# Public Key Infrastructure

## Customer Terms and Conditions

**1. Definitions**

1.1 In these PKI 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 Clydesdale Bank PLC (including Yorkshire Bank which is a trading name of Clydesdale Bank PLC). Clydesdale Bank PLC registered in Scotland with company number SC001111 whose registered office is at 30 St Vincent Place, Glasgow G1 2HL, and its successors and assigns;

"**Business Day**" "**Business Day**" means a day on which the Bank is ordinarily open to provide services of the kind contemplated in these PKI Terms and Conditions;

"**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 or in the case of a HSM, uniquely identifying the HSM containing the Private Key, corresponding to such Public Key, including those issued to you in accordance with these PKI Terms and Conditions;

"**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, authorised to hold, and issued with, a Certificate;

"**Certificate Policy**" or "**CP**" means either of the Identity or Utility Certificate Policies issued by the Bank (which 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 in relation to CPs;

"**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 or the Bank, 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 PKI Application Form;

"**Data Protection Laws**" means all laws that relate to data protection, privacy, the use of information relating to individuals, and/or the information rights of individuals including, without limitation, the Data Protection Act 1998, European Commission Directive 95/46/EC, the General Data Protection Regulation (EU) 2016/679 and all laws implementing them, in each case as may be replaced, extended or amended.

"**Digital Signature**" means the signing 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 the signing entity that is created by the entity applying its Private Key to a Digital Transmission for the purpose of confirming the identity of that signing entity, and is associated 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 signing entity'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 PKI Service, and which is signed with a Digital Signature and which includes a Certificate;

"**Group Companies**" means, in relation to a party to these PKI Terms and Conditions any group undertaking (as such term is defined in the Companies Act 2006, as amended from time to time) for the time being and 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;

"**Hardware Security Module**" or "**HSM**" means a PCI card or external device meeting the Bank's technical and other requirements and standards, for the time being and from time to time, relating to HSMs;

"**HSM Contact**" means the individual, whether an employee, agent or officer of the Customer appointed as the named contact point in respect of Certificates installed, or to be installed, on a given HSM;

"**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 limited liability corporation established in the state of Delaware, USA;

"**IdenTrust Service**" means the digital integrity and identify validation services provided by IdenTrust;

"**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 and Sign Online Smart cards;

"**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 section 123 of the Insolvency Act 1986 (the "Act") (other than by reason of the service of a written demand pursuant to section 123(1)(1) of the Act 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 dismissed within 28 days of its presentation;

(d) distress, 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;

(e) 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 party of your undertaking or assets; or

(f) if any event analogous to (a) to (e) of this definition shall occur in any other jurisdiction to which you are subject;

"**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 and HSM Contacts;

"**PKI Terms and Conditions**" means the terms and conditions governing the relationship between you and the Bank in relation to the PKI Service as set out in this document and the PKI Application Form;

"**PIN**" means a personal identification number or phrase, which may include alpha numeric or other symbol components, that is used by you or your Certificate Holder in conjunction with your Sign Online Smart card for the purpose of authorising Digital Transmissions;

"**Private Key**" means the key within any asymmetric key pair generated by a public key infrastructure service for a person or HSM which is normally known only by that person or, in the case of a HSM, installed securely on the HSM, 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 Terms and Conditions,
a Certificate Holder) may apply to electronic transmissions, messages or records for identification and communications 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 Terms and Conditions, a Certificate Holder or HSM);
"**Root Certificate Authority**" means IdenTrust or any other root Certificate authority used by the Bank from time to time;
"**PKI 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 the Sign Online Smart card or Smart cards issued to you or your Certificate Holders;
"**Sign Online Smart card**" means the smart card issued by the Bank to Certificate Holders appointed or selected by you;
"**Software**" means the software supplied or specified to you for use in connection with the PKI Service, from time to time, by or on behalf of the Bank or its agent;
"**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 "**your**" refers to the Customer(s) set out in the PKI Application Form who apply to use the PKI Service, and where there is more than one 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 PKI Service, any other Authorised Signatory.

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

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

1.4 If there is any conflict between the terms of the main body of these PKI Terms and Conditions and those contained in any Schedule or document referred to, to the extent of that conflict, the documents shall have the following order of precedence:
(a) the main body of these PKI Terms and Conditions;
(b) the Schedules to these PKI Terms and Conditions;
(c) the CPS or any CPs;

**2. Certificates**

2.1 The Bank may issue, or procure the issue of, Certificates to you as part of the PKI 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 Terms and Conditions.

