

The Royal Bank of Scotland plc Business Customer Agreement for the TrustAssured Service

These terms and conditions, the CERTIFICATE POLICIES and all other documents referred to herein set out the terms of agreement (the "Agreement") between you and The Royal Bank of Scotland plc for the use of the TRUSTASSURED SERVICE. This Agreement will be concluded once we accept your application by countersigning your BUSINESS CUSTOMER APPLICATION FORM.

Please note that these terms are in addition to any terms that already relate to your dealing and account(s) held with us and/or other members of The Royal Bank of Scotland Group of Companies and, in the event of any inconsistency between those terms and the terms of this Agreement specifically relating to the SERVICE, the terms of this Agreement will prevail.

1. Definitions

The Royal Bank of Scotland plc has a common set of definitions that are used in this Agreement and the other documents referred to in this Agreement. A definition for words appearing in capitals in these documents can be found in Schedule A to this Agreement.

2. Permitted Use of the Service and Your Responsibilities

2.1. You and your AUTHORISED OPERATORS may use the PERSONALISED SMARTCARD(s), smartcard reader(s), the SOFTWARE, HSM(s) and the SERVICE:

- 2.1.1. to sign electronically data and other communications to be sent to us and any RELYING CUSTOMER; and
- 2.1.2. to encrypt data and other communications to be sent to us and any RELYING CUSTOMER;
- 2.1.3. to decrypt data and other communications received from us and any SUBSCRIBING CUSTOMER;
- 2.1.4. to validate and authenticate digital signatures used to sign data and/or other communications received from us or SUBSCRIBING CUSTOMERS.

PROVIDED THAT such use is in the EUROPEAN UNION countries specified in Schedule A, the United States of America, or any other Jurisdictions that are also APPROVED by TrustAssured, and is otherwise strictly in accordance with the terms of this Agreement (including the CERTIFICATE POLICIES) and is solely for the purposes of your business. Personal use by you or your AUTHORISED OPERATORS is strictly prohibited.

- 2.2. You and your AUTHORISED OPERATORS shall promptly comply with such USER INSTRUCTIONS as we may issue from time to time. USER INSTRUCTIONS may be issued by phone, fax, e-mail or post or may be posted on a web site (www.rbs.co.uk).
- 2.3. You and your AUTHORISED OPERATORS must not use your KEY PAIRS and CERTIFICATEs, PERSONALISED SMARTCARD(s), smartcard reader(s), the SOFTWARE, HSM(s) or the SERVICE in connection with anything that:
 - 2.3.1. is illegal, unlawful or otherwise prohibited under any applicable law;
 - 2.3.2. involves any transaction for which you are not acting as a principal or as agent for a principal that has been disclosed to us in writing;
 - 2.3.3. is abusive, indecent, menacing, obscene,

offensive, defamatory, in breach of confidence; or

- 2.3.4. is in breach of any intellectual property rights or other third party rights.
 - 2.4. You are responsible for the supply and maintenance of the computer system(s) required to enable you to receive and use the SERVICE, and for ensuring compliance with the minimum configuration requirements specified by us for the time being and from time to time. You are responsible for obtaining any extra HARDWARE and SOFTWARE needed to ensure that your computer systems (including HSMs) are, and continue to be, compatible with the SERVICE and for the cost thereof.
 - 2.5. You acknowledge that you are familiar with, and agree to comply with, the policies and procedures established by us relating to the issuance, suspension, re-activation, expiration and revocation of CERTIFICATEs issued to you and your AUTHORISED OPERATORS that are detailed in the relevant CERTIFICATE POLICIES. Copies of the CERTIFICATE POLICIES are available on request.
 - 2.6. You and your AUTHORISED OPERATORS must only use HARDWARE and SOFTWARE, including HSMs, to access or otherwise use the SERVICE that complies with such specifications and requirements as IDENTRUST may require.
 - 2.7. You acknowledge that the laws of some countries restrict the use, import or export of encryption HARDWARE and SOFTWARE. Where you and/or your AUTHORISED OPERATORS take the SOFTWARE (or any computer on which it is installed), HSM(s) or PERSONALISED SMARTCARD(s) outside the United Kingdom you undertake to fully comply with local laws and regulations relating to their export and in particular you undertake to obtain any licence or approval that may be required.
 - 2.8. Before relying upon a digital signature generated by a SUBSCRIBING CUSTOMER, you or your AUTHORISED OPERATOR must authenticate and validate the signature using the SERVICE.
- ## 3. Appointment and Revocation of Authorised Operators
- 3.1. You may nominate one or more individuals to receive and utilise PERSONALISED SMARTCARD(s) on your behalf in accordance with the following procedure:
 - 3.1.1. your AUTHORISED SIGNATORY must complete, sign and return to us a BUSINESS CUSTOMER AUTHORISED OPERATOR Application Form which contains the details of the person(s) who you would like to become (an) AUTHORISED OPERATOR(s);
 - 3.1.2. you must satisfy yourself as to the identity of each person who you would like to become an AUTHORISED OPERATOR by examining sufficient personal identification such as a passport, driving licence, or National Insurance card.
 - 3.1.3. you must obtain the written consent of your AUTHORISED OPERATORS to the processing of their personal information in accordance with clause 16.2.
 - 3.2. You shall permit us or our authorised agents on

reasonable notice to carry out an audit during normal working hours at your premises for the purpose of verifying compliance by you with clause 3.1.3 and you shall provide us or our authorised agents with access to such relevant DOCUMENTATION and equipment as may be necessary for this purpose.

