Bank may from time to time notify You of the days or portions of days on which the Service may not be available.

5. Authentication of Identity

5.1 Prior to Certificates being issued to You, or to Your Certificate Holders on Your behalf, the Bank shall confirm Your identity in accordance with:

(a) "Know Your Customer" requirements specified by the Bank;
(b) these PKI HSM Terms and Conditions or the CPS, which is incorporated into Your Agreement available to You on request in accordance with clause 27; and
(c) any procedures mandated by the requirements of the banking licence regulator either for the Bank or the Certification Authority, whichever is the stricter from time to time.

5.2 The Bank may confirm the identity of Your Certificate Holders in accordance with the requirements set out in clause 5.1(a) to (c), but shall unless otherwise notified to You, follow the procedure set out in clause5.3.

5.3 You shall confirm the identity of Your potential Certificate Holders and their authority to act, and one of Your Authorised Signatories

shall notify the Bank of the identity of any potential Certificate Holder, and confirm their authority to act.

5.4 The Bank may rely upon any Digital Transmission issued in accordance with these PKI HSM Terms and Conditions by any Certificate Holder (where that Certificate Holder has been issued with a Certificate following a request to the Bank in accordance with clause 27) whose status as such has not been revoked by the Customer in accordance with clause 8.7(c)

6. Responsibility for Digital Transmissions

6.1 Subject to clause 6.2, and the detailed provisions relating to liability in the General Terms, provided that Your Certificates have not expired, or been suspended or revoked, You will be responsible for all transactions resulting from Digital Transmissions authenticated with a Digital Signature created with Your Private Key, and/or for which the Identity Certificate is confirmed as a valid Certificate through the Service.

6.2 Subject to the provisions relating to unauthorised transactions set out in the General Terms,where You have notified the Bank in accordance with clause 10.3 that the security of Your system has been compromised You will, for sixty (60) minutes from the time at which the Bank acknowledges Your notification by fax, or until the Bank has confirmed by fax that Your Certificates have been suspended or revoked, whichever is the sooner, remain responsible for all Digital Transmissions signed with Your Certificates.

6.3 Where You have confirmed to the Bank in accordance with clause 5 that an individual is authorised to act as a Certificate Holder, and provided (subject to clause 6.2) that Your Certificates have not expired, or been suspended or revoked, You will be responsible for all transactions resulting from Digital Transmissions, and You agree that each act or omission of any Certificate Holder (with respect to the relevant Certificate) shall for the purposes of these PKI HSM Terms and Conditions (and as applicable for the purposes of the rules applicable to the IdenTrust Service) be deemed to be Your act or omission.

7. Security

7.1 You are solely responsible for establishing and applying adequate security systems, controls and procedures in compliance with the certificate policy.

7.2 Device shipment and receipt.
Procedures should be detailed to ensure the integrity of the cryptographic device throughout the transport of the device from the manufacturer. Procedures include:
- Shipment through registered mail, or use of tamper evident packaging
- Inspection of tamper evident packaging
- Testing and verification of firmware setting

7.3 Device storage.
Procedures should ensure secure storage of HSMs with appropriate access controls. Procedures include:
- Inventory control
- Event logging
- Link to incident response procedures
- Audit procedures

7.4 Device handling.
Procedures should detail how HSMs are to be handled. Procedures include:
- Presence of two trusted employees
- Device installation procedures
- Device removal procedures
- Device repair and acceptance testing procedures
- Device repair location
- Device disposal procedures

7.5 Device Usage and retirement
Procedures should detail how HSM's are to be maintained and retired. Procedures include:
- Testing of devices and interfaces prior to usage
- Verification of correct processing on a periodic basis
- Diagnostic support procedures
- Procedures to erase keys prior to disposal
- Procedures for destroying casing/ module

7.6 The HSM must:
- Comply with the HSM specifications as set out in the IdenTrust HSM Compliance Requirements [IT-HSMCR];
- Export the Keys securely (if required); and Destroy the Keys if they have been loaded into a Key Storage Mechanism

7.7 If You obtain access to any information, including Confidential Information, that clearly does not concern You, You must:
(a) treat any such material as Confidential Information in accordance with clause 24; and
(b) notify the Bank immediately.

7.8 The customer shall be responsible for establishing and applying adequate security systems, controls and procedures in relation to
(a) The customers Private Keys and HSMs to prevent their loss, disclosure to any other party, modification or unauthorised use ; and
(b) Monitoring usage of the Trust Service by the customers personnel including without limitation, use of Digital Certificates and all outgoing BACSTEL –IP Transmissions

7.9 If the customer suspects, believes or becomes aware that a third party knows or has compromised the safekeeping of any of the Suppliers Private Keys or has compromised the security of any HSM on which such Private Key is stored, the customer shall notify the relevant member promptly.

7.10 The customer may, subject to the provisions of paragraph's 7.13 & 7.14 install the Private Keys, Public Keys and Digital Certificates issued to it by more than one member on a single HSM provided that each set of a Public Key, a Private Key and their associated Digital Certificate relating to a Trust Service is kept Logically separated from each other

7.11 The customer shall use the Trust Service and it's Private Keys, HSM's and Digital Certificates in accordance with the BACSTEL – IP Rules, the Trust Service Terms and Conditions and (where applicable) the IdenTrust Addendum and such technical user guides or manuals or other reasonable instructions as may be provided to the customer by the member from time to time

7.12 The customer will be responsible at all times for the generation of the Private Keys and Public Keys used by it in connection with a Trust Service and for the installation and management of such private keys and Public Keys (and Digital certificates associated with such Private Keys and Public Keys) on the relevant HSM.