**3. The PKI Service**

3.1 You may use the PKI Service provided by the Bank;
(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; or
(c) to carry out the activities set out in both (a) and (b) of this clause 3.1.

3.2 You agree that any use of Certificates issued to you in connection with the PKI 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 established or imposed under these PKI Terms and Conditions.
(c) You may only use Certificates in conjunction with IdenTrust applications or the IdenTrust Service
(d) 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.
(e) 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.
(f) 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.

3.3 You may not use your Private Keys, Certificates or HSMs:
(a) in relation to any transaction where you are not acting as principal, or agent for a principal disclosed to the Bank; or
(b) in connection with any Digital Transmission involving any transaction prohibited by applicable law or for, or in connection with, any illegal or unlawful purpose.

**4. Authentication of Identity**

4.1 Prior to issuing Certificates 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 Terms and Conditions or the CPS, which is available to you on request in accordance with clause 27;
(c) any procedures mandated by either local banking licence regulatory requirements, for the time being and from time to time.

4.2 The Bank may confirm the identity of your Certificate Holders in accordance with the requirements set out in clause 4.1 (a) to (c), but shall unless otherwise notified to the Customer, follow the procedure set out in clause 4.3.

4.3 The Customer shall confirm:
(a) the identity of its potential Certificate Holders and confirm their authority to act;
(b) the details to be included in Certificates installed on a HSM, and one of your Authorised Signatories shall notify the Bank of the identity of any potential new Certificate Holder, and confirm their authority to act.

4.4 The Bank may rely upon any Digital Transmission issued in accordance with these PKI Terms and Conditions by any Certificate Holder or HSM (where that Certificate Holder or HSM 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 7.5(b).

**5. Responsibility for Digital Transmissions**

5.1 Subject to clauses 5.2 and 16, 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 PKI Service.

5.2 Where you have notified the Bank in accordance with clause 9.3 that the security of your system has been compromised you will remain responsible for all Digital Transmissions signed with your Certificate during:
(a) the sixty (60) minute period immediately after the Bank acknowledges your notification by fax; or secure email and
(b) the period prior to the time the Bank has confirmed by fax or secure email that your Certificates have been suspended or revoked whichever is the sooner.

5.3 Where you have confirmed to the Bank in accordance with clause 4 that an individual is authorised to act as a Certificate Holder or a Certificate is to be installed on a HSM, and provided (subject to clause 5.2) 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, HSM Contacts and, in the case of a HSM, any processing or failure to process by a HSM, (with respect to the relevant Certificate) shall for the purposes of these PKI 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.

**6. Security**

6.1 You are solely responsible for establishing and applying adequate security systems, controls and procedures in accordance with the Certificate Policies and these PKI Terms and Conditions in relation to:
(a) your Software, any Sign Online Smart card, HSMs and any Private Keys issued to you or to your Certificate Holders or installed on your HSMs, to prevent their loss, disclosure to any other party, modification or unauthorised use;
(b) monitoring all usage of the PKI Service by your Certificate Holders and HSMs including, without limitation, all use of Certificates and all Digital Transmissions.

6.2 You must not disclose any PIN to anyone and must procure that your Certificate Holders do not disclose any PIN.

6.3 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. Operational Requirements**

7.1 Certificate application
Application forms for the issuance 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 Terms and Conditions.

7.2 Certificate issuance – Sign Online Smart cards
The process for Certificate issuance is as follows:
(a) the Bank will authenticate the identity of the applicant in accordance with clause 4 of these PKI Terms and Conditions;
(b) the Bank will generate and issue a Certificate for the applicant in accordance with these PKI Terms and Conditions, and in accordance with the rules applicable to the IdenTrust Service; and
(c) you or your Certificate Holder must acknowledge receipt of any Certificate, and (in accordance with clause 7.3(c)) check the accuracy of the information contained within that Certificate on the day of receipt of such Certificate (and in any event prior to its use).