- 3.3. We may refuse, for any reason, to issue a PERSONALISED SMARTCARD to any person you have nominated to receive one.
- 3.4. If a PERSONALISED SMARTCARD is issued to a person whom you have nominated, that person will become an AUTHORISED OPERATOR and all acts or omissions of such AUTHORISED OPERATORS arising out of or with respect to the SERVICE shall for all purposes be deemed to be your acts or omissions.
- 3.5. If you wish to revoke or suspend an AUTHORISED OPERATOR's CERTIFICATE (PERSONALISED SMARTCARD), then your AUTHORISED SIGNATORY must sign and return to us, in accordance with the procedure set out in clause 11.3. below, a duly completed BUSINESS CUSTOMER AUTHORISED OPERATOR CERTIFICATE MANAGEMENT FORM.

4. Establishment and Revocation of TrustAssured Service Enabled Applications

- 4.1. In the event that you wish to use any SOFTWARE (other than the SOFTWARE in connection with the SERVICE) you must first seek our approval by completing and returning to us an TRUSTASSURED SERVICE ENABLED APPLICATION COMPLIANCE DECLARATION.
- 4.2. You will provide us with such information and access to such materials as we may require to enable us to assess your application for approval and to otherwise satisfy ourselves that the application you intend to operate will comply with such requirements as we and/or IDENTRUST may impose from time to time. If we approve your application we will issue you with your CERTIFICATEs and associated Key Pairs for usage on an HSM in respect of that application. The CERTIFICATEs and associated KEY PAIRS must only be used in respect of that application.
- 4.3. You are responsible for obtaining, maintaining and operating the HSM with which the application will be associated and for ensuring compliance with the minimum configuration requirements and all other technical and procedural requirements specified by us and/or IDENTRUST.
- 4.4. In the event that you wish to use or reproduce any of our, or IDENTRUST' trade marks, trade names, devices, logos or designs, you shall provide us with details of the name, mark, device, logo and/or design in question and the manner in which it is intended to be used. In the event that we approve such use, you shall be required to enter into a separate licence agreement.
- 4.5. We may, in our absolute discretion, refuse to approve any application under this clause 4 or subject use of it to such conditions, as we may deem appropriate.
- 4.6. If you wish to revoke or suspend an TRUSTASSURED SERVICE ENABLED APPLICATION's CERTIFICATE your AUTHORISED SIGNATORY must complete and return an TRUSTASSURED SERVICE ENABLED APPLICATION CERTIFICATE MANAGEMENT FORM in accordance with the procedure set out in clause 11.3.6 below.
- 4.7. Where you wish to upgrade, replace or implement any changes to any SOFTWARE approved by us under this clause 4, your AUTHORISED SIGNATORY must complete and return a revised TRUSTASSURED SERVICE ENABLED APPLICATION COMPLIANCE DECLARATION in accordance with the procedure set out in clause 11.3.5 below. You must not make any such

upgrades, replacements or changes unless and until approved by us.

5. Responsibility for Digital Transmissions

- 5.1. Subject to clause 5.2, you will be responsible for data and other communications signed digitally using KEY PAIRS and CERTIFICATEs issued by us to you or your AUTHORISED OPERATORs where the Identity CERTIFICATE has been correctly confirmed through the SERVICE as not having expired, been suspended or revoked.
- 5.2. You will not be responsible under clause 5.1 in relation to digital signatures generated using Identity CERTIFICATEs issued by us to you or your AUTHORISED OPERATORs where the request to validate the digital signature has been received by us after
 - 5.2.1. you have notified the SECURITY LINE in accordance with clause 6.4 that the security of your HSM or the PERSONALISED SMARTCARD held by you or your AUTHORISED OPERATOR has been, or you believe it may have been lost, stolen, misused or compromised; or
 - 5.2.2. you have requested the suspension or revocation of the applicable PERSONALISED SMARTCARD or HSM (and related CERTIFICATEs) in accordance with the procedure set out in clause 11.3.
This clause 5.2 shall not apply where you or any of your AUTHORISED OPERATORs have acted fraudulently or colluded with others who have done so.

6. Security

- 6.1. You are responsible for establishing and applying adequate security systems, controls and procedures in relation to:
 - 6.1.1. the PERSONALISED SMARTCARDs, smartcard readers, HSMs and SOFTWARE used by you and your AUTHORISED OPERATORs, to prevent their loss, disclosure to any other party, modification or use in breach of the terms of this Agreement;
 - 6.1.2. monitoring all usage of the SERVICE by you and your AUTHORISED OPERATORs including, without limitation, all use of PERSONALISED SMARTCARDs and HSMs.
- 6.2. You and your AUTHORISED OPERATORs must keep the PERSONALISED SMARTCARDs and smartcard readers issued to you physically secure at all times and not leave them unattended. AUTHORISED OPERATORs must not disclose their PIN(s) to anyone.
- 6.3. You must keep your HSM(s) physically secure at all times and comply with all security requirements imposed by us and/or IDENTRUST in relation thereto at all times.
- 6.4. You will provide immediate and accurate notice to the SECURITY LINE in accordance with the procedure set out in clause 11.3.1 of all relevant information relating to any actual or suspected loss, theft, misuse or compromise of the security of any HSM or the PERSONALISED SMARTCARDs held by you and/or your AUTHORISED OPERATORs. In particular, if you suspect or become aware that a third party knows or has compromised the safekeeping of the PIN(s) or PRIVATE KEY(s) held by you (including within HSMs) or your AUTHORISED OPERATORs you must notify the SECURITY LINE immediately.

7. Provision of the Service

We will provide the SERVICE to you under the terms and conditions of this Agreement until this Agreement is terminated.

8. Service Support

We will provide support for the SERVICE as described in Schedule C.

9. Charges

You agree to pay the applicable charges as set out in Schedule D, together with any taxes applicable, for use of the SERVICE.

10. Service Availability & Performance

The availability and performance of the SERVICE will be as defined in Schedule E.

