

The **co-operative** bank  
good with money

The Co-operative Bank plc

Terms & Conditions

for the

bsecure 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 Co-operative Bank plc for the use of the bsecure Service. This Agreement will be concluded once we accept your application by countersigning your bsecure 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 Co-operative Bank P.l.c. 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 Co-operative Bank 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 Users may use the Personalised Smart Card(s), Smart Card 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 United Kingdom, 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 Users is strictly prohibited.
- 2.2. You and your Authorised Users 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.
- 2.3. You and your Authorised Users must not use your Key Pairs and Certificates, Personalised Smart Card(s), Smart Card 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 Users that are detailed in the relevant Certificate Policies. Copies of the Certificate Policies are available on request.

- 2.6. You and your Authorised Users must only use hardware and software, including HSMs, to access or otherwise use the Service that complies with such specifications and requirements as Identrus 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 Users take the Software (or any computer on which it is installed), HSM(s) or Personalised Smart Card(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 User must authenticate and validate the signature using the Service.

## 3. Appointment and Revocation of Authorised Users

- 3.1. You may nominate one or more individuals to receive and utilise Personalised Smart Card(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 User Application Form which contains the details of the person(s) who you would like to become (an) Authorised User(s);
  - 3.1.2. you must satisfy yourself as to the identity of each person who you would like to become an Authorised User 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 User(s) 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 Condition 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 Smart Card to any person you have nominated to receive one.
- 3.4. If a Personalised Smart Card is issued to a person whom you have nominated, that person will become an Authorised User and all acts or omissions of such Authorised Users 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 User's Certificate (Personalised Smart Card), then your Authorised Signatory must sign and return to us, in accordance with the procedure set out in Condition 11.3. below, a duly completed Business Customer Authorised User Certificate Management Form.

## 4. Establishment and Revocation of bsecure 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 a bsecure 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 Identrus 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 Identrus.
- 4.4. In the event that you wish to use or reproduce any of our, or Identrus' 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 Condition 4 or subject use of it to such conditions, as we may deem appropriate.
- 4.6. If you wish to revoke or suspend a bsecure Service Enabled Application's Certificate your Authorised Signatory must complete and return a bsecure Service Enabled Application Certificate Management Form in accordance with the procedure set out in Condition 11.3.6 below.
- 4.7. Where you wish to upgrade, replace or implement any changes to any software approved by us under this Condition 4, your Authorised Signatory must complete and return a revised bsecure Service Enabled Application Compliance Declaration in accordance with the procedure set out in Condition 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 Condition 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 Users 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 Condition 5.1 in relation to digital signatures generated using Identity Certificates issued by us to you or your Authorised Users where the request to validate the digital signature has been received by us after
  - 5.2.1. you have notified Computer Banking Services in accordance with Condition 6.3 that the security of your HSM or the Personalised Smart Card held by you or your Authorised User 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 Smart Card or HSM (and related Certificates) in accordance with the procedure set out in Condition 11.3.

This Condition 5.2 shall not apply where you or any of your Authorised Users 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 Smart Cards, Smart Card readers, HSMs and Software used by you and your Authorised Users, 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 Users including, without limitation, all use of Personalised Smart Cards and HSMs.
- 6.2. You and your Authorised Users must keep the Personalised Smart Cards and Smart Card readers issued to you physically secure at all times and not leave them

unattended. Authorised Users 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 Identrus in relation thereto at all times.
- 6.4. You will provide immediate and accurate notice to Computer Banking Services in accordance with the procedure set out in Condition 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 Smart Cards held by you and/or your Authorised Users. 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 Users you must notify Computer Banking Services 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 Co-operative Bank plc**