7.3 Certificate issuance – HSMs
The process for Certificate issuance is as follows:
(a) the Bank will authenticate the identity of the applicant in accordance with clause 4. The Bank will confirm to you whether or not the HSM you propose to use is of a type which is acceptable to IdenTrust;
(b) you 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 USB Token that is 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 Terms and Conditions, and in accordance with the rules applicable to the IdenTrust Service;
(d) the Certificate will be delivered to you in person by a member of the Bank; the Certificate will be saved on a USB Token or can be requested by your one of your Authorised Signatories by PGP encrypted mail, whilst on site.

One of your Authorised Signatories will also be on site when the Certificate is loaded to the HSM; and,
(e) you or your HSM Contact must acknowledge receipt of any Certificate, and (in accordance with clause 7.4(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).

7.4 Certificate acceptance
(a) You acknowledge that your first use, or that of any Certificate Holder, of the PKI Service, or of any Certificate (including any Certificate installed on a HSM), 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 available on request in accordance with clause 27), and these PKI Terms and Conditions.
(b) You acknowledge that your first use, or that of any Certificate Holder, of any Private Key (including any Private Key installed on a HSM) 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 Terms and Conditions.
(c) Your Certificate Holder(s) and HSM Contacts 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.

7.5 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 5.2. Pending the revocation or suspension of any Certificate, the provisions of clause 5.2 shall apply.
(b) The Bank shall act on any notice to revoke the status of Authorised Signatories, HSM Contacts or Certificate Holders, in accordance with clause 27.
(c) The Bank shall act to revoke or suspend a Certificate in accordance with the terms of this clause 7.5.
(d) A Certificate shall be revoked where the Bank 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 or HSM.
(ii) Material information contained in the Certificate is no longer valid.
(iii) The applicable Certificate Holder's Sign Online Smart card is irreversibly blocked, lost or stolen.
(iv) You, a HSM Contact or a Certificate Holder have breached a material obligation (which includes failure to pay charges as and when they fall due) of these PKI Terms & Conditions or under the applicable Certificate Policy.
(v) The performance of your, a HSM Contact's or a Certificate Holder's obligations under these PKI 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.
(vi) The Bank deems that the revocation of the Certificate is necessary or appropriate to maintain the integrity of the PKI Service.
(vii) The Bank is requested to revoke a Certificate by a valid legal authority, or by the Root Certificate Authority.
(viii) The HSM on which the Certificate is installed has been lost, stolen or otherwise compromised.
(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 in your Sign Online user pack) and submit this form as instructed by the Bank on the form.
(ii) the Bank will verify the authority of an Authorised Signatory to request the revocation; and,
(iii) the Bank will revoke, or procure the verification of, the Certificate which is the subject of the authenticated revocation request, in compliance with the requirements of the IdenTrust Scheme.
(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 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 Terms & Conditions (including your failure to pay charges as and when they fall due) or under the applicable Certificate Policy; or
(iii) a Certificate Holder requests that their Certificate be suspended; or
(iv) a request by a valid legal authority;
(v) a HSM Contact requests that their Certificate be suspended; and a Certificate will be un-suspended, where the Bank is advised of or becomes aware of any of the following circumstances:
(vi) the suspicion which caused the Identity or Utility Private Key to be suspected of compromise no longer exists; or
(vii) a Certificate Holder or HSM Contact, 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
(viii) a request by a valid legal authority; or
(ix) any unpaid charges have not been paid up-to-date.
(h) A Certificate shall also be suspended where the Bank:
(i) determines at its discretion that the use of the Certificate jeopardises the IdenTrust Service; or
(ii) deems it necessary to protect the PKI Service, or for any other reasonable business objective; and a Certificate will be un-suspended where the Bank;
(iii) determines at its discretion that the use of the suspended Certificate no longer jeopardises the IdenTrust Service; or
(iv) no longer deems it necessary to suspend a Certificate in order to protect the PKI Service, or to achieve any other reasonable business objective.
(i) 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 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:
(i) An Authorised Signatory must complete and sign a Certificate un-suspension form, and submit this form, as instructed by the Bank on the form.
(ii) The Bank 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
(iii) suspension warrant such an action.
(iv) The Bank will unsuspend the Certificate which is the subject of the authenticated un-suspension request, in compliance with the requirements of the IdenTrust Service.
(j) A Certificate issued under these PKI Terms and Conditions may be suspended for a period no greater than 60 days from the date of the suspension request, (at which point the Certificate will be revoked) or until the date of expiry, whichever occurs first.

