COMMERCIAL BANKING

Digital Identification Service

PKI Customer Agreement
Corporate Online Version
Unincorporated (including charities)
Partnerships (Scottish and English)
Limited Company/Public Limited Companies
Local Authorities
Limited Liability Partnerships
Sole Traders

BANK OF SCOTLAND

Contents

1. Definitions 1
2. Duration 2
3. Terms of use of the Digital Identification Service 2
4. Customer Obligations 3
5. Bank Obligations 3
6. Use of software with the Digital Identification Service 4
7. Confidentiality 4
8. Intellectual Property Rights 4
9. Policies and Procedures 4
10. Legal Effect 5
11. Recourse 5
12. Consent to Transfer of Information 5
13. Indemnity 5
14. Dispute Resolution 5
15. Acceptance 5
16. Compliance with Laws and Regulations 5
17. Digital Identification Service Fee 5
18. Termination 5
19. Consequence of Termination 5
20. Changes to this Agreement 5
21. The Bank's Right of Access 6
22. Assignment 6
23. Entire Agreement 6
24. Notices 6
25. Customer's Group 6
26. Law 6

The Schedule 7

1. Definitions

"**Additional Contact**" means an employee or agent of the Customer who has authority from the Customer to access and use the Digital Identification Service but who may not set up other Additional Contacts.

"**Additional Terms**" means those separate terms and conditions relating to products or services provided or supplied by the Bank or any Member of the Bank Group for use with the Digital Identification Service.

"**Agreement**", "**Customer Agreement**" or "**PKI Customer Agreement**" means this agreement and its schedule, as amended from time to time and any other documents generated in accordance with this Agreement or incorporated by reference.

"**Authenticated**" means that the Digital Signature in a Digital Transmission has been created with the Private Key associated with the Public Key contained within the Certificate presented as part of the Digital Signature.

"**Authorised User(s)**" means employees or agents of the Customer authorised by the Customer to access and use the Digital Identification Service.

"**Bank**" means Bank of Scotland plc, a company registered in Scotland with registered No. SC327000 and having its Registered Office at The Mound, Edinburgh EH1 1YZ.

"**Bank Group**" means: (a) the Bank; (b) any direct or indirect Subsidiary of the Bank; (c) any direct or indirect holding company of the Bank from time to time; and (d) any direct or indirect Subsidiary of any such holding company from time to time (the term "holding company" being defined in accordance with Section 1159 of the Companies Act 2006).

"**CA Certificate**" means a Certificate corresponding to the Private Key used by a Certificate Authority to digitally sign the Certificates it generates.

"**Certificate**" means an X509 v3 compliant, digitally signed data structure which immutably binds a Public Key to information uniquely identifying the possessor of the Private Key corresponding to the Public Key.

"**Certificate Authority**" means an authority trusted by one or more Participants to generate and assign Certificates.

"**Certificate Chain**" means a sequence of Certificates, together with the CA Certificate of the Certificate Authority who issued that Identity Certificate, plus the CA Certificates of any other Certificate Authority directly above it in Public Key Infrastructure hierarchy, up to the CA Certificate of the Root Certificate Authority of that Public Key Infrastructure.

"**Certificate Policy**" means a document that sets out the broad policy constraints imposed by a Certificate Authority on the operational use of Certificates issued within its Public Key Infrastructure.

"**Certificate Status Check**" means the process of checking the Validity of an Identity Certificate by issuing a Certificate Status Check.

"**Certificate Status Request**" means a Digital Transmission that requests confirmation of the status of an Identity Certificate included in a Digital Transmission as a Valid Certificate.

"**Certificate Status Response**" means a Digital Transmission transmitted by a Certificate Authority in response to a Certificate Status Request.

"**Commencement Date**" means the date the Customer first accesses or uses the Digital Identification Service.

"**Customer**" means the company, individual or other entity with whom the Bank is contracting under the terms of this Agreement, as identified in the application form submitted by the company, individual or other entity concerned.

"**Customer's Group**" shall mean the Customer and any Subsidiary as may be agreed with the Bank from time to time.

"**Digital Identification Service**" (which may also be referred to as the "HBOS Digital Identification Service") means the access and use of the Public Key Infrastructure using the Software, Hardware and Smart Cards and/or HSM(s) as further described in the Schedule.

"**Digital Signature**" means 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. A Digital Signature employs 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 electronic message in digital form sent within the IdenTrust System containing data, which a customer, a Participant, or IdenTrust Authenticates with a Digital Signature.

"**Dispute Resolution**" means the procedure to be used by parties in the event of a dispute. This process is set out in the document entitled "Dispute Resolution Procedure" which may be amended by the Bank from time to time.