11. Communication with The Royal Bank of Scotland plc

11.1. This clause shall govern all communications from you to us relating to the SERVICE, including:

- 11.1.1. BUSINESS CUSTOMER AUTHORISED OPERATOR Application Form;
- 11.1.2. BUSINESS CUSTOMER AUTHORISED OPERATOR Certificate Management Form;
- 11.1.3. TRUSTASSURED SERVICE ENABLED APPLICATION COMPLIANCE DECLARATION;
- 11.1.4. TRUSTASSURED SERVICE ENABLED APPLICATION CERTIFICATE MANAGEMENT FORM.

11.2. Subject to clause 11.3, all communications to be sent to us by you relating to the SERVICE can be by facsimile or by writing to the SERVICE OFFICE.

11.3. The following types of communication must be sent to us in the following form:

- 11.3.1. a notice to be given under clause 6.4 must be given by facsimile to the SECURITY LINE followed by confirmation by recorded delivery to the SERVICE OFFICE;
- 11.3.2. the signed original BUSINESS CUSTOMER APPLICATION FORM must be submitted to the SERVICE OFFICE;
- 11.3.3. the signed original BUSINESS CUSTOMER AUTHORISED OPERATOR Application Form must be submitted to the SERVICE OFFICE;
- 11.3.4. the BUSINESS CUSTOMER AUTHORISED OPERATOR Certificate Management Form must be submitted by fax followed by confirmation of the signed original to the SERVICE OFFICE;
- 11.3.5. the signed original TrustAssured Service Enabled Application Compliance Declaration must be submitted to the SERVICE OFFICE;
- 11.3.6. the TRUSTASSURED SERVICE ENABLED APPLICATION CERTIFICATE MANAGEMENT FORM must be submitted by fax followed by confirmation of the signed original to the SERVICE OFFICE.

11.4. We may act on any instruction that we receive relating to the SERVICE that has been signed by your AUTHORISED SIGNATORY, or otherwise reasonably appears to have been sent by you.

11.5. We may refuse to carry out an instruction if we reasonably believe that:

- 11.5.1. the instruction is invalid;
- 11.5.2. the instruction has not come from you; or
- 11.5.3. carrying out the instruction would result in a breach of the terms of this Agreement or of the rules of the IDENTRUST SCHEME.

In the event that we do so, we shall endeavour to notify you promptly thereafter.

12. Legal Effect

12.1. You agree that all data and other communications signed electronically using a KEY PAIR and CERTIFICATE issued to you or one of your AUTHORISED OPERATORS shall have the same legal effect, validity and enforcement as if the data and other

communications had been in writing signed by you or that AUTHORISED OPERATOR (as the case may be).

12.2. You and your AUTHORISED OPERATORS will not challenge the legal effect, validity or enforceability of data and other communications signed electronically using a Key Pair and CERTIFICATE issued to you or one of your AUTHORISED OPERATORS solely on the basis that it is in digital rather than written form.

12.3. You and your AUTHORISED OPERATORS shall not interfere with any procedures in relation to the logging or time-stamping carried out by the SOFTWARE or otherwise undertaken in connection with the SERVICE. Save in the case of manifest error or fraud, you acknowledge and agree that our records (including time stamps, logs and other material that is generated automatically) shall be deemed to be accurate unless the contrary is proven by you.

13. Call Recording

13.1. Telephone calls and e-mails may be monitored and/or recorded by or on behalf of The Royal Bank of Scotland plc:

- 13.1.1. for purposes of quality control and training;
- 13.1.2. to maintain and improve the SERVICE;
- 13.1.3. for security reasons;
- 13.1.4. to establish the existence of facts in the event of a dispute or misunderstanding and to ascertain compliance with applicable regulatory or self-regulatory practices.

13.2. In the event that it is necessary to access a recording for these purposes, the access will be made under appropriate supervision.

14. Accuracy of Information

14.1. You warrant the accuracy of all information supplied to us in relation to the SERVICE and, in particular, the BUSINESS CUSTOMER APPLICATION FORM and the other documents listed in clause 11.1. You will promptly notify us of any changes to the information described in this clause 14.1.

14.2. You will verify all information supplied to us that has been supplied by your AUTHORISED OPERATORS in relation to the SERVICE.

14.3. You will ensure that on receipt of each PERSONALISED SMARTCARD, each of your AUTHORISED OPERATORS verifies that the information contained in the CERTIFICATES on the PERSONALISED SMARTCARDS is complete, accurate and up-to-date.

14.4. You will, on receipt of HSM(s), verify that the information contained in the CERTIFICATES on the HSM(s) is complete, accurate and up-to-date.

14.5. You will promptly notify us when you would like to revoke or suspend the authorisation granted to an AUTHORISED OPERATOR or a TRUSTASSURED SERVICE ENABLED APPLICATION to utilise the SERVICE on your behalf.

15. Directory

15.1. You accept that your CERTIFICATES may be published in our directory service that may be made available to other customers within the IDENTRUST SCHEME.

16. Transfer of Information

16.1. Subject to clause 16.2, we will use all reasonable endeavours to ensure that all information about you, your AUTHORISED OPERATORS and your business received by or on behalf of us in connection with the SERVICE is kept confidential and is not disclosed to any third party. We are authorised to disclose information if that disclosure is:

- 16.1.1. made to the relevant authority where we are under a legal obligation to disclose the information; or