7.6 Certificate Security.
(a) Private Keys held in a HSM must be subject to access controls to ensure that personnel without appropriate authority cannot access the HSM and its contents.
(b) If an HSM stores its Private Key external to the smart card/module the following minimum security requirements should be implemented by you:
(i) the Private Key should be stored in an encrypted file protected by at least 168 Bit 3DES or 192 Bit AES encryption;
(ii) the directory where the Private Key is located should not be shared for public access.
(iii) the Private Key should only be decrypted within the HSM itself; and
(iv) the HSM should be configured on initial setup to require as a minimum 2 person present for start-up/recovery purposes.
(c) Electronically distributed Private Keys must be entered and output in at least 168 Bit 3DES or 192 Bit AES – encrypted format.

**8. Bank Obligations**

8.1 The Bank shall provide the PKI Service in accordance with the service level set out in clause 7.5(a) of these PKI Terms and Conditions, as may be amended in accordance with the Specification Change Procedures set out in clause 11 from time to time.

8.2 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 PKI Service.

**9. Customer Obligations**

9.1 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 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.

9.2 You shall notify the Bank of any compromise or suspected compromise of the security of:
(a) a Certificate issued by the Bank as part of the PKI Service; or
(b) the PKI Service, your system or any Sign Online Smart card; or
(c) any Public or Private Key relating to the registration authority or the
(d) Certification Authority; as soon as you become aware of such compromise.

9.3 If you suspect, believe or become aware that an unauthorised party knows your or any other PIN, or that the safekeeping of any of your Private Key(s), HSM(s), Sign Online Smart card(s) or Certificate(s) has or have been compromised, you must notify the Bank immediately.

9.4 You confirm that you are familiar with, and shall comply with, and shall ensure that your Personnel are familiar and comply with, the CPs and procedures (including policies and procedures relating to the Bank's issuance, expiration and revocation of Certificates), 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 Terms and Conditions.

9.5 You shall comply, or ensure that any element of your system interfacing with or necessary to operate the PKI Service complies, with the minimum technical specifications set out in Schedule 2 in respect of the use of Sign Online Smart cards and set out in Schedule 3 in respect of the use of HSMs. 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 PKI Service, and you will be responsible for maintaining such system, software or telecommunication links at your expense.

**10. Customer Support**

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

10.2 The Bank shall not be obliged to provide support in respect of:
(a) improper installation, use, operation, or neglect, of the Software, any HSM or any Sign Online Smart card; or
(b) use of the Software, HSM or any Sign Online Smart card for purposes for which it was not designed; or
(c) any problem related to any failure on your part to comply with the provisions of clause 9.4 or clause 9.5; or

(d) any repair, alteration or modification of the Software or any Sign Online Smart card (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
(e) where applicable, your failure to install any new release or upgrade of the Software issued to you by the Bank, or its agent; or
(f) your use of the Software, HSM or any Sign Online Smart card other than as specified in any user guide supplied by the Bank, or its agent; or
(g) any unforeseeable impact on the existing software, operating system or applications on your information technology or telecommunications systems; or
(h) any software or hardware supplied by a third party other than where such third party supplied software has been supplied by or on behalf of the Bank, or in accordance with the Bank's specifications.

**11. Change Procedure**

11.1 The Bank may alter these PKI Terms and Conditions from time to time. Any such change may be made only prospectively, and no retrospective amendments will be made.

11.2 The Bank will incorporate any such change (other than the application of, or a change to, charges payable in respect of the PKI Services in which event clause 12.3 shall apply) into a new version of these PKI Terms and Conditions. The date and time at which the new version becomes effective will be indicated on the first page of such version, but will other than as set out in clause 11.4 be no less than 30 days after the Bank has notified you of the prospective changes. The most recent version these PKI Terms and Conditions will supersede all previous versions and be binding upon you in respect to use of or reliance upon Certificates after the date the change becomes effective.

11.3 Where the Bank takes the view that changes to these PKI Terms and Conditions will have a material impact on Customers, HSM Contacts or Certificate Holders, holding or responsible for Certificates issued by the Bank, the Bank will:
(a) incorporate such proposed changes into a new version of these PKI Terms and Conditions; and
(b) inform you, your HSM Contacts and your Certificate Holders (as necessary) of the proposed changes in accordance with this clause 11.

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

11.5 The Bank or its agent may change any aspect of the PKI Service, or associated systems. The Bank will, to the extent possible, give you reasonable notice of such changes, in accordance with this clause 11.