"**FIPS 140-2**" means The Federal Information Processing Standards publication 140-2 "Security Requirements for Cryptographic Modules". Security level 2 requires that the cryptographic module is tamper evident and that tamper evident locks or seals must be broken to attain physical access to cryptographic keys. Security level 3 requires that in addition to being tamper evident, the cryptographic module is tamper proof using such mechanisms as deleting all cryptographic material if the cover or doors of the cryptographic module are opened. More information on FIPS 140-2 can be found at: **www.itl.nist.gov/fipspubs/**

"**Hardware**" means the Smart Cards and Smart Card Readers provided by the Bank to the Customer under the terms of this Agreement.

"**Helpdesk**" means the helpdesk provided specifically for Customers to report loss of Smart Cards and compromise or suspected compromise of Smart Cards and Private Keys. The Helpdesk is available by telephone between the hours of 7:30am and 6:00pm Monday to Friday, except Bank Holidays.

"**HSM**" means BACS-specific hardware security module used with the Digital Identification Service in accordance with the terms of this Agreement.

"**HSM Minimum Standards**" means the HSM technical specifications, security requirements and operating models issued to the Customer in writing from time to time.

"**Identity Certificate**" means a Certificate issued by a Participant to a Customer that can be used by Relying Customers to check the Validity of that Customer's Digital Signatures.

"**Identity Key**" means the unique Private Key(s) issued by the Bank to the Customer under the Identity Certificate policy issued by the Bank which are used by the Customer to create Digital Signatures.

"**IdenTrust**" means IdenTrust, Inc, a Delaware limited liability company and ultimate owner of the IdenTrust System.

"**IdenTrust Root Validation Authority**" means the IdenTrust System component hosted by IdenTrust that responds to Certificate Status Checks on Participants' Certificates.

"**IdenTrust System**" means the computer network, communications and other systems operated by or on behalf of IdenTrust and Participants through which Participants and IdenTrust communicate and offer the Digital Identification Services.

"**ITSEC**" means "The Information Security Evaluation Criteria" issued by the European Commission. An ITSEC rating of E4 High gives the maximum assurance from security engineering based on rigorous commercial development practices. More information on ITSEC can be found at **www.cesg.gov.uk**

"**Key Manager**" the role holding overall responsibility for key management operations within the HSM-owning organisation.

"**Key Management**" the policies, procedures and technical controls concerned with ensuring the security of cryptographic keys.

"**Key Pair**" means an entity's Private Key and the corresponding Public Key.

"**Nominated Representative**" means employees and agents of the Customer who have been authorised by the Customer to request the Bank to grant or revoke access to the Digital Identification Service to the Customer's Authorised Users.

"**Participants**" means an entity: (a) that has entered into a signed agreement for Participants with IdenTrust and (b) acts as a Certificate Authority and (c) provides Certificate Status information to its Relying Customers and other Participants. The Bank is a "Participant" by virtue of it being the successor entity to the Governor and Company of The Bank of Scotland.

"**PIN**" means personal identity number used to access the Digital Identification Service in conjunction with the Smart Card.

"**Private Key**" means that key of an entity's asymmetric key pair that shall normally be available for use only to that entity. A Private Key is one-half of a cryptographic Key Pair as drawn from the class of asymmetric key cryptographic functions used in the IdenTrust System that IdenTrust, a Participant or a Customer may apply to electronic transmissions, messages or records for identification and communication purposes, including to place a Digital Signature on a Digital Transmission. Customer and Participant Private Keys are a minimum of 1024 bits long and the IdenTrust Private Key is 2048 bits long.

"**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 the IdenTrust System that is uniquely related to the Private Key of IdenTrust, a Participant, or a Customer.

"**Public Key Infrastructure**" means a structure of hardware, software, people, processes and policies that employs Digital Signature technology to facilitate a verifiable association between the public component of an asymmetric Key Pair with a specific subscriber that possesses the corresponding Private Key. The Public Key may be provided for Digital Signature verification, Authentication of the subject in communication dialogues, and/or for message encryption key exchange or negotiation.

"**Relying Customer**" means a Customer that makes Certificate Status Requests to its Participant.

"**Revoke**" means with respect to a Certificate that its Certificate Authority, or IdenTrust, designates it, with immediate and irrevocable effect, as not Valid. When a Certificate has been Revoked its status is "Revoked".

"**Root Certificate Authority**" means a Certificate Authority at the apex of a hierarchy of Certificate Authorities that has signed its own Certificates. The IdenTrust Root Certificate Authority is the Root Certificate Authority in the IdenTrust System.

"**Signatory**" means a party that has agreed to be bound by contract with IdenTrust in order to perform the functions of a Participant in the IdenTrust System.

"**Smart Card**" means a card containing a computer chip that has been certified by a body independent of the Smart Card manufacturer and the Bank as meeting the security standard ITSEC E4 High.

"**Smart Card Reader**" means a hardware device that provides an interface between the Smart Card and the Software.