7.13 The customer shall generate a separate Public Key and Private Key pair afresh for each Digital Certificate to be issued to it under the Members Trust Service and shall not:
(a) Submit a Public Key for certification to more than one entity or to the same entity more than once or
(b) Use the Public Key for any purpose other than in connection with the Member's Trust Service and BACSTEL-IP

7.14 The Customer shall keep each HSM or other storage mechanism for operational Private Keys and Public Keys relating to the customers activities in connection with Bacstel-IP physically (as opposed to logically) separate from that for any Public Keys and Private Keys used for any other purposes (including test, development and demonstration purposes)

8. Operational Requirements

8.1 Certificate application
Application forms for the issue of a Certificate must be completed and submitted for approval by the Bank before any Certificate may be issued. An application for a Certificate will only be processed if the Customer has previously signed and agreed to these PKI HSM Terms and Conditions.

8.2 Certificate issue
The process for Certificate issue is as follows:
(a) The Bank will authenticate the identity of the applicant in accordance with clause 5. The Bank will also ensure that the HSM is IdenTrust Compatible
(b) The customer will provide the Bank with a PKCS #10 Public Key Signature Request, which is needed to generate the PKCS #7 Signed Public Key Certificate. This request can be received in the form of a PGP encrypted e-mail or by a disc that was contained in a tamper proof envelope.

(c) The Bank will or will procure that its Certification Authority will generate and issue a Certificate for the applicant in accordance with these PKI HSM Terms and Conditions, and in accordance with the rules applicable to the IdenTrust Service.

(d) The Live certificate will be delivered to the customer in person by a member of the Bank; The Certificate will be saved on a disc or can be requested by the the Bank employee by PGP encrypted mail, whilst on site. The the Bank employee will also be on site when the certificate is loaded to the HSM or KSM.

(e) You or Your Certificate Holder must acknowledge receipt of any Certificate, and (in accordance with clause 8.4(c) check the accuracy of the information in conjunction with that Certificate on the day of its receipt (and in any event prior to its use).

8.3 Certificate Activation

(a) Keys to be Certified by the Bank

To procedurally ensure all IdenTrust Keys have been generated in approved hardware, Participants requiring Key Certification by the Bank must ensure:

- HSM Key generation is in the presence of at least two persons of the organization;
- One of these two persons is at least of Senior Management Level; and
- Details of the persons witnessing generation are communicated to the Bank when request verification is conducted.

(b) Random Number Generation

Key generation must use a random number generator (RNG) or pseudo random number generator (PRNG) meeting the specification of Annex C ANSI X9.82 or equivalent. By equivalent, it is meant that another international standard may be acceptable. The Bank will determine acceptability of any standard other than the above

(c) Activating Your Private Key

Your Private Key must only be activated where:

- You have been issued a Key Storage Mechanism (KSM) with a Key Pair or an HSM, using which you generate a Key Pair;
- You have acknowledged receipt of the Private Key
- A Customer Agreement between that Customer and its Issuing Participant has been executed.

(d) Key generation

- The HSM must export the Keys securely (If required) and destroy the Keys if they have been loaded into a Key Storage Mechanisom.
- HSMs must meet the technical requirements specified by IdenTrust from time to time (including the requirement that they must be FIPS 140-2 Level 2 or FIPS 140-2 Level 3 provided that the RSA key length selected is a minimum of 2048 bit). These requirements are available on request.

(e) Private keys must not exist in plain text outside of the designated FIPS level of crytopgraphic Module. Where there is a requirement for a private key to exist outside of a HSM then that key must be protected using 2-key triple DES (or equivalent) or a key-splitting method must be deployed such that the key is split into key shares to mitigate the risk of disclosure to a third party, or capture of that information by a third party.

(f) The HSM must:

(i) Create signatures using SHA-1 and RSA with 160-bit HASH Keys (as described in PKCS #1, v2.0)

(ii) Use signature scheme RSASSA-PKCS-v1_5

(g). The KSM must be able to generate RSA-based digital signatures using 2048 bit Keys based on the following signature scheme and method:

(h). PKCS#11

The KSM MUST provide a PKCS#11 interface to the certificate(s) and key material.

(i). Microsoft Cryptographic API

If the KSM is used on a Microsoft operating system then the KSM MUST provide support for accessing the certificate(s) and keys using the Microsoft Cryptographic API (CAPI).

8.4 Certificate acceptance

(a) You acknowledge that Your first use, or that of any Certificate Holder, of the Service, or of any Certificate, shall be deemed to be an acceptance of the Certificate, and of the terms of the Bank's CPS, Identity Certificate Policy, Utility Certificate Policy (each of which is incorporated into Your Agreement and available on request in accordance with clause 27) and these PKI HSM Terms and Conditions.

(b) You acknowledge that your first use, or that of any Certificate Holder, of any Private Key shall be deemed to be an acceptance of the related Certificates, and of the terms of the Bank's CPS, Identify Certificate Policy, Utility Certificate Policy and these PKI HSM Terms and Conditions.

(c) Your Certificate Holder(s) will check the accuracy of all information issued in conjunction with a Certificate, prior to any use of that Certificate, and first use of any such Certificate shall be deemed to be confirmation that such information is accurate.

8.5 Certificate Security

Private Keys held in a HSM must be subject to access controls to ensure that personnel without appropriate authority cannot access the HSM and It's contents.

If an HSM stores its secret key external to the Card/Module the following Minimum Security Requirements should be implemented:

- The Key should be stored in an encrypted file protected by at least 168 Bit 3DES or 192 Bit AES encryption.
- The directory where the Secret Key is located should not be shared for public access.
- The Key should only be decrypted within the HSM itself.
- The HSM should be configured on initial setup to require as a minimum 2 person present for startup/recovery purposes.