**12. Fees**

12.1 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 PKI Service, from time to time. The Bank will, in consideration of your complying with the obligations set out in these PKI 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 PKI Service.

12.2 You shall be responsible for paying all telecommunication or similar costs associated with your connection to the PKI Service.

12.3 You shall be responsible for paying charges applicable to the PKI Services at the then current rate published by the Bank. The application of any new charges, or changes to existing charges, will take effect no less than 30 days after the Bank has notified you of the prospective changes.

**13. Intellectual Property Rights Ownership**

13.1 Subject to clause 13.2, you acknowledge that the Bank and/or IdenTrust own all rights in the Certificates, any private key storage mechanisms (including, but not limited to, any Sign Online Smart card), 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 PKI Service from time to time.

13.2 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**

13.3 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 13.

13.4 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 on receipt of a request to do so in accordance with clause 27.

**14. Intellectual Property Rights Indemnity**

14.1 Subject to clause 14.2, 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 Software or any Sign Online Smart card constitutes an infringement in the United Kingdom of any third party intellectual property rights.

14.2 The Bank will not indemnify you as provided in clause 14.1 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
(d) permit the Bank or its agent to modify, alter or substitute the infringing part of the Software or any Sign Online Smart card at its own expense in order to avoid continuing infringement, or at the option of the Bank, authorise the Bank or its agent to procure for you the authority to continue the use and possession of the infringing Software or any Sign Online Smart card.

14.3 The Bank will not indemnify you to the extent that an infringement, suspected infringement or alleged infringement arises from:
(a) use of the Software or any Sign Online Smart card in combination by any means and in any form with other software, programs or applications not specifically approved by the Bank; or
(b) use of the Software in a manner or for a purpose not reasonably contemplated or not authorised by the Bank; or
(c) modification or alteration of the Software without the prior written consent of the Bank; or
(d) any transaction entered into by you relating to the Software without the Bank's prior written consent; or t
(e) The Bank 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 is compelled to observe from time to time, or from ensuring that the PKI Service is in accordance with the Gatekeeper Scheme.

14.4 You will indemnify the Bank 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 14.3; or
(b) the ability of the Bank to defend the claim has been prejudiced by your failure to comply with any requirements of paragraph 14.2.

**15. Data Protection**

15.1 When the Bank gathers personal information from you, Certificate Holders or Authorised Signatories to make the Services available, the Bank is acting as a data controller. All of the up to date information about how we will gather, create, share and look after any personal information in providing the Services can be found in the Fair Processing Notice at: www.cbonline.co.uk/privacyor www.ybonline.co.uk/privacy. Where we need consent to use personal information we will highlight this to you in the application process and ask for consent separately.

15.2 You agree to provide our Fair Processing Notice at: www.cbonline.co.uk/privacy or www.ybonline.co.uk/privacy to your Certificate Holders, Authorised Signatories, and anyone else whose personal information you pass to the Bank to make the Services available.

15.3 You and the Bank will each at all times comply with Data Protection Laws when using personal information.

15.4 For the purposes of this Clause [15], "personal information" means personal data provided or otherwise made available to the Bank for the purpose of the Services, and "data controller" and "personal data" have the meaning given to them in the Data Protection Laws.

**16. Liability**

16.1 Save as otherwise set out in this clause 16, 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 PKI Service is associated.

16.2 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 PKI Service, except to the extent that:
(a) fraud, wilful or gross negligent acts or omissions of the Bank cause loss or damage; or
(b) Payment Services Regulations 2009 ("the regulations") apply in which event the relevant account or product (as appropriate) terms and conditions which implement or address the regulations will apply.

16.3 If the Bank fails to comply with these terms and conditions, the Bank shall not be responsible for any
(i) loss of profits,
(ii) loss of business,
(iii) loss of goodwill
(iv) loss of anticipated savings or
(v) any other loss that you suffer that is not foreseeable. A loss is foreseeable if it is an obvious consequence of such failure or if it was contemplated by you and the Bank at the time the Bank first provide the PKI Service to you.