- 11.1. This Condition shall govern all communications from you to us relating to the Service, including:
  - 11.1.1. Business Customer Authorised User bsecure Application Form;
  - 11.1.2. Business Customer Authorised User Certificate Management Form;
  - 11.1.3. bsecure Service Enabled Application Compliance Declaration;
  - 11.1.4. bsecure Service Enabled Application Certificate Management Form.
- 11.2. Subject to Condition 11.3, all communications to be sent to us by you relating to the Service can be by facsimile or by writing to Computer Banking Services and should include the Registration Reference Number.
- 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 Condition 6.4 must be given by facsimile to Computer Banking Services followed by confirmation by recorded delivery to Computer Banking Services;
  - 11.3.2. the signed original bsecure Application Form must be submitted to Computer Banking Services;
  - 11.3.3. the signed original Business Customer Authorised User Application Form must be submitted to Computer Banking Services;
  - 11.3.4. the Business Customer Authorised User Certificate Management Form must be submitted by fax followed by confirmation of the signed original to Computer Banking Services;
  - 11.3.5. the signed original bsecure Service Enabled Application Compliance Declaration must be submitted to Computer Banking Services;
  - 11.3.6. the bsecure Service Enabled Application Certificate Management Form must be submitted by fax followed

by confirmation of the signed original to Computer Banking Services.

- 11.4. We may act on any instruction, which includes the Registration Reference Number, that we receive relating to the Service that has either been signed by your Authorised Signatory or requested by an Authorised User(s).
  - 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 Identrus 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 Users shall have the same legal effect, validity and enforceability as if the data and other communications had been in writing signed by you or that Authorised User (as the case may be).
- 12.2. You and your Authorised Users 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 Users solely on the basis that it is in digital rather than written form.
- 12.3. You and your Authorised Users 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 Co-operative Bank 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 bsecure Application Form and the other documents listed in Condition 11.1. You will promptly notify us of any changes to the information described in this Condition 14.1.
- 14.2. You will verify all information supplied to us that has been supplied by your Authorised Users in relation to the Service.
- 14.3. You will ensure that on receipt of each Personalised Smart Card, each of your Authorised Users verifies that the information contained in the Certificates on the Personalised Smart Cards 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 User or a bsecure 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 Identrus scheme.

## 16. Transfer of Information

- 16.1. Subject to Condition 16.2, we will ensure that all information about you, your Authorised Users 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 Condition 11 or 25.
- 16.2. Without prejudice to Condition 3.1.3, you acknowledge that The Co-operative Bank plc, other Participants, Identrus 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 Users 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 to treat (and to ensure that your Authorised Users treat) any information received through the Service about other Customers as Confidential Information in accordance with Condition 19.

## 17. Data Protection

- 17.1. Subject to those provisions below the heading "Using and Sharing your Information, 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 Condition 17 "personal data" and "processing" shall have the meanings ascribed to them in the Data Protection Act 1998.



### 17.4 Using and Sharing Your Information

Your information may be held by us in any form and on any Group database and used by us and the Group for the purposes set out below.

We and the Group may use, analyse and assess your information to maintain and develop our relationships with you. This may include the following purposes:

- to consider any applications made by you;
- helping us to make credit decisions about you and anyone to whom you are linked financially or other members of your household;
- to deal with your account(s) or run any other services we provide to you;

- to consider and implement business, product and technology developments;
- to undertake statistical analysis, financial risk assessment, money laundering checks (which may include telephoning you), compliance and regulatory reporting, fraud prevention and debt tracing;
- to help us or our insurance underwriters to make decisions on insurance proposals and claims such as motor, household, credit and life and other insurance proposals and insurance claims for you and anyone else linked to your insurance proposal or claim
- to help us identify products and services which may be of interest to you (unless you have asked us not to);
- meeting any obligations we may have under the card scheme your card is issued under.

We may link your information between your account(s) and other products and services you have with us or the Group and with information about others with whom you have a financial link.

We and the Group may identify and tell you by letter, telephone, fax, including automated dialling, e-mail or any other means of communication about products and services which may be of interest to you and which are offered by us, the Group or other carefully selected organisations or companies (if you do not wish to receive such information please write to us at Customer Services, The Co-operative Bank p.l.c., P.O. Box 250, Skelmersdale, WN8 6WT for more details, but please note this may mean you will not receive information about business, product or service developments which may be of benefit to you). You do agree that we can forward any newsletter, statement message, new terms and conditions or information about any changes to the way your account(s) operate or provide information on card carriers.