"**Software**" means the drivers and utilities provided by the Bank for use in relation to the Digital Identification Service that enable the Customer to sign electronic data using the Private Identity Key stored in their Smart Card, and to perform various administrative and diagnostic functions with respect to the Smart Card and Smart Card Reader.

"**Subscribing Customer**" means a Customer that obtains a Certificate from an issuing Participant for use in connection with the IdenTrust System.

"**Subsidiary**" shall have the meaning specified in section 1159 of the Companies Act 2006.

"**Suspend**" means with respect to a Digital Certificate, that its Certificate Authority, or IdenTrust designates it, with immediate, but revocable, effect as not Valid. When a Certificate has been Suspended its status is "Suspended".

"**Utility Certificate**" means a Certificate issued by a Participant to a Customer that can be used by the Customer to facilitate the confidentiality and integrity of Digital Transmissions.

"**Utility Key**" means the unique Private Key(s) issued by the Bank to the Customer under the Utility Certificate policy issued by the Bank which may be used by the Customer for data encryption and key exchange.

"**Valid**" means with respect to a Certificate that it is not known to have been Revoked or Suspended and, if the Relying Customer has already properly Authenticated the corresponding Digital Signature and the accompanying Certificate Chain, they can gain complete assurance that:

a. The Digital Transmission associated with the Digital Signature has not been altered since the Digital Signature was created;

b. The Private Key used to create the Digital Signature has been issued by a Participant to the entity named in the Certificate;

c. The Private Key used to create the Digital Signature has not been reported to the Participant as lost, stolen or otherwise compromised in such a way as to cause the Participant to Revoke or Suspend the corresponding Certificate in accordance with the policies set out in the Certificate Policy under which the Certificate was issued;

d. The Participant that issued the Certificate is a member of IdenTrust;

e. The Participant's Private Key has not been reported to IdenTrust as compromised.

"**X.509 v3**" means the Public Key Infrastructure standards developed by ISO/IEC/ITU and published by the Internet Society in RFC 3280. More information on RFC 3280 can be found at: **www.ietf.org/rfc**

1.1 In this Agreement:

a. references to any statute or regulation shall include references to such statute or regulation as amended, extended or consolidated or made from time to time;

b. any use of the word "including" shall be treated as "including without limitation";

c. where the Customer enters into this Agreement for the benefit of the Customer's Group then any reference to the Customer shall be deemed also a reference to the Customer's Group unless otherwise specified in this Agreement.

2. Duration

The Bank shall provide, or procure the provision of, the Digital Identification Service from the Commencement Date to the Customer until terminated under the terms of this Agreement.

3. Terms of use of the Digital Identification Service

3.1 In order to access and use the Digital Identification Service the Customer shall appoint Authorised Users who will be entitled to act on the Customer's behalf in relation to any matter concerning the Digital Identification Service. Nominated Representatives shall be nominated to the Bank by the Customer in writing. The Customer shall provide the Bank with a specimen signature for each of its Nominated Representatives. Upon a signed request from a Nominated Representative the Bank shall issue an Authorised User with a PIN and a Smart Card upon the Bank accepting the Customer as being a suitable user for the Digital Identification Service and the registration process being fully completed. Upon registration the Bank shall allow the Authorised User access and use of the Digital Identification Service. A Nominated Representative may act as an Authorised User of the Digital Identification Service.

3.2 The Authorised Users may use Smart Cards to sign electronically data and other communications; to encrypt data and other communications; decrypt data and other communications and validate and authenticate Digital Signatures used to sign data and/or other communications. The Customer may use HSM(s) as an alternative method to using Smart Cards, Smart Card Readers and Software to access and use the Digital Identification Service. The Customer may use as a back up the Software, Smart Cards and Smart Cards Readers together with the Digital Identification Service. Where the Customer has opted to use HSM(s), the registration process shall also require the Customer to provide an Additional Contact for each HSM they intend to utilise.

3.3 Each Authorised User, Nominated Representative and Additional Contact must at all times be employed by the Customer under a contract of employment or under contract. Each Authorised User and Additional Contact shall be duly authorised by the Customer

through the Nominated Representative to access and use the Digital Identification Service. If at any time, an Authorised User, Nominated Representative or Additional Contact shall cease to be employed by the Customer under a contract of employment or under a contract or has their authority revoked by the Customer, the Customer must immediately notify the Bank and the Bank shall then revoke the Certificates or PIN issued to such user in order to terminate their access to the Digital Identification Service. The Smart Card issued to that Authorised User or Nominated Representative shall be destroyed by the Customer.

3.4 The Digital Identification Service is provided solely for the Customer's own business use (including use by Authorised Users and/or Additional Contacts) and the Customer will not sell or attempt to sell or transfer the Digital Identification Service (or any part or facility of it) to any third party.