Electronically distributed secret and private keys must be entered and output in at least 168 Bit 3DES or 192 Bit AES -encrypted format

8.6 Certificate expiry

A Certificate will expire in accordance with the terms on which it is issued.

8.7 Certificate revocation and suspension

(a) The Bank shall act on any notice given in accordance with clause 27 to revoke or suspend a Certificate held by You or Your Certificate Holder, within no more than 60 minutes of any confirmation that the Bank has received notice requesting such revocation or suspension, in accordance with clause 6.2. Pending the revocation or suspension of any Certificate, the provisions of clause 6.2 shall apply.

(b) The Bank shall act on any notice to revoke the status of an Authorised Signatory or Certificate Holder, in accordance with clause 27.

(c) The Bank shall act to revoke or suspend a Certificate in accordance with the terms of this clause 8.7.

(d) A Certificate shall be revoked where the Bank or its Certification Authority is advised of or becomes aware of any of the following circumstances:

(i) You no longer have exclusive control of the Private Key, due to circumstances including but not limited to, a loss, theft, modification, unauthorised disclosure or other compromise of the Private Key of any Certificate Holder.

(ii) Material information contained in the Certificate is no longer valid.

(iii) You or a Certificate Holder have breached a material obligation under the applicable Certificate Policy or these PKI HSM Terms and Conditions.

(iv) The performance of Your or a Certificate Holder's obligations under these PKI HSM Terms and Conditions or under the CPS has been delayed or prevented by an act of God, natural disaster, computer or communications failure, change in statute, regulation, or other law; official government action, including but not limited to acts by agencies responsible for export control administration, or other cause beyond Your reasonable control, and the

Certificate has been or may be materially threatened or compromised.
(v) The Bank, or the Certification Authority, deems that the revocation of the Certificate is necessary or appropriate to maintain the integrity of the Service.
(vi) The Bank, or the Certification Authority, is requested to revoke a Certificate by a valid legal authority, or by the Root Certificate Authority.
(vii) IdenTrust has determined that there is an immediate and material threat to the safe and sound operation of the IdenTrust Service.
(viii) IdenTrust is prevented for any reason from operating or otherwise determines to discontinue the IdenTrust Service.
(ix) You or a Certificate Holder request that the Certificate be revoked.
(x) The Bank is required to do so under an applicable law or regulation or order of a court or other regulatory body.
(xi) Where reasonably possible (and where it would not be a breach of security or be against the law), the Bank will attempt to contact You either by telephone or in writing when it takes action under Clause8.7 (d), and explain its reasons for doing so.
(xii) Where the Bank has taken action under this Clause 8 unless it terminates the agreement as a result, the Bank will allow the normal use of Your Account to resume as soon as practicable once its reasons for taking such action cease to exist.

(e) A Certificate revocation request will only be processed if it has been received from an Authorised Signatory. In order to request the revocation of a Certificate:
(i) an Authorised Signatory must complete and sign a Certificate revocation form in the form provided by the Bank Forms are available on request from the Bank.
(ii) The Bank will verify the authority of an Authorised Signatory to request the revocation.
(iii) The Bank will revoke, or procure the revocation of, the Certificate which is the subject of the authenticated revocation request, in compliance with the requirements of the IdenTrust Service.

(f) In the case of actual or suspected Private Key compromise, You must request revocation immediately upon detection of the compromise or suspected compromise, via an Authorised Signatory.

(g) A Certificate shall be suspended where the Bank, or its Certification Authority, is advised of or becomes aware of any of the following circumstances:
(i) There is a suspicion of Identity and/or Utility Certificate Private Key compromise, but this has not been verified; or
(ii) You are in breach of the obligations of these PKI HSM Terms and Conditions; or
(iii) You or a Certificate Holder requests that the Certificate be suspended; or
(iv) A request by a valid legal authority; or
(v) If the Certificate is digitally identified to a CA Certificate (on which the Bank is relying) which has expired or is revoked.

(h) A Certificate will be un-suspended, where the Bank, or its Certification Authority, is advised of or becomes aware of any of the following circumstances:
(i) The suspicion which caused the Identity or Utility Private Key to be suspected of compromise no longer exists; or
(ii) A Certificate Holder, in conjunction with an Authorised Signatory, requests that their Certificate be un-suspended provided that such Certificate Holder originally requested that the Certificate be suspended; or
(iii) A request by a valid legal authority.

(i) A Certificate shall also be suspended where the Bank, or its Certification Authority;
(i) determines at its discretion that the use of the Certificate jeopardises the IdenTrust Service; or
(ii) deems it necessary to protect the Service, or for any other reasonable business objective;
and will be un-suspended where the Bank, or its Certification Authority;
(i) determines at its discretion that the use of the suspended Certificate no longer jeopardises the IdenTrust Service; or
(ii) no longer deems it necessary to suspend a Certificate in order to protect the Service, or to achieve any other reasonable business objective.

(j) Suspensions need not be initiated by an Authorised Signatory, but a request to un-suspend a Certificate will only be processed if received from an Authorised Signatory.
The process for Certificate suspension is as follows:
(i) On receipt of a Certificate suspension form the Bank will suspend, or procure the suspension of, the Certificate which is the subject of the suspension request, in compliance with the requirements of the IdenTrust Service.
The process for Certificate un-suspension is as follows:
(ii) An Authorised Signatory must complete and sign a Certificate un-suspension form, and submit this form, as instructed by the Bank on the form.
(iii) The Bank, or its Certification Authority, will verify the authority of the Authorised Signatory to request the un-suspension. The Bank may reject a request to un-suspend a Certificate where the request is received from an Authorised Signatory if, in the opinion of the Bank, the circumstances of the initial suspension warrant such an action.
(iv) The Bank, or its Certification Authority, will un-suspend the Certificate which is the subject of the authenticated un-suspension request, in compliance with the requirements of the IdenTrust Service.