We will disclose information outside the Group only:

- where you have provided your agreement;
- to our agents or subcontractors for operational reasons;
- to our affinity partner(s) if you have an affinity product(s);
- to any persons, including, but not limited to, insurers, who provide a service or benefits to you or for us in connection with your account(s);
- to licensed credit reference agencies as set out below;
- to fraud prevention and other agencies to help prevent crime or where we suspect fraud;
- if compelled to do so by law;
- for the purpose of compliance and regulatory reporting (for example to the Banking Code Standards Board or Mortgage Code Compliance Board) and to confirm your identity for money laundering purposes, which may include checking the electoral register;
- to any person to whom we will or intend to transfer our rights or obligations;
- if your card or PIN are lost or stolen, or to meet any obligation we may have under any card scheme your card is issued under.

We may disclose your information to licensed credit reference and/or fraud prevention agencies to help make financial or insurance proposals and claims decisions (this will be during the application process and on an ongoing basis, to decide whether to continue to make products or services available to you or adjust any level of credit) for you and anyone with whom you are linked financially or other members of your household – our enquiries or searches may be recorded – and credit reference agencies may supply us with financial information.

We may also disclose information to licensed credit reference agencies about how you conduct your account(s) and this information may be shared with other financial institutions to help make financial decisions about you and

anyone with whom you are linked financially or other members of your household. If you borrow and do not repay in full and on time, we may tell credit reference agencies who will record the outstanding debt.

A link between joint applicants and/or any individual identified as your financial partner will be created at credit reference agencies, which will link your financial records. You and anyone else with whom you have a financial link understand that each other's information will be taken into account in all future applications by either or both of you. This linking will continue until one of you successfully files a disassociation at the credit reference agencies.

You agree that your information may be transmitted to, from and/or through any country as a result of your use of your account(s) and any services which form part of your account(s) irrespective of the levels of data protection provided in any particular country and at your own risk. If we transfer your information to an agent or subcontractor who provides a service to us in another country outside the European Economic Area we will ensure they agree to treat your information with the same level of protection as us.

If you write to us and pay a fee you have a right of access to your information held by us. Write to us at Customer Care, The Co-operative Bank p.l.c., P.O. Box 101, 1 Balloon Street, Manchester, M60 4EP.

You have a right of access to your information held by credit reference agencies on payment of a fee. If you ask we will tell you the name and address of the credit reference agencies we may use.

We may record and/or monitor telephone calls to enhance security, sort out complaints, improve our customer service and for staff training purposes.

## 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 Users as part of the Service from time to time and you acknowledge that we and/or Idenirus 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 Co-operative Bank plc's trade marks, trade names, logos or designs.
- 18.3. You acknowledge that Idenirus is the sole and exclusive owner of all rights, title and interest in and to the Idenirus 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 Idenirus 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 Users 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 condition 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 Condition 20. Where the Hardware and/or Software is subject to a licence granted by a Third Party Product Provider, the provisions of Condition 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 Users 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 attempt to do any of the following or allow your Authorised Users 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 Condition 20 shall terminate on termination of this Agreement.
- 20.5. You shall have no right to bsecure, sub-license or otherwise transfer any rights in any Hardware or Software without our prior written consent.
- 20.6. Identrus may in its own right enforce this Condition 20.
- 20.7. You acknowledge and agree that:
- 20.7.1. the licence granted by this Condition 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 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 Condition 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 Condition 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 User 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 Identrus 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 User 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 Users 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 Condition 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 User 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 Users':
- 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 Identrus 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, 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 Users; or
- 23.2.2. a given Authorised User's access to the Service where the Service has not been used by that Authorised User during the immediately preceding 90 day period.
- 23.3. Where access has been suspended under Condition 23.2, we will reactivate your access to the Service if you instruct us by re-submitting a request for reactivation in accordance with Condition 11.
- 23.4. We may suspend and/or revoke Certificates issued to you and/or your Authorised Users to protect our interests, our customers interests or Identrus'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 Condition 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 Users 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 Users 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 Users' 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 Users 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 Condition 24.

### 25. Notice

- 25.1. Notices served by you under this Agreement must be made in writing to Computer Banking Services and be signed by your Authorised Signatory.
- 25.2. Notices to be served by us under this Agreement shall be given to the primary or secondary contacts specified on the bsecure 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 Conditions 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 Condition 28, shall be settled in accordance with our Dispute Resolution Procedure for the bsecure Service.
- 28.2. You agree that any dispute between you and any Participant (other than us) and/or Identrus or any dispute with us that involves related claims by or against other Participants and/or Identrus arising out of or in connection with the Service or the Identrus Scheme shall be finally settled pursuant to the Identrus 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 Identrus 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 Co-operative

Bank 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. We reserve the right to change any aspect of the Service or vary the terms of except as provided in Condition 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, if such are to your disadvantage. Any other changes can be effected immediately and we will notify you direct within days of the change.