3.5 The Digital Identification Service must not be used by the Customer or any Authorised user in a way that does not comply with:

a. the terms of any legislation or any licence which applies to the Customer;

b. any instructions or requirements given to it by the Bank; or

c. any transaction for which the Customer is not acting either as principal or as agent for a principal that has been disclosed to the Bank.

3.6 The Digital Identification Service must not be used by the Customer or any Authorised User:

a. fraudulently, in connection with a criminal offence, or otherwise unlawfully;

b. to send, receive or use any information or material which is offensive, abusive, indecent, defamatory, obscene or menacing or in breach of confidence, copyright, piracy or any other rights.

3.7 Certificates issued as part of the Digital Identification Service must only be used with services or products supplied or approved by the Bank or by any member of the Bank Group and not for any other purpose.

3.8 If the Customer, Authorised User or Additional Contact or anyone else with or without the Customer's knowledge or approval uses the Digital Identification Service in contravention of clause 3.5, 3.6 or 3.7 the Bank may treat such contravention as a material violation or breach of this Agreement which cannot be cured.

3.9 If the Customer chooses to use the Digital Identification Services outwith the UK they shall comply with any relevant laws and regulations relating to the relevant jurisdiction in which the Digital Identification Service is used. In particular, the Customer accepts that there may be export and import laws with regard to export and import of the Digital Identification Service and that it is the Customer's responsibility to ensure compliance with such laws or regulations. The Bank cannot accept responsibility for complying with such laws and regulations and shall not be liable for any failure on the part of the Customer to observe these laws or regulations.

4. Customer Obligations

4.1 The Customer shall:

4.1.1 supply such information or data as may be required by the Bank from time to time and complete fully any documentation required by the Bank;

4.1.2 notify the Bank of named Authorised Users through the Nominated Representatives and request Smart Cards and PINs for these Authorised Users;

4.1.3 provide Smart Cards and PINs only to named Authorised Users for the duration of their employment or engagement and for the duration of this Agreement;

4.1.4 ensure that Authorised Users who are in receipt of Smart Cards and PINs and users of HSM(s) are aware of and comply with the security arrangements and confidentiality restrictions detailed in this Agreement;

4.1.5 be responsible for the security and proper use of all Smart Cards, PINs and HSM(s) used in connection with the Digital Identification Service and take all necessary steps to ensure that they are kept securely;

4.1.6 immediately inform the Bank if compromise, or suspected compromise, of its Private Key(s) occurs. Compromise shall include the following:

a. the Smart Card containing the Private Key is no longer under the control of the Authorised User to whom the Smart Card was issued;

b. the Customer has reason to believe the PIN is known or is likely to have become known to a party other than the Authorised User to whom the Smart Card was issued.

4.1.7 immediately advise the Bank of information relating to (i) any changes to the ongoing validity and/or accuracy of its Certificate(s), Public Key and/or Private Key or information given during the registration process, or (ii) any compromise or suspected compromise of the security of the computer on which the Software has been installed or Smart Card(s) or (iii) any compromise or suspected compromise of the security of the HSM(s). The Customer must report such events to the Helpdesk.

4.2 Where the Customer uses HSM(s), the Customer shall comply with the Key Management standards as defined in the HSM Minimum Standards for Digital Identity Customers and shall review Key Management procedures on a regular basis updating them as necessary.

4.3 The Customer shall comply with such directions, instructions, policies and procedures in relation to the Digital Identification Service as may be issued by the Bank from time to time and, if appropriate, shall comply in particular with the HSM Minimum Standards for Digital Identity Customers.

4.4 The Customer shall appoint a Key Manager for the duration of this Agreement and advise details of the Key Manager to the Bank. This will form part of the Customer registration process.

4.5 The Customer shall ensure that adequate business continuity processes are developed and maintained.

4.6 Except for the Software and Hardware provided by the Bank, the Customer is responsible for providing suitable computer hardware, software and telecommunications equipment to access and use the Digital Identification Service. In particular, where the Customer intends on using HSM(s), the HSM(s) shall be obtained by the Customer from third party service providers. The Customer, or in conjunction with its third party service provider, shall prepare, install, configure and test and ensure that the HSM(s) are ready to communicate with the Digital Identification Service. The Customer shall be responsible for all Key Management functions required to be performed on the HSM(s).

4.7 The HSM(s) shall meet the criteria set out within the HSM Minimum Standards for Digital Identity Customers.

4.8 The Customer is responsible for the acts and omissions of all its Authorised Users, Nominated Representatives and Additional Contacts in connection with the Digital Identification Service and liable for any failure by any of its Authorised User(s), Nominated Representatives and Additional Contacts to observe the terms and conditions of this Agreement.

4.9 The Customer warrants the accuracy of any information submitted to the Bank and contents of its Certificate(s).

4.10 The Customer shall ensure that the new Authorised User signs an appropriate declaration concerning the use of data relating to them.