(k) A Certificate issued under these PKI Terms and Conditions may be suspended for a period no greater than 60 days from the date of suspension request. After 60 days, the Certificate will be revoked, unless the certificate has expired in the meantime.

8.8 Following revocation of a Certificate or other termination of Your Agreement, You shall, at the request of the Bank, cease using that or any other Certificate and destroy as promptly as possible all Private Keys, Public Keys, Certificates and IdenTrust Specifications.

9. Bank Obligations

9.1 The Bank shall provide the Service in accordance with the service levels set out in these PKI HSM Terms and Conditions, as may be amended in accordance with the Specification Change Procedure set out in clause 12 from time to time.

9.2 The Bank shall use reasonable endeavours to ensure that the OCSP Responder is available 24 hours per day, 7 days per week, save where it is necessary for the OCSP Responder to be unavailable for maintenance, upgrades or in response to any emergency, including but not limited to any breach of security. In the event that the Bank intends to make the OCSP Responder unavailable, it will use reasonable endeavours to minimise any disruption to You, or to the Service.

10. Customer Obligations

10.1 You shall promptly notify the Bank of;
(a) any developments which may have a material adverse impact on Your ability to meet Your obligations under these PKI HSM Terms and Conditions; and
(b) any critical event which may cause financial damage and/or disturbance to the Bank's operations, or the operations of any of the Bank's Group Companies.

10.2 You shall notify the Bank of any compromise of the security of:
(a) a Certificate issued by the Bank as part of the Service; or
(b) the Service, Your system or any HSM; or
(c) any Public or Private Key relating to the registration authority or the Certification Authority;
as soon as You become aware of such compromise.

10.3 If You suspect, believe or become aware the validity or accuracy of any of Your Private Key(s), or Certificates has been compromised or if You or any of Your Personnel become aware of any of the

grounds for revocation or suspension of Certificates which are set out in clause 8.7, You must notify the Bank immediately.

10.4 You shall comply with, and shall ensure that Your Personnel comply with, any Certificate Policy or other procedure, user guide or manual or other instruction provided to You by the Bank, or its agent, from time to time and, where necessary, shall ensure that Your Personnel, including Certificate Holders and Authorised Signatories, are aware of and act in accordance with Your obligations under these PKI HSM Terms and Conditions.

10.5 You shall comply, or ensure that any element of Your system interfacing with or necessary to operate the Service complies, with the minimum technical specifications set out in section 8. The Bank makes no representations or warranties as to the suitability of any system or software (including telecommunications links) provided by You for the purpose of using the Service, and You will be responsible for maintaining such system, software or telecommunication links at Your expense.

10.6 You accept that, to the extent permitted by law, all warranties (express and implied) including any warranty of fitness for a particular purpose or of accuracy of information provided in respect of the Service, the Private/Public Key pairs, the Certificates or otherwise are excluded.

10.7 You shall ensure that each of Your Digital Transmissions and any notice to the Bank under these PKI HSM Terms and Conditions includes a time stamp.

10.8 You will at any time and from time to time on reasonable notice from the Bank (except in an emergency) demonstrate to the Bank's satisfaction full compliance with Your obligations under these PKI HSM Terms and Conditions and, in default, shall allow access for the Bank or its agents to Your premises, Personnel, records and systems to enable the Bank or its agents to check such compliance and will pay the Bank's costs of so doing.

11. Support

11.1 The Bank will provide support for the Service, during the hours of 9am to 5pm in the United Kingdom on Business Days, as set out in Schedule 1.

11.2 The Bank shall not be obliged to provide support in respect of:

(a) improper installation, use, operation, or neglect, of any HSM; or

(b) any problem related to any failure on Your part to comply with the provisions of clause 10.4 or clause 10.5; or

(c) any repair, alteration or modification of the HSM (including the whole or any component part thereof) by any person other than the Bank's Personnel or without the Bank's prior written consent; or

(d) any software or hardware supplied by a third party other than where it has been supplied by or on behalf of the Bank, or in accordance with the Bank's specifications.

12. Specification Change Procedure

12.1 The Bank may alter these PKI HSM Terms and Conditions from time to time in accordance with the provisions for variations set out in the General Terms.

12.2 Where the Bank takes the view that changes to these PKI HSM Terms and Conditions will have a material impact on Customers, or Certificate Holders, the Bank will:

(a) incorporate such proposed changes into a new version of these PKI HSM Terms and Conditions; and

(b) inform You, and Your Certificate Holders (as necessary) of the proposed changes in accordance with this clause 12.

12.3 Changes to these PKI HSM Terms and Conditions which, in the reasonable judgment of the Bank, will have no impact or only a minimal impact on Customers, or Certificate Holders will be effective immediately upon notification to You and will apply to all Certificates issued subsequently.

12.4 The Bank or its agent may change any aspect of the Service, or associated systems. The Bank will, to the extent possible, give You reasonable notice of such changes, in accordance with this clause 12.

13. Fees

13.1 You will pay to the Bank, on demand, the fees and charges payable to the Bank under the terms and conditions applicable to any account or other product You may hold with the Bank from time to time, and as may be notified to You in connection with the Service, from time to time. The Bank will, in consideration of Your complying with the obligations set out in these PKI HSM Terms and Conditions, and in consideration of Your continued operation of Your account(s) with the Bank (including the payment of applicable fees) provide You with the Service.

13.2 You shall be responsible for paying all telecommunication or similar costs associated with Your connection to or use of the Service.