### **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.

“Authorised User” means any person issued with a Personalised Smart Card at your request pursuant to the procedures set out in Condition 3.

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

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

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

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

“bsecure Service Enabled Application Compliance Declaration” means the document that forms part of the Agreement between you and The Co-operative Bank 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.

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

“bsecure Application Form” means the application form for the Service that forms part of the Agreement between you and The Co-operative Bank plc.

“Business Customer Authorised User Application Form” means the application form to be used for the nomination of Authorised Users of the Service that forms part of the Agreement between you and The Co-operative Bank plc.

“Business Customer Authorised User Certificate Management Form” means the form to be used for the deletion, suspension and re-activation of Authorised Users of the Service that forms part of the Agreement between you and The Co-operative Bank 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 Identrus Scheme.

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

“Computer Banking Services” means the telephone line maintained by us to receive reports of security incidents, or suspected incidents, concerning the Service: Tel: 08457 616 616, Fax: 0161 480 2501 and the Office maintained by us to which Customer application details and notices relating to the Agreement are to be addressed. Contact details Computer Banking Services, The Co-operative Bank plc, Kings Valley, Yew Street, Stockport SK4 2JU. Tel: 08457 616 616, Fax: 0161 480 2501, E-Mail: computer.banking@co-operativebank.co.uk

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

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



“Customer Service Manager” means Computer Banking Services, The Co-operative Bank plc, Kings Valley, Yew Street, Stockport SK4 2JU. Tel: 08457 616 616, Fax: 0161 480 2501, E-Mail: computer.banking@co-operativebank.co.uk

“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 bsecure 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 Identrus Dispute Resolution Procedures and the Dispute Resolution Procedure for the bsecure Service.

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

“Hardware” means any equipment provided to you by us or on our behalf for use of the Service including, without limitation, Personalised Smart Card(s), Smart Card 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.

“Helpdesk” means the Customer Helpdesk maintained by us to provide information and assistance to you in relation to the Service. Contact details Computer Banking Services, The Co-operative Bank plc, Kings Valley, Yew Street, Stockport SK4 2JU. Tel: 08457 616 616, Fax: 0161 480 2501, E-Mail: computer.banking@co-operativebank.co.uk

“Identity Certificate” means a Certificate that is issued by an Issuing Participant to a Subscribing Customer under the Identrus 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.

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

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

“Identrus Scheme” means the infrastructure and scheme operated by Identrus 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 Identrus Scheme, its Private Key and corresponding Public Key.

“Personalised Smart Card” or “Smart Card” means a card containing a computer chip that meets the specifications and standards specified by Identrus.

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

“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 Identrus Scheme that a Customer may apply to electronic data for identification purposes to generate a digital signature.

“Registration Reference Number” means the twelve (12) character identifier generated by us at the time of your application.

“Relationship Manager” means the individual identified on the bsecure 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 Identrus Scheme to a Relying Customer and that has entered into a Customer Agreement with that Relying Customer.

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

“Service Owner” means The Co-operative Bank plc, Identrus Programme Director, Level 6, Drapers Gardens, 12 Throgmorton Avenue, London EC2N 2DL.

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

“Software” means the software provided, or otherwise made available, to you by or on behalf of The Co-operative Bank 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 Co-operative Bank plc”, “we”, “our”, “us” means The Co-operative Bank plc.

“The Co-operative Bank Policy Approval Authority” means the authority established within The Co-operative Bank 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 Co-operative Bank plc for the provision of the Service.

## **SCHEDULE B**

### **The bsecure 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 bsecure 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 Computer Banking Services 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 Smart Card, PIN, HSM (if applicable) and Private Keys.
  - Request Certificate issuance, suspension, re-activation and revocation concerning your Authorised Users 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 Smart Cards following Certificate renewal.
5. 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 bsecure Service Charges Schedule**

Please contact your Relationship Manager or Computer Banking Services for a current copy of the Charges Schedule for the bsecure Service.

## **SCHEDULE E**

### **The bsecure 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).