5. Bank Obligations

5.1 The Bank shall, or shall procure that another member of the Bank Group shall, subject to these terms and conditions:

a. provide the Digital Identification Service in accordance with the Certificate Policies;

b. provide the Digital Identification Service with the reasonable skill and care of a competent provider of similar services;

c. accept the authority of the Customer's Nominated Representative to nominate Authorised Users;

d. provide the Helpdesk facility;

e. email the Authorised User with the contents of their Identity Certificate;

f. for Smart Card users, supply copies of the Software as required by the Customer but not more than one copy of the Software per Smart Card;

g. for Smart Card users, supply Hardware as required by the Customer;

h. for Smart Card users, generate and deliver all required Key Pairs and Certificates in a manner compliant with the requirements of the relevant Certificate Policies;

i. email the Authorised User regarding Certificate expiry;

j. verify the signature of the Nominated Representative before fulfilling a request for Smart Cards and PINs for Authorised Users.

5.2 It is technically impracticable to provide a fault free Digital Identification Service and the Bank does not undertake to do so. The Bank will, however, repair any reported faults as soon as it reasonably can.

5.3 Occasionally, the Bank may:

a. change the technical specification of the Digital Identification Service though the Bank will try to give as much notice as possible of any changes that affect the Customer;

b. suspend the Digital Identification Service for operational reasons such as repair, maintenance or improvement of the Digital Identification Service or because of an emergency. The Bank will provide as much on-line, written or oral notice as is reasonably possible and will restore the Digital Identification Service as soon as it reasonably can.

5.4 The Bank reserves the right to decline the issue of Certificates.

5.5 The Bank shall not be obliged to provide Helpdesk facility in relation to:

a. improper use, operation or neglect of Hardware or Software;

b. use of the Hardware or Software for purposes for which it was not designed;

c. any repair, alteration or modification of the Hardware or Software by any person other than the Bank or a Bank agent;

d. any unforeseen impact on the existing applications on your computer system;

e. any software or hardware supplied by a third party;

f. the introduction of any virus or other malicious code.

6. Use of software with the Digital Identification Service

6.1 In the event the Customer wish to use any software (other than the Software) in relation to the Digital Identification Service the prior written consent of the Bank is required.

6.2 The Customer agrees to immediately install and use any upgrades or replacements to the Hardware and/or Software as may be made available from time to time.

7. Confidentiality

Each party shall treat as confidential all information obtained from the other pursuant to this Agreement and shall use it only for the purposes of this Agreement and shall not without prior written consent of the other divulge such information except to:

a. the receiving party's own employees, directors and officers including Authorised Users and/or Additional Contacts and only to those employees (including agents and contractors) who need to know the same;

b. members of the Bank Group;

c. the receiving party's auditors, professional advisers, any regulatory authority, HM Inspector of Taxes, HM Customs & Excise and any other bodies having a statutory or regulatory right to receive that information or to whom the receiving party has a statutory or regulatory obligation to disclose that information and then only in pursuance of and to the extent of such right or obligation.

Provided that this clause shall not extend to information which was rightfully in the possession of either party prior to the date of this Agreement, which is already public knowledge or which becomes so at a future date (otherwise than as a result of breach of this clause) or which is trivial or obvious. This clause shall not apply to the Certificates, Public Keys and Certificate Status.

8. Intellectual Property Rights

8.1 For the duration of this Agreement the Bank grants the Customer a non-exclusive non-transferable licence to use the Software. The Customer shall not, without the Bank's prior written consent, copy or (except as permitted by law) decompile or modify the Software, nor copy the manuals or documentation.

8.2 The Customer shall not without the Bank's prior written consent, modify or take apart the Hardware.

8.3 All Software, Hardware and facilities provided by the Bank to the Customer under this Agreement are and shall remain the property of the Bank or its agents.

8.4 The Customer acknowledges that it does not own or claim any right of copyright or other intellectual property rights in the Software, Hardware, Certificates, PIN or any other documentation or information supplied by the Bank.

8.5 The Customer agrees that it will not use any trademarks, tradenames, logos or other intellectual property rights belonging to or used by the Bank or the Bank Group or IdenTrust without the prior written consent of the Bank.

9. Policies and Procedures

9.1 The Customer shall comply with the following policies and procedures:

a. by requesting the Bank to issue it a Smart Card, the Customer is authorising the Bank to securely generate two Private Keys – the Identity Key and Utility Key to certify the corresponding Public Keys and deliver above keys and Certificates to the Customer on the Smart Card;

b. the Customer's Certificates and Smart Card(s) will be valid for a maximum of four years from the date of issue, after which time they will expire and must no longer be used. The date of expiry of the Customer's Certificates and Smart Card is printed on the Smart Card;

c. by requesting the Bank to issue it an HSM Certificate, the Customer is authorising the Bank to deliver Certificates to the Customer. Such Certificates will be valid for a maximum of four years from the date of issue, after which they will expire and must no longer be used.