- 16.1.2. made in the course of the provision by us of the SERVICE in accordance with this Agreement and any USER INSTRUCTIONS given by us; or
- 16.1.3. made with your consent in accordance with clause 11 or 25.
- 16.2. Without prejudice to clause 3.1.3, you acknowledge that The Royal Bank of Scotland plc, other Participants, IDENTRUST and their employees and agents may and you hereby authorise each of them to, within the limits of applicable law, hold, transmit receive or otherwise process any data or information about, regarding or involving you and your AUTHORISED OPERATORS among and between themselves and other third parties, both within the European Economic Area (EEA), and within countries outside the EEA which may not provide a level of protection of personal data equivalent to that which is available within the EEA:
- 16.2.1. to provide the SERVICE to you;
- 16.2.2. to resolve any dispute arising from the SERVICE; or
- 16.2.3. pursuant to applicable law.
- 16.3. You agree (and to ensure that your AUTHORISED OPERATORS treat) any information received through the SERVICE about other Customers as CONFIDENTIAL INFORMATION in accordance with clause 19.
- 17. Data Protection**
- 17.1. Where personal data is processed by or on behalf of us, we will undertake such processing purely for the purpose of providing the SERVICE to you and will do so in accordance with the terms of this Agreement.
- 17.2. We will implement appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to such personal data in compliance with the Data Protection Act 1998.
- 17.3. For the purpose of this clause 17 "personal data" and "processing" shall have the meanings ascribed to them in the Data Protection Act 1998.
- 18. Ownership**
- 18.1. Except as may be expressly provided for in this Agreement, you shall not obtain any rights, title or interest in the HARDWARE (including the Key Pairs and CERTIFICATEs contained therein), DOCUMENTATION, SOFTWARE, DIRECTORY ENTRIES and such other materials as may be provided to you and your AUTHORISED OPERATORS as part of the SERVICE from time to time and you acknowledge that we and/or IDENTRUST and/or third parties own all such rights, titles and interests.
- 18.2. You are given no rights under this Agreement to use, copy or reproduce in any way any of The Royal Bank of Scotland plc's trade marks, trade names, logos or designs.
- 18.3. You acknowledge that IDENTRUST is the sole and exclusive owner of all rights, title and interest in and to the IDENTRUST trade marks, trade names, logos or designs.
- 19. Confidentiality**
- 19.1. "Confidential Information" means all information of a confidential nature (including, without limitation, all information relating to the IDENTRUST SCHEME and all trade secrets, financial, operating, economic, technical, programming and other commercial know-how) and any copies or records thereof, whether presented orally or in writing, in any medium, directly or indirectly disclosed by us to you pursuant to or in connection with this Agreement, but excluding information which is
- 19.1.1. in the public domain otherwise than in circumstances giving rise to a breach of the terms of this Agreement;
- 19.1.2. already known to you at the time the information is disclosed by us;
- 19.1.3. subsequently received by you in good faith from a non-party to this Agreement who has the prior right to make such subsequent disclosure;
- 19.1.4. approved in writing for unrestricted release or unrestricted disclosure by us; or
- 19.1.5. developed independently by you other than from information disclosed by us or disclosed in breach of any of the obligations contained in this Agreement.
- 19.2. You and your AUTHORISED OPERATORS must keep confidential all CONFIDENTIAL INFORMATION and not disclose it to any party or use it other than for the performance of this Agreement. You further agree that, without our prior express written consent, you shall never disclose, directly or indirectly, in whole or in part, alone or in conjunction with others, any CONFIDENTIAL INFORMATION to anyone other than to your employees and agents with a need to know such CONFIDENTIAL INFORMATION for purposes contemplated by this Agreement.
- 19.3. Notwithstanding clause 19.2, you shall be entitled to produce or disclose CONFIDENTIAL INFORMATION required by applicable law, regulation or court order, or any regulatory body or stock exchange, provided you have (if reasonably practicable) given us prior written notice of such request such that we have a reasonable opportunity to defend, limit or protect such production or disclosure.
- 19.4. Copies or reproductions of CONFIDENTIAL INFORMATION shall not be made except to the extent reasonably necessary and all copies made shall be our property.
- 19.5. You undertake immediately upon our written request in the event of a breach of this clause 19 by you or on termination of this Agreement whichever is the earlier either:
- 19.5.1. promptly to return all documents and other material on any medium whatsoever in your possession, custody or control that bear or incorporate any CONFIDENTIAL INFORMATION; or
- 19.5.2. promptly to destroy by shredding or incineration all documents and other materials on any medium whatsoever in your possession, custody or control that bear or incorporate any part of CONFIDENTIAL INFORMATION and to certify to us that this has been done.
- 20. Hardware and Software Licence**
- 20.1. HARDWARE and SOFTWARE is licensed for use by you on the terms of this clause 20. Where the HARDWARE and/or SOFTWARE is subject to a licence granted by a THIRD PARTY PRODUCT PROVIDER, the provisions of clause 20.7 shall apply. The HARDWARE and/or the SOFTWARE shall be licensed to you on a non-exclusive, non-transferable basis for use by you and your AUTHORISED OPERATORS only to enable you to obtain and use the SERVICE but not otherwise.
- 20.2. You must install and use such upgrades or replacements to the HARDWARE and SOFTWARE as may be made available from time to time as soon as possible after receipt of such upgrades or replacements. You will promptly comply with our USER INSTRUCTIONS regarding the materials being upgraded or replaced including returning them to us or destroying them if we so direct.