14. Intellectual Property Rights Ownership

14.1 Subject to clause 14.2, You acknowledge that the Bank, its Certification Authority and/or IdenTrust own all rights in the Certificates, any Private Key storage mechanisms, any specifications or documentation relating to the IdenTrust Service, the IdenTrust Marks, and any other materials as may be provided to You as part of the Service from time to time.

14.2 Where materials are provided to You under a licence or sub-licence, You acknowledge that the Bank and/or its licensors own all rights in such materials.

Sub-Licence of the IdenTrust Marks

14.3 The Bank grants to You a non-exclusive, non-transferable, royalty-free, personal sub-licence to use the IdenTrust Marks:

(a) solely for the purpose of indicating that You transmit or accept Digital Transmissions authenticated through the IdenTrust Service;

(b) in accordance with the IdenTrust Marks and Brand Usage Guidelines (the "Guidelines"), as amended from time to time; and

(c) on the terms of this clause 14.

14.4 You shall have no right to assign, sub-license or otherwise transfer or purport to transfer any of the rights in the IdenTrust Marks without the prior written consent of IdenTrust. The terms of this sub-licence shall be binding on You, Your legal representatives and permitted successors and assigns. The Bank shall provide a copy of the Guidelines which are incorporated into Your Agreement on receipt of a request to do so in accordance with clause 27.

14.5 You shall notify the Bank as soon as You become aware of any actual or potential infringement, misuse or misappropriation of any right in the IdenTrust Marks and shall provide the Bank with such information or other assistance as it shall reasonably request in connection with the same.

14.6 On termination of this sub-licence, You shall immediately cease using the IdenTrust Marks and all materials bearing the same and, on request by the Bank, destroy all such materials.

15. Intellectual Property Rights Indemnity

15.1 Subject to clause 15.2, the Bank will indemnify You against liability arising under any final judgment in proceedings brought by a third party against You which determine that Your authorised use of the Certificates constitutes an infringement in the United Kingdom of any third party intellectual property rights.

15.2 The Bank will not indemnify You as provided in clause 15.1 unless You:

(a) notify the Bank in writing as soon as practicable of any infringement, suspected infringement or alleged infringement; and

(b) give the Bank, or its agent, the option to conduct the defence of such a claim, including negotiations for any settlement or compromise of that claim prior to the institution of legal proceedings; and

(c) provide the Bank with reasonable assistance in conducting the defence of such a claim; and

15.3 The Bank will not indemnify You to the extent that an infringement, suspected infringement or alleged infringement arises from:

(a) the Bank's following the system or technical documentation relating to the IdenTrust Service, any other specification issued by the Root Certificate Authority or by any third party whose requirements the Bank, or its Certification Authority, is

compelled to observe from time to time.

15.4 You will indemnify the Bank and its Group Companies against any loss, costs, expenses, demands or liability, whether direct or indirect, arising out of a claim by a third party alleging infringement of intellectual property rights, if and to the extent that;
(a) the claim arises from an event specified in paragraph 15.3; or
(b) the ability of the Bank to defend the claim has been prejudiced by Your failure to comply with any requirement of paragraph 15.2.

16. Data Protection

16.1 You and the Bank will each at all times comply with Data Protection Law, as amended from time to time, when processing personal data (as those terms are defined in the Laws), including obtaining any necessary informed consent to all processing required under these PKI HSM Terms and Conditions. Each party to these PKI HSM Terms and Conditions will take appropriate technical and organisational measures, from time to time, against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Where the Bank acts as a data processor on Your behalf, it will do so only in accordance with Your instructions and with this clause 16.

16.2 Your Certificate Holders and Authorised Signatories are entitled to obtain a copy of the personal data the Bank holds about them by contacting Your normal Relationship Manager and upon payment of the appropriate fee.

16.3 The Bank will not disclose personal data about You or Your Certificate Holders or Authorised Signatories, and in particular any details of name and address held by the Bank, to a third party except as set out in this clause 16, or with Your or their consent, or otherwise in accordance with Data Protection Laws, as amended from time to time, or the Business Banking Code.

16.4 You acknowledge that the Bank may disclose personal data as follows:-
(a) to Personnel of the Bank and its Group Companies to administer the Service, subject to such Personnel undertaking to keep personal data confidential; or
(b) to any Root Certificate Authority, and their employees and agents, involved in providing the Service (which recipient(s) may subsequently disclose such personal data to the extent necessary to provide the Service, or facilitate its provision to You); or
(c) to Personnel and distributors of the Bank contracted to provide any support or administration, IT, facilities management or similar services to the Bank; or
(d) to any company or organisation to which the Bank transfers its responsibilities to provide the Service to You to; or
(e) to any other party to a transaction, or to anyone else connected with any transaction, using the Service or their respective bankers, agents and intermediaries;
(f) to third parties including relevant professional advisers to the extent necessary in relation to any dispute between You and the Bank or any Root Certificate Authority; or
(g) if required by applicable law or pursuant to an order of a court or other government or regulatory authority with which the Bank is legally obliged to comply;
even though those parties to whom personal data is disclosed may be located outside the European Economic Area in countries where the level of protection for privacy of personal data, may not be as extensive as that within the European Economic Area.

16.5 The Bank may disclose information about You, or Your Certificate Holders or Authorised Signatories to its Group Companies in order to provide or develop the Service, but will not give information about You to its subsidiaries or associated companies for marketing purposes, without Your permission. You can choose not to receive any marketing information relating to the Bank's products and services by notifying the Bank in writing.

16.6 Telephone conversations may be recorded or monitored, for security purposes and to maintain a high standard of service.

16.7 In order to comply with its/their obligations under financial legislation, for audit purposes or to answer any future queries in respect of the same, or Your personal data, the Bank may retain personal data after Your contract with the Bank has ended. The Bank will not hold personal data for any longer than is necessary for the above purposes.