9.2 The Customer agrees that they shall inform the Bank promptly of any of the following occurring:

a. The Customer's Private Keys have been, or are suspected of being, compromised as specified in clause 4.1.6;

b. The Authorised User to whom the Smart Card and Certificates have been issued, is no longer an employee or agent of the Customer;

c. The PIN has been entered incorrectly five (5) consecutive times, causing the Smart Card to be irreversibly disabled; or

d. The Smart Card has ceased to function.

In such circumstances the Bank shall Revoke, or at the Bank's discretion Suspend, the relevant Customer Certificates. The Bank may Suspend rather than Revoke the Certificate if the Bank decides there is a reasonable doubt as to whether the Customers Private Key has been compromised.

9.3 Where the Bank has opted to Suspend a Customer's Certificate on the circumstances detailed above, the Customer shall have a period of sixty (60) days during which they may request the Bank to remove Suspension of their Certificate if the circumstances which caused the Certificate's Suspension no longer apply. The Bank reserves the right to withhold removal of Suspension of the Customer's Certificate(s). On the sixty first (61) day of Certificate Suspension the Bank shall Revoke the Suspended Certificate. The Bank reserves the right to Revoke or Suspend a Customer's Certificate at any time for any reason and where such Revocation or Suspension takes place the Customer may terminate this Agreement immediately.

9.4 In the event that a Customer's Smart Card and the Certificates therein, expire or are Revoked, or the Smart Card becomes inoperable, the Customer shall destroy the Smart Card. The Customer acknowledges that Certificate Policies and Dispute Resolution Procedures documentation has been provided.

10. Legal Effect

10.1 The Customer agrees that: (a) all Digital Transmissions signed with a Digital Signature created with any Customer's Private Key, and Authenticated with the Customer's Public Key, for which the corresponding Identity Certificate is confirmed as valid through the Digital Identification Service, shall have the same legal effect, validity and enforceability as if the content of the Digital Transmission had been in writing manually signed by that Customer, and (b) the Customer shall not challenge the legal effect, validity or enforceability of a Digital Transmission or a Digital Signature on the ground that it is in digital rather than written form.

10.2 This Agreement shall be enforceable notwithstanding any change in the name of the Customer or any change in the constitution of the Customer or its successors or by the amalgamation with any third party.

11. Recourse

The Customer agrees that its only recourse in connection with the Digital Identification Service, including with respect to claims arising out of the negligence of any party, is to the Bank only and to the extent provided for in this Agreement. The Customer expressly recognises and agrees that it has no recourse in this regard to IdenTrust, a Signatory or any other party in connection with the Digital Identification Service, but may have recourse or liability under applicable law to another customer that is the counter-party with respect to a Digital Transmission sent or received by the Customer. This clause shall not be construed, however, to exclude liability for gross negligence or wilful misconduct. Neither the Bank nor its agents are responsible for any liabilities arising directly or indirectly from use and management of HSM(s) owned by the Customer.

12. Consent to Transfer of Information

The Customer acknowledges and authorises that the Bank, Signatories, IdenTrust, and their employees and agents may, within the limits of applicable law, transmit and receive any data or information about, regarding or involving the Customer and its Authorised Users and Additional Contacts among and between themselves and other third parties: (a) to provide the Digital Identification Service to the Customer; (b) to resolve any dispute arising from the Digital Identification Service; or (c) pursuant to applicable law. The Bank shall not use such data or information for any other purpose. In the event applicable law requires the written consent of any of its Authorised Users and Additional Contacts to such use, the Customer shall do so. The Customer accepts that its Certificates may be published in the Bank directory service that may be made available to other customers within the IdenTrust scheme.

13. Indemnity

13.1 The Customer shall indemnify the Bank, and each Bank Group entity, for any liability which the Bank, and any Bank Group entity, may incur resulting from the Customer's (a) conduct, resulting in the erroneous issue of a Valid Certificate Status Response with respect to a Certificate registered to the Customer, (b) failure to comply with the terms and conditions of this Customer Agreement, (c) use of its Certificates with Digital Transmissions or any other electronic messages or communications sent to persons or entities that are not customers of a participant in the IdenTrust System.

13.2 The Bank accepts unlimited liability for death or personal injury resulting from its negligence and clause 13.4 shall not apply to such liability. Further, nothing in this Agreement or the Additional Terms shall exclude or restrict either party's liability for fraud or fraudulent misrepresentation.

13.3 Neither the Bank, nor any Bank Group entity, shall be liable to the Customer, either in contract, tort (including negligence) or otherwise for direct or indirect loss of profits, business or anticipated savings, nor for any indirect or consequential loss or damage including delays or for any destruction of data.

13.4 Except in the case of any liability which arises under clause 13.2, the Bank's liability to the Customer in contract, delict (including negligence) or otherwise in relation to this Agreement is limited to the total amount specified in the Additional Terms.