- 20.3. Save to the extent permitted by law, you must not and must not attempt to do any of the following or allow your AUTHORISED OPERATORS or any third party to do so:
- 20.3.1. copy, publish, sell, rent, lease, de-compile, reverse engineer or modify the SOFTWARE or any part or parts thereof;
- 20.3.2. sell, rent, lease, reverse engineer, modify or tamper with any of the HARDWARE or any part or parts thereof.
- 20.4. All rights granted to you by this clause 20 shall terminate on termination of this Agreement.
- 20.5. You shall have no right to assign, sub-licence or otherwise transfer any rights in any HARDWARE or SOFTWARE without our prior written consent.
- 20.6. IDENTRUST may in its own right enforce this clause 20.
- 20.7. You acknowledge and agree that:
- 20.7.1. the licence granted by this clause 20 shall be subject to any licence granted to us by a THIRD PARTY PRODUCT PROVIDER of any of the HARDWARE and/or SOFTWARE;
- 20.7.2. you will comply with any additional terms imposed by the THIRD PARTY PRODUCT PROVIDER of any of the HARDWARE and/or SOFTWARE. Such additional terms will be notified to you either when the HARDWARE in question and/or SOFTWARE is/are provided to you or when you install and use them. If you refuse to accept any such terms you must return the HARDWARE and SOFTWARE to us and this Agreement will terminate on our receipt thereof and the provisions of clause 24 shall apply.
- 20.7.3. if any licence granted to us by a THIRD PARTY PRODUCT PROVIDER is terminated, the licence granted by this clause 20 will also terminate and you must stop using the HARDWARE and/or SOFTWARE (as the case may be) and destroy all copies of it or return them as instructed by us.

21. Recourse

- 21.1. When you or your AUTHORISED OPERATOR act as a SUBSCRIBING CUSTOMER:
- 21.1.1. You agree that your only recourse in connection with the SERVICE, including with respect to claims arising out of the negligence of any person, is to us and only to the extent provided for in this Agreement.
- 21.1.2. You expressly recognise and agree that you have no recourse in this regard to IDENTRUST or another Participant in connection with the SERVICE, but may have recourse or liability to the RELYING CUSTOMER under applicable law.
- 21.2. When you or your AUTHORISED OPERATOR act as a RELYING CUSTOMER:
- 21.2.1. You agree that you shall have no recourse of any kind against any party, except us or the SUBSCRIBING CUSTOMER, in connection with the SERVICE, including with respect to claims arising out of the negligence of any person.
- 21.2.2. You may have recourse to us to and only to the extent provided for in this Agreement and may have recourse or liability to the SUBSCRIBING CUSTOMER under applicable law.

22. Liability and Indemnity

- 22.1. We will take all reasonable care to prevent the release of viruses or other damaging code in provision of the SERVICE, related DOCUMENTATION or correspondence. However, we will not be liable for any damages that arise from this and you are advised to deploy your own anti-virus mechanisms.**

22.2. We shall not be liable to you either in contract, tort (including negligence) or otherwise for:

- 22.2.1. any loss or damage that you suffer as a result of your use of the SERVICE unless such loss or damage is caused directly by our negligence or by a breach of this Agreement by us;
- 22.2.2. any direct or indirect loss of profit, goodwill, business or anticipated savings nor for any indirect or consequential loss or damage resulting from your and/or your AUTHORISED OPERATORS use of, or inability to use, the SERVICE, the HARDWARE or the SOFTWARE;
- 22.2.3. any losses resulting from third party services outside our reasonable control (including, but not limited to, telephone and browser services);
- 22.2.4. any loss caused by delay by us in performing or failure to perform our obligations under this Agreement if the delay or failure results from events or circumstances outside our control. Such delay or failure will not constitute a breach of this Agreement;
- 22.2.5. any loss suffered as a result of our refusal under clause 11.5.
- 22.3. Nothing in this Agreement shall limit either party's liability for death or personal injury resulting from its negligence or breach of this Agreement.
- 22.4. We expressly disclaim any warranty that data or communications sent or received through the SERVICE meet local legal requirements to effect a binding transaction or produce material that will be admissible as evidence in legal proceedings.
- 22.5. When you or your AUTHORISED OPERATOR act as a RELYING CUSTOMER, our liability to you for providing an incorrect IDENTITY VALIDATION shall be limited to £350 in respect of any single incorrect IDENTITY VALIDATION or series of related incorrect IDENTITY VALIDATIONS and is conditional on you informing us of any such claim within 14 days of the incorrect IDENTITY VALIDATION.
- 22.6. Our maximum aggregate liability to you howsoever arising from or in connection with this Agreement (whether for breach of contract, negligence, misrepresentation or otherwise) shall not in any circumstances exceed the greater of £65,000 or the amount of charges paid by you to us in relation to the SERVICE over the one-year period preceding the event for which we are alleged to be liable.
- 22.7. You will indemnify us for any liability or loss incurred by us resulting from your or your AUTHORISED OPERATORS':
- 22.7.1. use of HARDWARE and/or SOFTWARE and any electronic messages or communications sent to persons or entities that are not RELYING CUSTOMERS of a Participant in the IDENTRUST SCHEME; or
- 22.7.2. failure to comply with the terms of this Agreement.

23. Suspension of Service and Certificates

- 23.1. We reserve the right to suspend the SERVICE for repair, maintenance, and/or upgrade work. We will endeavour to give you such reasonable notice as circumstances permit but we do not guarantee that we will be able to do so in all cases. Notice may be given by facsimile, e-mail, posted on a web site (www.rbs.co.uk), by phone or by post.

- 23.2. We reserve the right to suspend:
- 23.2.1. your access to the SERVICE where the SERVICE has not been used by you or any of your AUTHORISED OPERATORS; or
 - 23.2.2. a given AUTHORISED OPERATOR's access to the SERVICE where the SERVICE has not been used by that AUTHORISED OPERATOR during the immediately preceding 90 day period.
- 23.3. Where access has been suspended under clause 23.2, we will reactivate your access to the SERVICE if you instruct us by re-submitting a request for reactivation in accordance with clause 11.
- 23.4. We may suspend and/or revoke CERTIFICATES issued to you and/or your AUTHORISED OPERATORS to protect our interests, our CUSTOMERs interests or IDENTRUST's interests, upon expiry of the SUSPENSION GRACE PERIOD, upon receipt of multiple suspension requests or upon termination of this Agreement, as described in the CERTIFICATE POLICIES.