16.4 If for any reason (including faults or defects in a Sign Online Smart card or the Software or other components supplied to you by, or on behalf of, the Bank, in connection with the PKI Service) the Software or Sign Online Smart card fails, is unavailable or does not perform as expected or required by you, such that you are not able to use the PKI Service or complete transactions, the Bank will not be responsible for, or be liable for, any resulting loss or damage that is foreseeable. For the avoidance of doubt, the Bank is not responsible for, and has no liability in connection with, any HSM used by you. A loss is foreseeable if it is an obvious consequence of such failure, unavailability or performance or if it was contemplated by the Bank and you at the time you agreed to be bound by these terms and conditions. The Bank will not be responsible for any loss or damage that you suffer as a result of improper or incorrect use of the Sign Online Smart card or PKI Service by your Certificate Holder, or as a result of the act or omission of a third party.

16.5 The Bank will 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.

16.6 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. Financial Responsibility**

17.1 Subject to any limitation imposed by law, you will indemnify and continue to indemnify the Bank, its Certificate issuer and IdenTrust fully against any liability, loss or damage suffered or incurred by any of them, howsoever arising and by whosoever caused, whether arising directly or indirectly, in relation to:
(a) conduct on the part or you, on your behalf or by your Certificate Holders or HSM Contacts resulting in the erroneous issuance of valid Certificate status response being generated with respect to a Certificate registered to you or your Certificate Holders; or
(b) any failure on your part to comply with these PKI Terms and Conditions; or
(c) use of Certificates issued to you or your Certificate Holders with Digital Transmissions or any other messages or communications, sent or generated by you or your Certificate Holders, to persons or entities that are not IdenTrust Participants or their customers; or
(d) 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.

17.2 You will indemnify and continue to indemnify the Bank fully against any liability, loss or damage suffered or incurred by it, howsoever arising and by whomsoever caused, whether arising directly or indirectly from your use and operation of PKI Service, or your access to the PKI Service, except to the extent such liability, loss or damage is due to the wilful acts or negligence of the Bank or otherwise limited by law.

17.3 Subject to the limitation of liability provisions set out in Clause 16 and any relevant terms and conditions applicable to the account or product provided to you by the Bank, 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.

17.4 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 27.3.

**18. Software Licence**

18.1 You are granted a non-exclusive non-transferable licence to use the Software.

18.2 The following terms shall apply to the licence of the Software:
(a) You must and must procure that your Certificate Holders shall:
(i) use Sign Online Smart cards and the Software for the purposes of the PKI Service only;
(ii) install, use and upgrade the Software, or where applicable any Sign Online Smart cards issued, as per the user guide issued by the Bank from time to time;
(iii) where you are provided with an upgrade, as soon as practicable after receipt:
(1) install it on to your computer system;
(2) if instructed to do so by the Bank, stop using the old Software or Sign Online Smart card; and
(3) if instructed to do so by the Bank, destroy the old Software or Sign Online Smart card.
(b) You must not and must procure that your Certificate Holders shall not:
(i) copy, publish, sell, rent, lease, de-compile, reverse engineer or modify the Software (or any part of it);
(ii) make use of any Sign Online Smart card, or the Software, except as expressly permitted by these PKI Terms and Conditions, by law or as agreed in writing by the Bank.
(c) All rights and licences granted to you by this clause 18 shall terminate:
(i) on termination of these PKI Terms and Conditions; or
(ii) on termination of the IdenTrust Specification License Agreement between the Bank and IdenTrust for any reason.

18.3 The following additional terms shall apply to the licence of the Software:
(a) the Bank and you agree and intend that these PKI Terms and Conditions will provide certain rights to the benefit of IdenTrust, and that IdenTrust shall be a deemed third party beneficiary of these PKI Terms and Conditions;
(b) you may use the Software, the Sign Online Smart card or the PKI Service in connection with the use or operation of the IdenTrust Service and for no other purpose;
(c) you shall have no right to assign, sub-license or otherwise transfer any of the rights in the Software without the prior written consent of the Bank and the software developer; and
(d) upon termination of these PKI Terms and Conditions for any reason, you must promptly cease using any IdenTrust Marks and the Software.

**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 PKI Service. Any additional terms relating to such Hardware, or to such technical specification, will be notified to you in accordance with clause 11 (Specification Change Procedure).

**20. Warranties**

20.1 You warrant that any information submitted to the Bank or to their agent, including to any 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 PKI 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 PKI 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 Terms and Conditions.