13.5 The Customer agrees that any loss or damage suffered by any member of the Customer's Group as a result of any breach or default by the Bank of its obligations under this Agreement shall be deemed to be loss or damage suffered by the Customer with the intent that the Bank shall be liable to the Customer rather than to the Customer's Group in respect of that loss or damage. In this regard, the Customer shall act as agent for and on behalf of the Customer's Group.

13.6 Each provision of this Agreement, excluding or limiting liability, operates separately. If any part is held by a court to be unreasonable or inapplicable, the other parts shall continue to apply.

14. Dispute Resolution

The Dispute Resolution Procedures document shall apply.

15. Acceptance

The Customer agrees that its use of a Private Key shall be deemed to be an acceptance of the related Digital Certificate and the terms and conditions of the Certificate Policies as well as the terms and conditions of this Agreement. The Bank shall be entitled to act on any instruction received which has been signed by Authorised Users or Nominated Representatives or otherwise reasonably appears to have been sent by the Customer. The Bank may refuse to carry out an instruction if the Bank reasonably believes that the instruction is invalid; has not come from the Customer or carrying out the instruction would result in breach of this Agreement

16. Compliance with Laws and Regulations

Both parties shall comply with all applicable laws and regulations.

17. Digital Identification Service Fee

A fee is not currently charged for the Digital Identification Service but the Bank reserves the right at any time to charge a fee plus VAT to the Customer. The Bank may advise of any future fees by giving the Customer not less than 28 (twenty eight) days prior written notice.

18. Termination

18.1 The Bank may terminate this Agreement or cease to provide the Digital Identification Service to the Customer:

a. on twenty eight (28) business days prior written notice; or

b. with immediate effect in any of the following circumstances:

i. if IdenTrust has suspended or withdrawn its authorisation for the Digital Identification Service;

ii. where the Bank considers it appropriate to do so in order to protect the security, integrity or reputation of the Digital Identification Service; or

iii. where the Customer is in breach of any provision of this Agreement; or

iv. if the Customer becomes insolvent or bankrupt; or

v. in the event of force majeure.

A party may not terminate for its own breach.

18.2 Termination under this paragraph is without prejudice to any rights that may have accrued to either party before termination.

18.3 If the Bank delays in acting upon a breach of this Agreement that delay will not be regarded as a waiver of that breach.

18.4 The Customer may terminate this Agreement upon 28 (twenty eight) days prior written notice.

19. Consequence of Termination

19.1 Upon termination of this Agreement the Customer shall promptly destroy the Software and Hardware, PINs and any data or information belonging to the Bank.

19.2 The provisions of clauses 7, 8, 12, 13 and 14 shall survive termination of this Agreement.

20. Changes to this Agreement

The Bank may change the terms and conditions of this Agreement at any time on ninety (90) days' notice to the Customer. The parties agree that the consent of any Subsidiary Companies who may be party to this Agreement is not required.

21. The Bank's Right of Access

Without prejudice to any other provision of this Agreement, the Bank (and/or its agents) shall throughout the term of this Agreement have the right at all reasonable times and on giving a minimum of 48 hours' notice to enter upon the premises of the Customer and to be provided with access to all information, documents, plans relating to performance of the Customer's obligations under this Agreement and in particular access to the Customer's Key Management. Additionally the Customer will give the Bank (and/or its agents) all reasonable assistance to interpret such information, documents, plans including access to personnel working with matters referred to in this Agreement.

22. Assignment

The Customer may not assign or transfer any of its rights or obligations under this Agreement, without the written consent of the Bank (the Bank shall not unreasonably withhold consent), except that the Bank may assign its rights or obligations (or both) to a Bank Group company without consent.

23. Entire Agreement

This Agreement and the Additional Terms contain the whole agreement between the parties and supersedes all previous written or oral agreements relating to its subject matter.

24. Notices

The Customer must notify the Bank of current email address of Nominated Representative to whom notices will be sent. Notices given under this Agreement may be delivered by email or in writing. A notice from the Bank which is sent by email to the Customer's email address will be deemed effective three (3) days after the date it is sent. A notice from the Customer to the Bank will be deemed effective when received by the Bank at the email address notified by the Bank to the Customer. Notices may also be given under this Agreement in writing and delivered by hand, or sent by prepaid post, as follows: (a) to the Bank; (b) to the Customer's address detailed at the beginning of this Agreement or any other address that the Customer may notify the Bank from time to time.

25. Customer's Group

25.1 The Customer warrants that it has full power and authority to enter into this Agreement on its own behalf and on behalf of and for the benefit of the Customer's Group. In this regard, the parties agree that the obligations that the Customer has to the Bank under this Agreement shall also be construed as obligations that the Customer's Group have to the Bank.

25.2 The Customer shall be responsible for ensuring that members of the Customer's Group taking the benefit of this Agreement comply with any obligations that apply to them under this Agreement.