24. Termination

- 24.1. Either party may terminate this Agreement by giving the other 30 days notice in accordance with clause 25.
- 24.2. We may terminate this Agreement forthwith on written notice if:
- 24.2.1. you are subject to an INSOLVENCY EVENT;
 - 24.2.2. you or any of your AUTHORISED OPERATORS persistently breach or commit a material breach of this Agreement which is not remedied within 30 days of a request to do so by us;
 - 24.2.3. you or any of your AUTHORISED OPERATORS commit, or attempt to commit, a fraud using the SERVICE or otherwise use the SERVICE in an illegal or unlawful way;
 - 24.2.4. we cease to offer the SERVICE; or
 - 24.2.5. you or your AUTHORISED OPERATORS' use of the SERVICE is likely to bring us or the SERVICE into disrepute;
 - 24.2.6. it is reasonably necessary to protect us and/or you.
- 24.3. Upon termination of this Agreement by either party:
- 24.3.1. provision of the SERVICE shall cease;
 - 24.3.2. you and your AUTHORISED OPERATORS must de-install the HARDWARE and SOFTWARE from your computer systems and, at our option, immediately destroy in accordance with our instructions or return promptly via secure courier to us at your cost, all KEY PAIRS, CERTIFICATES, HARDWARE and SOFTWARE (including the media on which the SOFTWARE was originally provided along with any copies made by you or on your behalf and any copies of the KEY PAIRS and CERTIFICATES held by you or on your behalf);
 - 24.3.3. you must immediately pay to us any outstanding charges due under the SERVICE.
- 24.4. This agreement will continue until terminated in accordance with this clause 24.

25. Notice

- 25.1. Notices served by you under this Agreement must be made in writing to the SERVICE OFFICE and be signed by your AUTHORISED SIGNATORY(s).
- 25.2. Notices to be served by us under this Agreement shall be given to the primary or secondary contacts specified on the BUSINESS CUSTOMER APPLICATION FORM to the addresses set out therein. You may change your AUTHORISED SIGNATORY, primary or secondary contacts (or any of their details) at anytime by notice in writing, which change shall take effect upon approval thereof by us. Unless otherwise specified in this Agreement, notices shall be sent by post or fax.

26. Transfer of Rights

- 26.1. You are not entitled to assign, sub-licence or otherwise transfer any of your rights under this Agreement.
- 26.2. We may assign, sub-licence or otherwise transfer any of our rights under this Agreement.

27. Sub-contractors

- 27.1. You may sub-contract any of your obligations under this Agreement without our consent.
- 27.2. If you do use such sub-contractors, such use shall be without prejudice to your obligations under this Agreement and you shall be responsible for all acts and defaults of the sub-contractor.
- 27.3. You must procure that sub-contractors shall be subject to provisions identical in all material respects to clauses 19, 20 and 24.

28. Dispute Resolution

- 28.1. Any dispute solely between you and us, arising out of or in connection with the SERVICE, not otherwise provided for in this clause 28, shall be settled in accordance with our DISPUTE RESOLUTION PROCEDURE for the TRUSTASSURED SERVICE.
- 28.2. You agree that any dispute between you and any Participant (other than us) and/or IDENTRUST or any dispute with us that involves related claims by or against other Participants and/or IDENTRUST arising out of or in connection with the SERVICE or the IDENTRUST SCHEME shall be finally settled pursuant to the IDENTRUST DISPUTE RESOLUTION PROCEDURES. You expressly consent to being joined as a party to any DISPUTE RESOLUTION in respect of such disputes and in accordance with the IDENTRUST DISPUTE RESOLUTION PROCEDURES.

29. Waiver and Whole Agreement

- 29.1. No act, omission or delay by us shall be a waiver of our rights or remedies under this Agreement unless otherwise agreed in writing by us.
- 29.2. This Agreement and the documents referred to herein constitute the whole agreement between The Royal Bank of Scotland plc and you relating to the SERVICE and supersedes any previous agreement between the parties in relation to the SERVICE. All terms which may be implied by law into this Agreement are hereby excluded.
- 29.3. You acknowledge that you have not been induced to enter into this Agreement by any representation, warranty or undertaking not expressly incorporated into it. So far as permitted by law and except in the case of fraud, you agree and acknowledge that your only rights and remedies in relation to any representation, warranty or undertaking made or given in connection with this Agreement shall be for breach of the terms of this Agreement.
- 29.4. If any term of this Agreement is held to be invalid, the remaining terms of this Agreement shall continue to be valid to the fullest extent permitted by law.

30. Third Party Rights

- 30.1. Except as provided in clause 20, non-parties may not enforce this Agreement by virtue of the Contracts (Rights of Third Parties) Act 1999.
- 30.2. No consent will be required from any non-parties to vary the terms of this Agreement.

31. Variation

- 31.1. We reserve the right to vary the terms of this Agreement or the other documents referred to herein at any time provided that we give you at least 30 days' prior notice before such changes take effect.
- 31.2. We reserve the right to change any aspect of the SERVICE. We will give you reasonable notice of such changes.

32. Applicable Law

The terms and conditions of this Agreement will be construed in accordance with English law and will be subject to the non-exclusive jurisdiction of the English courts.

SCHEDULE A

Definition of Terms

In this Agreement the following terminology shall have the following meanings.

“TrustAssured Service” or “Service” means the service to be provided under the terms of this Agreement as described in Schedule B.

“TrustAssured Service Enabled Application” means a computer service/application that has been constructed to make use of the Service.

“TrustAssured Service Enabled Application Certificate Management Form” means the document that forms part of the Agreement between you and The Royal Bank of Scotland plc to be used for the deletion, suspension and re-activation of Certificates used by TrustAssured Service Enabled Applications.

“TrustAssured Service Enabled Application Compliance Declaration” means the document that forms part of the Agreement between you and The Royal Bank of Scotland plc that defines the purpose and operation of the application, together with details of the hardware and software that will be used to deliver the application.