17. Liability

17.1 Save as otherwise set out in this clause 17, the Bank's liability to You will be in accordance with the terms and conditions applicable to the account or product provided to You by the Bank with which Your use of the Service is associated.

17.2 The Bank's liability shall be limited to the amount set out in the terms and conditions applicable to the account or product offered to You by the Bank with which You use this Service, except to the extent that wilful or negligent acts or omissions of the Bank cause loss or damage.

17.3 The Bank will not be responsible for, and exclude liability for, indirect or consequential loss or damage that You may suffer or incur for any reason including but not limited to loss of profits, anticipated savings or loss of business or revenue.

17.4 If for any reason (including faults or defects in components supplied to You by, or on behalf of, the Bank, in connection with the Service) the Certificates are unavailable or do not perform as expected or required by You, such that You are not able to use the Service or complete transactions, including as a result of improper or incorrect use of the Certificates or Service by Your Certificate Holder, or as a result of the act or omission of a third party, the Bank will not be responsible for, or be liable for, any resulting loss or damage.

17.5 The Bank shall not be liable for any liability, loss or damage arising from a transaction resulting from Digital Transmissions authenticated with a Certificate created with Your Private Key;
(a) where such Certificate has expired; or
(b) where the Bank has received a request to revoke or suspend a Certificate, for up to sixty (60) minutes from the time of confirmation that such request has been received, or until Your Certificate has been suspended or revoked, whichever is the sooner.
For the avoidance of doubt, where You or Your Certificate Holder make a Digital Transmission based upon a Certificate that has expired, or in relation to which receipt of a suspension or revocation request has been acknowledged by or on behalf of the Bank, in the event that the Bank or its agent acts on the Digital Transmission in question where such is in respect of a transaction authorised by You, the Bank shall not be liable to You.

17.6 The Bank shall not be responsible or any loss, damage or liability that You may suffer or incur by reason of or in connection with:
(a) the Bank acting on any facsimile instruction which purports to have been despatched from You by any person appearing to be an Authorised Signatory; or
(b) any error contained in any facsimile message irrespective of whether the error originated in the transmission or the receipt of the facsimile message; or
(c) any delays in transmission or payment resulting from an error or errors contained in any facsimile message; or
(d) any non-receipt by the Bank of a facsimile message which appears to have been transmitted by You.

17.7 You agree that each act or omission of each of Your Authorised Signatories and Certificate Holders shall for all purposes of these PKI HSM Terms and Conditions be deemed to be an act or omission of You.

17.8 If the Bank elects to provide any aspect of the Service through an agent or sub-contractor (which, for the purposes of this clause 17.8, shall include the Bank's Certification Authority) then You agree that no such agent or sub-contractor will have any liability to You and that You will not be entitled to make any claim against them.

18. Financial Responsibility

18.1 You will indemnify and continue to indemnify the Bank, its Group Companies, its Certification Authority and any agent or sub-

contractor through whom the Bank elects to provide any aspect of the Service from time to time and IdenTrust fully against any liability, loss or damage suffered or incurred by them, howsoever arising and by whomsoever caused, whether arising directly or indirectly, in relation to:

(a) conduct by You leading to an erroneous valid Certificate status response being generated with respect to a Certificate registered to You; or
(b) conduct on the part of Your Certificate Holders; or
(c) conduct by any third party supplier of software or systems that You instruct, save where such supplier is engaged on the instructions of the Bank; or
(d) Digital Transmissions, sent or generated by You or Your Certificate Holders, to persons or entities that are not IdenTrust Participants; or
(e) any failure on Your part to comply with these PKI HSM Terms and Conditions; or
(f) otherwise Your use and operation of the Service, or Your access to the Service, except to the extent such liability, loss or damage is due to the wilful acts or negligence of the Bank.

18.2 The Bank may, at its discretion debit Your account with all sums paid, charged or incurred by the Bank in effecting instructions that purport to have been despatched from You by an Authorised Signatory, or any person who appears to be an Authorised Signatory, and on demand, You will place the Bank in funds to meet such debits.

18.3 You agree not to make any claim or demand against the Bank in respect of any such loss, damage or liability, and shall indemnify the Bank against any loss, damage or liability the Bank may suffer or incur as a result of acting in accordance with the provisions of clause 27.2.

19. Hardware

The Bank or its agent may supply, or offer to supply, You with Hardware from time to time, or supply You with minimum technical specifications for infrastructure required for the use of, or integration with, the Service. Any additional terms relating to such Hardware, or to such technical specification, will be notified to You in accordance with clause 12 (Specification Change Procedure).

20. Warranties

20.1 You warrant that any information submitted to the Bank, or to their agent, including to any Certification or Root Certificate Authority in connection with a request for a Certificate, or the confirmation of any Certificate as a valid Certificate, is accurate.

20.2 You shall take reasonable steps to ensure that all material provided by You, or on Your behalf from time to time, to the Bank or its agent, including to any Root Certificate Authority or otherwise used by it or them in connection with the Service contains no viruses, worms, Trojan horses, time bombs, time locks or similar programs or devices.

21. Recourse

21.1 You agree that Your only recourse in connection with the Service, including with respect to claims arising out of the negligence of any person, is to the Bank, and only to the extent provided for in these PKI HSM Terms and Conditions.

21.2 You recognise and agree that You have no recourse in this regard to IdenTrust, any IdenTrust Participant, the Bank's Certification Authority or any other person, in connection with the Service, but may have recourse or liability to other Customers, or customers of other IdenTrust Participants, that are the counter-parties to Digital Transmissions sent or received by You.

21.3 Nothing in this clause 21 shall be construed to exclude liability for gross negligence or wilful misconduct, or for any other liability that cannot be excluded by law.