25.3 Any loss or damage suffered by any member of the Customer's Group as a result of any breach or default by the Bank shall be deemed to be loss or damage suffered by the Customer with the intent that the Bank shall be liable to the Customer rather than the relevant member of the Customer's Group.

25.4 Nothing in this Agreement shall be deemed to entitle the Customer to recover twice in respect of the same loss.

26. Law

This Agreement will be governed by and construed according to English law and you submit to the exclusive jurisdiction of those courts, unless your Registered Office is situated in, or your central management and control is exercised from Scotland, in which case it will be governed by and construed according to Scottish law and you prorogate the jurisdiction of those courts.

The Schedule

Description of the Digital Identification Service

1. The Digital Identification Service consists of:

a. The Certificate Authority, which issues Certificates to Customers;

b. The Validation Authority, which gives Certificate Status Responses to Certificate Status Checks, made on Bank issued Certificates by Customers or other IdenTrust Participants;

c. Identity and Utility Certificates;

d. *See note 1. Key Pairs (Private and Public Keys);

e. Smart Cards, which hold Customers' Private Keys and Certificates;

f. Smart Card Readers and Software, which in conjunction with the Smart Cards allow Customers to generate Digital Signatures on electronic data.

The Digital Identification Service is part of the IdenTrust System, which provides Certification and Validation Digital Identification Services to IdenTrust Participants.

Note 1: For Customers requiring to use their own HSM(s) as the security storage device for Private Signing Keys, Key Pairs will be considered to fall outwith the Digital Identification Service.

For this service, Key Management will be the responsibility of the Customer.

2. The Smart Card

Every Smart Card issued under this Agreement will be issued with and will store the following digital information:

a. The Authorised User's Identity and Utility Key Pairs;

b. The Authorised User's Identity and Utility Certificates certified by the Certificate Authority;

c. The Certificate Authority Identity and Utility Certificates certified by the IdenTrust Root Certificate Authority;

d. The IdenTrust Root Certificate Authority Certificate, which is self-certified and is the base of the Certificate Chain used to validate Digital Signatures created with the Smart Card.

During Smart Card manufacture the Private Key is never held outside of the Smart Card in unencrypted form, and after the Private key is injected into the Smart Card, any encrypted copy of the key external to the Smart Card is destroyed.

During the Smart Card's operation Private Keys never leave the Smart Card and all encryption operations are performed on board the Smart Card.

3. The Private Identity Key

The Private Identity Key stored on the Smart Card is used by the Authorised User to create Digital Signatures. Its value is not known to the Bank, and the Smart Card contains the only copy of the key within the Certificate Authority's sphere of operation.

Every signing operation using the Private Identity Key requires the Authorised User to enter their PIN using the Software provided.

4. The Software

The Software provides the following functions:

a. It requires the Authorised User to change their PIN the first time they use their Smart Card;

b. It requires the Authorised User to sign data with the assurance that the data they see displayed by the Software is the data they are signing;

c. It provides diagnostic functions, which the Bank or its agent may ask the Authorised User to use to diagnose problems with Smart Cards or Smart Card Readers.

5. Validation and Digital Identification Services

The Bank and IdenTrust require that any entity relying (the Relying Customer) on a Digital Signature created with a Private Identity Key certified by the Certificate Authority must:

a. Have signed a Customer Agreement with an IdenTrust Participant;

b. Check the Certificate Chain presented in the Digital Signature and the value of the Digital Signature to ensure that the data that has been signed has not been altered since it was signed, and that the Key Pair of the signer of the data has been certified by an IdenTrust Participant, and that their Certificate has not expired;

c. Make a Certificate Status Check on the Identity Certificate and Certificate Authority Identity Certificate to ensure that both are still Valid;

d. Certificate Status Checks are made to the Relying Customer's Participant. The Relying Customer's Participant will make a Certificate Status Check on:

   i. The Identity Certificate to the Digital Identification Service;

   ii. The Certificate Authority Identity Certificate to the IdenTrust Root Validation Service.

The Digital Identification Service will only accept Certificate Status Checks made by Customers whose Certificates are Valid, and IdenTrust Participants whose Certificates are Valid.

If a Certificate Status Check is made on a Revoked Certificate, the Digital Identification Service will not provide the reason for Revocation in the Certificate Status Response.

All Certificate Status Checks are Digitally Signed by the entity making the check and all Certificate Status Replies are Digitally Signed by the entity making the reply.

Our Service Promise

If you experience a problem, we will always try to resolve it as quickly as possile. Please bring it to the attention of any member of staff. Our complaints procedures are published at **bankofscotlandbusiness.co.uk/contactus**

Please contact us if you'd like this information in an alternative format such as Braille, large print or audio.

If you have a hearing or speech impairment you can use Text Relay (previously Typetalk).

BANK OF SCOTLAND

PM0241 0816