“Approved” means that the jurisdiction has been assessed by the TrustAssured PAA for suitability and if found to be an acceptable jurisdiction that the necessary application form (BCA) has then been provided to the Customer to allow them to request provision of the Service.

“Authorised Operator” means any person issued with a Personalised smartcard at your request pursuant to the procedures set out in clause 3.

“Authorised Signatory” means that (or those) individual(s) that is (are) authorised by your Business, and accepted by The Royal Bank of Scotland plc, from time to time, to sign the Business Customer Application Form and to authorise instructions to The Royal Bank of Scotland plc.

“Business” means a limited company; partnership; sole trader; club; society; charity; trust or other unincorporated body.

“Business Customer Application Form” means the application form for the Service that forms part of the Agreement between you and The Royal Bank of Scotland plc.

“Business Customer Authorised Operator Application Form” means the application form to be used for the nomination of Authorised Operators of the Service that forms part of the Agreement between you and The Royal Bank of Scotland plc.

“Business Customer Authorised Operator Certificate Management Form” means the form to be used for the deletion, suspension and re-activation of Authorised Operators of the Service that forms part of the Agreement between you and The Royal Bank of Scotland plc.

“Certificate” means an X.509 v.3 compliant digitally signed data structure that immutably binds a Public Key to information uniquely identifying the possessor of the Private Key corresponding to such Public Key and that is issued by a Participant to a Customer under the Identrust Scheme.

“Certificate Policies” means the documents issued by The Royal Bank of Scotland plc that set out the broad policy constraints that are imposed by The Royal Bank of Scotland plc’s certification authority concerning the operational use of Certificates issued within its infrastructure. Policy documents are issued for Identity and Utility Certificates.

“Confidential Information” shall have the meaning given in clause 19.

“Customer” means an entity that has entered into an agreement with a Participant governing the provision of services under the Identrust Scheme to the entity by that Participant.

“Directory Entries” means a database of Certificates and other information relating to users of the Service.

“Dispute Resolution” means a dispute to be conducted in accordance with one of the Dispute Resolution Procedures.

“Dispute Resolution Procedure for the TrustAssured Service” means the procedure contained in a document of that name as provided to you and as varied by us from time to time in accordance with this Agreement.

“Dispute Resolution Procedures” means the Identrust Dispute Resolution Procedures and the Dispute Resolution Procedure for the TrustAssured Service.

“Documentation” means material published by us, and/or Identrust, and/or third parties that describes the functionality or instructions on using the Service.

“European Union” includes only the following Countries: Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Slovenia, Spain, Sweden, United Kingdom.

“Hardware” means any equipment provided to you by us or on our behalf for use of the Service including, without limitation, Personalised smartcard(s), smartcard reader(s), Hardware Security Module (HSM) and/or other hardware token(s), including any updates issued to you.

“Hardware Security Module” or “HSM” means an electronic device attached to a computer system that is used to securely hold the cryptographic keys.

“Head of TrustAssured”, means The Royal Bank of Scotland plc, Head of TrustAssured, 5th Floor, 2 Waterhouse Square, 138–142 Holborn, London EC1N 2TH.

“Helpdesk” means the Customer Helpdesk maintained by us to provide information and assistance to you in relation to the Service. Contact details The Royal Bank of Scotland plc, The TrustAssured Service Operations Team, 5th Floor, 2 Waterhouse Square, 138–142 Holborn, London EC1N 2TH
Tel No: +44 (0)20 7427 9355

Fax No: +44 (0)20 7427 8342

E-Mail: TrustAssured.helpdesk@rbs.co.uk

“Identity Certificate” means a Certificate that is issued by an Issuing Participant to a Subscribing Customer under the Identrust Scheme to enable the Subscribing Customer to create digital signatures.

“Identity Validation” means the process whereby we validate and authenticate a digital signature for you as part of the Service.

“Identrust” means Identrust, LLC, a Delaware limited liability company.

“Identrust Dispute Resolution Procedures” means the process set forth in the Identrust Dispute Resolution Procedures document [IL-DRP] as varied from time to time for resolving a dispute arising from the Identrust Scheme.

“Identrust Scheme” means the infrastructure and scheme operated by Identrust for the provision of digital signature and identity validation services to Customers.

“Insolvency Event” means:

- (a) you at any time cease or suspend the payment of your debts or be or be deemed unable to pay your debts; or
- (b) any step, application or proceeding is taken by you or against you, for your dissolution, winding up or bankruptcy or the appointment of a receiver, administrative receiver, administrator or similar officer to you or over all or any part of your assets or undertaking;
- (c) where you are a partnership, such partnership is dissolved or joins or amalgamates with any other partnership;
- (d) you commence negotiations with any of your creditors with a view to the general readjustment or rescheduling of your indebtedness, make a proposal for a voluntary arrangement or enter into an arrangement for the benefit of any of your creditors;
- (e) you suspend or cease or threaten to suspend or cease all or a substantial part of your operations;

or if any event occurs which, under the applicable law of any jurisdiction, has an analogous or equivalent effect to any of the events mentioned above.

“Issuing Participant” means, with respect to a Certificate, the Participant that issued that Certificate.

“Key Pair” means, with respect to any party in the Identrust Scheme, its Private Key and corresponding Public Key.

“Personalised smartcard” or “smartcard” means a card containing a computer chip that meets the specifications and standards specified by Identrust.

“PIN” (Personal Identity Number) means the eight (8) character random alpha/numeric code that must be entered in order to use your Personalised smartcard.

“Public Key” means the key of an entity’s asymmetric key pair that can be made public.

“Private Key” means one half of a cryptographic Key Pair (kept secret by the holder) as drawn from the class of asymmetric key cryptographic functions used in the Identrust Scheme that a Customer may apply to electronic data for identification purposes to generate a digital signature.