21.2 You recognise and agree that you have no recourse in this regard to IdenTrust, or any IdenTrust Participant in connection with the PKI 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 fraud, 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 signed with a Digital Signature created with your Private Key(s) (which shall be deemed to include the Private Keys of Certificate Holders and/or relating to Certificates installed on HSMs) and authenticated with your Public Key, for which the corresponding Identity Certificate is confirmed as valid, shall have the same legal effect, validity and enforcement as if the Digital Transmission had been in writing, and signed by you or on your behalf.

22.2 You will not challenge the legal effect, validity or enforceability of a Digital Transmission 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 the Sign Online Smart card supplied or HSMs.

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 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.

**23. Termination**

23.1 The Bank may suspend or terminate your use of the PKI Service, in whole or in part, at any time, with immediate effect without prior notification to you, if it determines that you or any of your HSM Contacts or Certificate Holders have breached any of these PKI Terms and Conditions, or as it sees fit in order to protect the security of the Bank, or of the PKI Service, or otherwise to protect the Bank's interests.

23.2 The Bank may terminate these PKI Terms and Conditions, and/or suspend or terminate your use of the PKI Service, forthwith, by giving notice in writing:
(a) on the occurrence of an Insolvency Event in relation to you; or
(b) If you (or your HSM Contacts or Certificate Holders) are in breach of any provision of these PKI Terms and Conditions; or
(c) if the Bank ceases to offer the PKI Service on a permanent basis.

23.3 Without prejudice to the provisions of 23.1 and 23.2, the Bank may terminate these PKI Terms and Conditions, and/or suspend or terminate your use of the PKI Service, by giving you 30 days' notice in writing.

23.4 You may terminate your use of the PKI Service by giving the Bank 30 days' written notice of termination. Such termination:
(a) will not be effective unless the notice of termination is actually received by the Bank at the address specified in clause 27; and
(b) will take effect from 5pm, London time, on the Business Day after the day on which the Bank actually receives notice of termination; and
(c) will not affect any obligations incurred by you in respect of use of the PKI Service prior to the time at which termination takes effect under paragraph 23.3 (b).

23.5 All monies due and owing to the Bank in connection with the PKI Service, if not already due and payable, will immediately become due and payable upon the date that the Bank actually receives notice of termination.

23.6 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.

23.7 If the Bank receives transactions via the PKI 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.

23.8 Upon termination of these PKI Terms and Conditions by either party:
(a) you will immediately de-install and return (at your cost) the Software, and all materials relating to the Software, to the Bank, and remove all copies of the Software from any computer, server or local area network on which the Software is installed. Any right to use the Software and related components will terminate upon receipt of any termination notice.
(b) you will return all Sign Online Smart card or Smart cards issued to you or the Personnel to the Bank.
(c) you will de-install any Certificates issued by the Bank to you and related Private Keys installed on any HSMs.

23.9 These PKI 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 PKI Service, without the prior written consent of the Bank or its agent as appropriate. Any specifications and documentation relating to the IdenTrust Service shall be deemed to be the Confidential Information of the Bank and accordingly shall be kept strictly confidential by you.

24.2 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 this clause 24.

24.3 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;

(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 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.

24.4 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 PKI Service and who have been made aware of and instructed to observe the terms of this clause 24, save only that that Bank may disclose Confidential Information to its Group Companies, in order to provide or develop the PKI Service.

24.5 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.

24.6 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.

24.7 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.

24.8 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 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.

24.9 Upon the earliest of:
(a) termination of these PKI 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 24.9.

**25. Dispute Resolution Procedures**

25.1 In the event that you wish to complain about any aspect of the PKI Service, you may contact the Bank at the following address:
Customer Assist Team Clydesdale Bank PLC 1st Floor, Guildhall,
57 Queen Street, Glasgow, G1 3ER Telephone: 0800 055 6655
Email: customer.assist@cybg.com
The Bank will use reasonable endeavours to resolve your complaint, in accordance with our complaint handling procedures (as available on the Bank's website or on request, from time to time).
If, after the Bank has issued a final response to your complaint, or after 40 Business Days if the Bank has not been able to issue a final response, you may take a complaint to the Financial Ombudsman at the following address:
Financial Ombudsman Service South Quay Plaza
183 Marsh Wall London E14 9SR
Making a complaint will not prejudice your right to instigate legal proceedings.