22. Legal Effectiveness of Certificates

22.1 You agree that all Digital Transmissions authenticated with a Digital Signature created with Your Private Key(s) shall have the same legal effect, validity and enforcement as if the Digital Transmission had been in writing, and signed by You.

22.2 You will not challenge the legal effect, validity or enforceability of a Digital Transmission or Certificate on the basis that it is in digital rather than written form.

22.3 You shall not interfere with any procedures in relation to the logging or time-stamping of Digital Transmissions or the verification of Digital Signatures generated using any Certificate supplied.

22.4 All records of Digital Transmissions shall be admissible in court, and shall be deemed to constitute evidence of the facts contained therein, save as set out in clause 22.5.

22.5 You acknowledge and agree that all records of the time at which an event took place generated in accordance with these PKI HSM Terms and Conditions shall be deemed to be correct, and shall be accepted by You as conclusive evidence of the time at which such an event took place, other than in relation to fraud or manifest error, or where proved to the contrary by You.

23. Termination

23.1 The Bank may suspend or terminate Your use of the Service, in whole or in part, at any time, in accordance with the termination provisions set out in the General Terms.

23.2 You may terminate Your use of the Service by giving the Bank one month's written notice of termination. Such termination:

23.3 will not be effective unless the notice of termination is actually received by the Bank at the address specified in the General Terms and;

23.4 will take effect from 5pm, London time, on the Business Day after the day on which the Bank actually receives notice of termination; and

23.5 will not affect any obligations incurred by You in respect of use of the Service prior to the time at which termination takes effect under paragraph 23.4.

23.6 All monies due and owing to the Bank in connection with the Service, if not already due and payable, will immediately become due and payable upon the date that the Bank actually receives notice of termination or upon which the Bank terminates Your Agreement.

23.7 The Bank may in its sole discretion decide not to process any transactions that have been forward-dated to take effect after the time at which termination takes effect.

23.8 If the Bank receives transactions via the Service after notice to terminate has been given by either party, but before termination has taken effect, those transactions may be acted upon before termination, but shall not be acted upon after termination.

23.9 These PKI HSM Terms and Conditions will continue indefinitely, save in the event of an earlier termination in accordance with this clause 23.

24. Confidentiality

24.1 You shall not use or disclose to any third party or permit any others to use or disclose to any third party, any Confidential Information received from the Bank, or its agent, for any purpose other than the development or operation of the Service, without the prior written consent of the Bank or its agent as appropriate. The Bank shall not disclose to any third party, or permit any others to disclose to any third party, any Confidential Information received from You or Your Certificate Holders or Authorised Signatories, other than in accordance with clauses 16 and 24.

24.2 Except when otherwise provided by applicable law, the obligations of this clause 24 shall not apply to any disclosure of Confidential Information if that disclosure:

(a) is necessary to provide any aspect of the IdenTrust Service including disclosure between the Bank and its Certification Authority;
(b) is pursuant to the investigation or resolution of an alleged error;
(c) is pursuant to a dispute resolution or the resolution of a dispute arising under these PKI HSM Terms and Conditions;
(d) is otherwise authorised by the parties with an interest in the information;
(e) is required by applicable law or is pursuant to an order of a court or other government or regulatory authority with which

the recipient is legally obliged to comply;

(f) is pursuant to a demand made by any government regulatory agency or authority with jurisdiction over the recipient.

24.3 A recipient of Confidential Information shall limit disclosure of such Confidential Information to its employees, professional advisers, consultants and representatives who require access to such information to enable the recipient to develop and operate the Service and who have been made aware of and instructed to observe the terms of this clause 24, save only that the Bank may disclose Confidential Information to its Group Companies, in order to provide or develop the Service.

24.4 A recipient shall provide notice to the disclosing party as promptly as reasonably possible in the event the recipient learns of an actual or potential breach of confidentiality of any Confidential Information of the disclosing party and shall reasonably co-operate with that disclosing party to remedy such breach of confidentiality and, if possible, recover any disclosed Confidential Information.

24.5 If a recipient is required by an order of any court or other government agency to disclose any Confidential Information disclosed to it, it shall provide the disclosing party with prompt written notice of any such requirement so that the disclosing party may seek an appropriate protective order or waive compliance with the provisions hereof. Upon the request and at the expense of the disclosing party the recipient will reasonably co-operate with the disclosing party to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded such Confidential Information.

24.6 Nothing in this clause 24 shall be construed as:

(a) confirming an expressed or implied licence or an option of a licence to a recipient, whether under any patent, copyright, trade mark, licence right or trade secret owned or obtained by the disclosing party; or

(b) obliging a party to enter into any other agreement of any kind with another party.

24.7 The parties agree that in the event of any breach by a recipient of any of the obligations in this clause 24, the disclosing party shall have the right to:

(a) receive compensation for actual damages from the recipient for any losses incurred by reason of such breach, including reasonable legal costs; and

(b) apply pursuant to the dispute resolution procedure set out in these PKI HSM Terms and Conditions, or to a court of competent jurisdiction, for the entry of an immediate order to restrain or enjoin the breach of such obligations by the recipient and otherwise to specifically enforce the provisions of this clause 24. The recipient hereby waives the claim or defence in any such action that the disclosing party has an adequate remedy at law or in damages, and shall not claim in any such action or proceeding the claim or defence that such a remedy at law or in damages exists.

24.8 Upon the earliest of:

(a) termination of these PKI HSM Terms and Conditions; or

(b) the request of a disclosing party;

a recipient shall promptly (but in any event within 30 days following termination or receipt of any request) return to the disclosing party, or at the disclosing party's option, destroy, any Confidential Information (and all copies thereof made by or for the recipient) in tangible form in any and all media, and delete or erase such Confidential Information (and copies) from computer systems, in the possession, custody or control of the recipient or any person acquiring such Confidential Information (and copies) through the recipient. The recipient shall certify to the disclosing party, in writing, that it has complied with the requirements of this clause 24.8.