“Relationship Manager” means the individual identified on the Business Customer Application Form or their replacement from time to time.

“Relying Customer” means a Customer that requests from its Relying Participant confirmation of the status of a Certificate included in a digital transmission as a valid Certificate.

“Relying Participant” means the entity that provides services under the Identrust Scheme to a Relying Customer and that has entered into a Customer Agreement with that Relying Customer.

“Security Line” means the telephone line maintained by us to receive reports of security incidents, or suspected incidents, concerning the Service Tel: Freephone 0800 587 1597 or Tel No: +44 (0)20 7427 9355 Fax No: +44 (0)20 7427 8342 E-Mail: TrustAssured.helpdesk@rbs.co.uk

“Service” or “the TrustAssured Service” means the service to be provided under the terms of this Agreement as described in Schedule B.

“Service Office” means office maintained by us to which Customer application details and notices relating to the Agreement are to be addressed. Contact details The Royal Bank of Scotland plc, The TrustAssured Service Operations Team, 5th Floor, 2 Waterhouse Square, 138–142 Holborn, London EC1N 2TH.

Tel: Freephone 0800 587 1597 or

Tel No: +44 (0)20 7427 9355 Fax No: +44 (0)20 7427 8342

E-Mail: TrustAssured.helpdesk@rbs.co.uk

“Service Owner” means The Royal Bank of Scotland plc Head of TrustAssured, 5th Floor, 2 Waterhouse Square, 138–142 Holborn, London EC1N 2TH.

“Subscribing Customer” means a Customer that obtains a Certificate from an Issuing Participant for use in connection with the Identrust Scheme.

“Software” means the software provided, or otherwise made available, to you by or on behalf of The Royal Bank of Scotland plc from time to time for use in connection with the Service.

“Suspension Grace Period” means the period of time during which a Certificate can remain suspended, after which it is automatically revoked.

“The Royal Bank of Scotland plc”, “we”, “our”, “us” means The Royal Bank of Scotland plc.

“The Royal Bank of Scotland Policy Approval Authority” means the authority established within The Royal Bank of Scotland plc consisting of representatives of its management to create, monitor and amend the policy documentation relating to the Service.

“Third Party Product Provider” means an external organisation that has developed and/or supplied Hardware and/or Software.

“User Instructions” means any guidance, advice, notification, letter or other communication from us to you that defines or otherwise explains how to use the Service or any part(s) of it.

“you”, “your” means the Business which has entered into this Agreement with The Royal Bank of Scotland plc for the provision of the Service.

SCHEDULE B

The TrustAssured Service

Description of Service

The SERVICE consists of the provision of facilities and equipment to allow you to use digital signatures to confirm your identity in communications with us and third parties and the verification of the identity of parties sending communications including their digital signatures to you.

SCHEDULE C

The TrustAssured Service

Support Services

Under the terms and conditions of this Agreement, we will provide to you at the fees specified in Schedule D the following support services:

1. Access to a telephone HELPDESK and SECURITY LINE between the hours of 08.00 and 18.00 Monday to Friday excluding English Bank and Public Holidays to:
 - Receive general advice and guidance relating to usage of the SERVICE, completion of forms and any other aspects of the SERVICE.
 - Receive technical support and guidance relating to the HARDWARE and SOFTWARE.
 - Report instances, or believed instances, of security breaches relating to your PERSONALISED SMARTCARD, PIN, HSM (if applicable) and PRIVATE KEYS.
 - Request CERTIFICATE issuance, suspension, re-activation and revocation concerning your AUTHORISED OPERATORs and HSMs (if applicable).
2. Provision of HARDWARE and SOFTWARE upgrades as determined and distributed by us from time to time
3. Provision of replacement HARDWARE and SOFTWARE (media) where the original becomes faulty or is lost/ stolen and is correctly reported to us as a security compromise.
4. Provision of new PERSONALISED SMARTCARDs following CERTIFICATE renewal.
Provision of configuration and operational changes as determined and distributed by us from time to time in the form of USER INSTRUCTIONS.
We shall not be obliged to provide support in respect of:
 - improper installation, use, operation or neglect of the HARDWARE or SOFTWARE;
 - use of the HARDWARE or SOFTWARE for purposes for which it was not designed;
 - any repair, alteration or modification of the HARDWARE or SOFTWARE (in whole or in part) by any person other than us or our agent, without our prior written consent or in breach of the terms of this Agreement;
 - where applicable, your failure to install within a reasonable time any new release of HARDWARE or SOFTWARE issued to you by us;
 - your use of a computer system other than as specified in USER INSTRUCTIONS issued by us;
 - any unforeseeable impact on the existing applications on your computer system;
 - any SOFTWARE or HARDWARE supplied by a third party, unless agreed by us in writing;
 - failure to comply with USER INSTRUCTIONS, CERTIFICATE POLICIES or this Agreement;
 - the introduction of any virus or other malicious code.If we agree to undertake additional support (which is not included in the support services described above), you will be advised of any costs payable before the additional support is provided.

SCHEDULE D

The TrustAssured Service

Charges Schedule

Please contact your RELATIONSHIP MANAGER or the SERVICE OFFICE for a current copy of the Charges Schedule for the TRUSTASSURED SERVICE.

SCHEDULE E

The TrustAssured Service

Service Availability and Performance

The SERVICE will be made available to you 24 hours per day, 365 days per year, subject to the terms of this Agreement. Note that end to end performance throughout the SERVICE cannot be guaranteed as it is formed from a number of services which are outside our control, e.g. Internet communication services, SUBSCRIBING CUSTOMER computer system, RELYING CUSTOMER application/service, Issuing and RELYING PARTICIPANTS' services (as appropriate).