25.2 In the event of any dispute solely between you and the Bank, arising out of or in connection with the PKI Service, which we have not resolved in accordance with the complaints handling mechanism set out in clause 25.1, you may instigate legal proceedings against the Bank, subject to restrictions in these PKI Terms and Conditions.

25.3 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.

25.4 You agree that, in the event of any dispute between you and any IdenTrust Participant other than the Bank and/or between you and IdenTrust, or any dispute with the Bank that involves related claims by, or against, other IdenTrust Participants, and/or IdenTrust, which dispute arises out of or in connection with the PKI Service or the IdenTrust Services, shall be finally settled pursuant to the IdenTrust Dispute Resolution Procedures, a copy of which is available on request in accordance with clause 27.

25.5 You expressly consent to being joined as a party to any dispute resolution procedure in respect of disputes provided for under clause 25.2, and in accordance with the IdenTrust Dispute Resolution Procedures.

25.6 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 and will not challenge such determination in any other forum.

**26. Sub – Contractors**

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

**27. Notices**

27.1 Where you are required to give notice or are permitted to make requests to the Bank in accordance with clauses 4, 7, 9, 13 or 25, such notice or permitted request shall be sent to the Bank's Sign Online Support office at:
Sign Online Support
Clydesdale Bank PLC
2nd Floor Payments
Customer Support Centre
40 St Vincent Place Glasgow
G1 2HL

27.2 Notices, certificates, consents, approvals and other communications in connection with these PKI Terms and Conditions must be given in writing, and be signed by one of your Authorised Signatories unless:
(a) otherwise specified in these PKI Terms and Conditions; or
(b) the Bank otherwise determines.

27.3 The Bank is hereby authorised to accept, and act upon on your behalf, any facsimile 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.

27.4 A communication is deemed to be received by you when it is sent by the Bank and is deemed to be effective from that date or the effective date appearing on the communication (if after the date is sent) even if no person is aware of its receipt.

27.5 A communication is deemed to be sent from where the sender has its place of business or last known address. For the purposes of this clause:
(a) if the sender or recipient has more than one place of business, the place of business is the sender's or recipient's principal place of business.
(b) if the sender or recipient does not have a place of business, the place of business is the sender's or recipient's usual place of residence.
(c) the date of receipt of a notice given by you to the Bank is deemed to be the date of actual receipt by the Bank and is deemed to take effect from 5pm on the business day after the date of actual receipt, save for notices under clause 5 and 7.4 relating to the suspension or revocation of Certificates, which shall take effect as set out in those clauses.

**28. Entire agreement and enforceability**

28.1 Your application form (once approved by the Bank), these PKI 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 PKI 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 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 these PKI Terms and Conditions without the prior written consent of the Bank such consent not to be unreasonably withheld or delayed.

29.2 The Bank may assign any of its rights and interests under these PKI Terms and Conditions, without your consent.

29.3 Nothing in these PKI 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 Terms and Conditions including, without limitation, those provisions which provide a benefit to IdenTrust.

**30. Governing law**

30.1 These PKI Terms and Conditions and the transactions contemplated by these PKI Terms and Conditions are governed by and construed in accordance with the law of the country in which the branch of the Bank holding your main business banking connection is situated and each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the courts of that country.

**31. Good Banking**

31.1 We are fully committed to high standards of service, treating our customers fairly, helping our customers understand how their accounts operate and giving them a better understanding of banking services and maintaining confidence in the security and integrity of banks. For further information please refer to our website or contact your branch or Relationship Manager.

**Schedule 1: Support**

The Bank will provide support for the PKI 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 10.2.
In the event that you wish to obtain support, you should contact the Sign Online Support on 0800 077 8040.

**Schedule 2: Minimum Technical Specifications (other than for HSMs)**

Minimum 120 Mb hard disk space free Microsoft Windows 7, 8, 8.1, 10
Internet Explorer IE11 Internet Connection
USB connectivity for Smart Card Reader Computers on which Classic Client is to be installed must have at least: 1 Gigahertz (GHz) processor or faster for 32-bit or 64-bit versions of Windows 1 GB of RAM for 32-bit versions of Windows 2 GB of RAM for 64-bit versions of Windows
In addition, each user workstation must have at least 120 MB of available hard disk space for eSigner to operate correctly

**Schedule 3: Minimum Technical Specifications for HSMs**

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).

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

cbonline.co.uk | ybonline.co.uk



DU591 (02/18)