25. Dispute Resolution Procedures

25.1 If You are not happy with any part of Our service, please ask Us for a copy of Our leaflet 'Putting things right for you' or visit Our website. We aim to deal with complaints in a way Our customers are satisfied with.

If You have followed Our published complaint procedures and You disagree with the response We have given, You can refer the matter to the Financial Ombudsman Service. Details are available from Us or from www.financial-ombudsman.org.uk.

If You are a Corporate Opt-out Customer You will not be able to complain to the Financial Ombudsman Service. Further details are available in Our leaflet 'Putting things right for you'.

You will also be able to contact the Financial Conduct Authority (FCA) or the Payment Systems Regulator (PSR) if You think that We have broken the Payment Services Regulations 2017.

The FCA and the PSR will use this information to inform their regulatory activities. More information can be found at https://www.psr.org.uk/sites/default/files/media/ PDF/PSR-PSD2-approach-factsheet-Sep-2017.pdf

25.2 Making a complaint will not prejudice Your right to instigate legal proceedings.

25.3 In the event of any dispute solely between You and the Bank, arising out of or in connection with the Service, which has not been resolved in accordance with the complaints handling procedure set out in clause 25.1, You may instigate legal proceedings against the Bank, subject to restrictions in these PKI HSM Terms and Conditions.

25.4 The Bank will not intervene in any dispute between Customers and third party complainants in relation to the registration or use of a subject name in a Certificate. In the event that any party notifies the Bank that it has a claim in respect to the subject name in a Certificate, or any other information contained in a Certificate, the Bank will notify You of such notification of a dispute but will take no other action.

25.5 You agree that, in the event of any dispute between You and any IdenTrust Participant other than the Bank or between You and the Bank's Certification Authority, and/or between You and IdenTrust, or any dispute with the Bank that involves related claims by, or against, other IdenTrust Participants, any Certification Authority and/or IdenTrust, which dispute arises out of or in connection with the Service or the IdenTrust Services, shall be finally determined pursuant to the IdenTrust Dispute Resolution Procedures (which are incorporated into Your Agreement and a copy of which is available on request in accordance with clause 27) and You will not challenge any such determination in any other forum.

25.6 You expressly consent to being joined as a party to any dispute resolution procedure in respect of disputes provided for under clause 25.3, and in accordance with the IdenTrust Dispute Resolution Procedures.

25.7 In the event that You, or a counter-party to a Digital Transmission sent or received by You, seek a determination under the IdenTrust Dispute Resolution Procedures, as to whether a Digital Signature is genuine, valid, binding and legally enforceable, You acknowledge and agree that such determination shall be final.

26. Sub-Contractors

Subject to the provisions of this clause 26, the Service will be provided by the Bank but, for the avoidance of doubt, You acknowledge that the Bank may provide the Service using third party sub-contractors.

27.Notices

27.1 All notices or communications required or permitted under the Agreement shall comply with the notice provisions set out in the General Terms.

27.2 The Bank is hereby authorised to accept, and act upon on Your behalf, any facsimile or other written message received by the Bank which purports to have been despatched from You, acting by an Authorised Signatory, or a person who appears to be an Authorised Signatory at the time the message is received, irrespective of whether the message in fact was despatched by an Authorised Signatory.

28. Entire Agreement and Enforceability

28.1 Your application form (once approved by the Bank), these PKI HSM Terms and Conditions, and the terms and conditions applicable to any other account or product provided to You by the Bank with which Your use of the Service is associated, are the entire agreement between You and the Bank, and all other terms, conditions, undertakings and warranties (whether implied by law or otherwise) are excluded, to the extent permitted by law.

28.2 In the event that any provision of these PKI HSM Terms and Conditions is held to be unenforceable, it will not affect the validity and enforceability of the remaining provisions and will be replaced by an enforceable provision that comes closest to the intention underlying the unenforceable provision.

29. Assignment and Third Party Rights

29.1 You may not assign or transfer to any other person or entity any of Your rights and interests under Your Agreement without the prior written consent of the Bank.

29.2 The Bank may assign any of its rights and interests under Your Agreement, without Your consent.

29.3 Nothing in these PKI HSM Terms and Conditions shall give any rights to any Third Party under the Contracts (Rights of Third Parties) Act 1999, save as expressly set out in these PKI HSM Terms and Conditions including, without limitation, those provisions which provide a benefit to IdenTrust, other IdenTrust Participants, any Certification Authority or the Bank's agents or sub-contractors.

30. Governing Law

30.1 Your Agreement and the transactions contemplated by these PKI HSM Terms and Conditions are governed by and construed in accordance with the laws of Northern Ireland and each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the courts of Northern Ireland.

Danske Bank is a trading name of Northern Bank Limited which is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority and complies with the FCA's requirements to pay due regard to customers' interests and to treat customers fairly.

Schedule 1: Support

The Bank will provide support for the Service, during the hours of 9am to 5pm in the United Kingdom on Business Days.
Support is subject to the exclusions set out in clause 11.2.
In the event that You wish to obtain support, You should contact the Bacs Customer Service on 0345 603 4615.

This publication is also available in Braille, in large print, on tape and on disk. Speak to a member of staff for details.

Registered in Northern Ireland Number: R568.
Registered office:
Donegall Square West
Belfast
BT1 6JS.
www.danskebank .co.uk

Northern Bank Limited is a member of the Danske Bank Group.

Correct as at 05/2018