BT Managed Public Key Infrastructure Security Service Annex

BT Reference No. **-**** -*****

1 Definitions

The following definitions apply, in addition to those in the General Terms and Conditions and the General Services Schedule.

"AA Kit" means the BT Equipment, Software drivers and Automated Administration Certificate.

"AA Software" means the Software provided as part of Automated Administration.

"Activation" means the preparation of the Control Centre and associated Service(s) for the Customer's account by the Helpdesk, and the activation of the CA(s) as part of the Customer's BT Managed PKI Security Single Application.

"Administrator Certificate" means a Certificate provided solely to the Administrator for the purposes of managing the LRA on behalf of the Customer.

"Agreement" means this Service Annex, the General Services Schedule, the General Terms and Conditions, the Order Form and the Charges List, which in the event of conflict rank in the order of precedence set out herein.

"BT CPS" means the BT Certificate Practice Statement, which is a statement of the practices and procedures which BT uses to manage and operate the BT Public Certification Services, as amended from time to time by BT.

"CA" means a Certification Authority which is a function responsible for issuing End User Certificate(s) to End User(s).

"CGI Script" means a computer code script written in Common Gateway Interface, which is a protocol for passing data between web servers and a software application screen.

"CRL" means a Certificate Revocation List which is a computer file containing an entry for all Certificates issued under the appropriate hierarchy which have been revoked before their expiry date.

"CSV file" means a comma-separated values file, which is a computer file, containing a series of text values separated by a comma, which can be read by a relational database application.

"Customer Data" means information about the Customer, Administrator, System Administrator or End User, which may include personal data subject to laws or regulations, provided by the Customer on the Order Form or otherwise in writing as part of the Order process.

"CVM" means Certificate Validation Module which is a Software patch provided by BT to validate Certificates.

"Directive" means the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

"End User" means the Customer, or a person who applies via the Customer, and who will use the End User Certificate(s).

"End User Certificate" means the Certificate provided by BT to End User(s).

"End User Page" means an HTML coded page(s) for the use of the Customer and the Customer's End

User(s).

"HTML" means Hypertext Markup Language, which is a set of symbols or codes inserted into a file intended for display on an Internet browser.

"IA" means an Issuing Authority, which is the function that performs the task of issuing End User Certificates to End User(s).

"LDAP" means Lightweight Directory Access Protocol, a directory architecture protocol which operates over TCP/IP.

"LH Software" means the Local Hosting Software which comprises CGI Scripts and executable code to allow locally hosted End User Pages to function with the Customer's BT Managed PKI Security Service.

"LRA" means a Local Registration Authority.

"Minimum Period" means a period of 365 days from and including the Operational Service Date.

"ODBC" means Open Database Connectivity, which is a standard or open application programming interface for accessing a database.

"Operational Service Date" means the date that the first Administrator first completes the on-line ordering/ registration process.

"Passcode Authentication" means a temporary password provided via the Administrator to an End User which is used to identify the End User to BT when downloading their End User Certificate.

"PCS" means BT Managed PKI Security Public Certification Services, which provide Certificates under a Public Hierarchy to the Customers and End Users in accordance with the BT CPS.

"Period" means any consecutive period of 365 days following the Minimum Period.

"PKI" means Public Key Infrastructure.

"PIN" means an alphanumeric pass code.

"Pre-Production Service" means the Service provided by BT on which BT will perform Set Up of the Customer's Managed PKI Security, enabling the Customer to integrate and test the Service.

"Private Hierarchy" means a single CA or hierarchy of CAs chained up to a common Root Key which belongs to the Customer and is not generally available in the public domain.

"Private Key" means a mathematical key (kept secret by the Customer, Administrator or End User) which interfaces with the matched Public Key and which may be used to: (i) create a Digital Signature; (ii) encrypt and decrypt files or messages and (iii) provide proof of identity to access secure web sites.

"Public Hierarchy" means a hierarchy of CAs chained up to a common Root Key which is available in the public domain.

"Public Key" means a mathematical key that can be made publicly available. A Public Key may be used to verify signatures created with its corresponding Private Key. Depending on the algorithm used to create the Public and matched Private Key(s), the Public Key of the intended recipient may also be used to encrypt

messages or files which can then be decrypted with its corresponding Private Key.

"Qualified Certificate" means a Certificate which meets the requirements laid down in Annex 1 of the Directive and is provided by a CA that fulfils the requirements in Annex II of the Directive.

"RA Kit" means the BT Equipment (comprising a smart card to store the Administrator Certificate and a smart card reader) and Administrator Certificate.

"Real Time" means the level of computer responsiveness that an End User senses as immediate.

"Repository" means a database, accessible on-line, containing Certificates, Public Keys, Customer Data and other information relating to the Service.

"Root Key" means the Public Key of the CA at the top of the Customer's hierarchy, under which subordinate CAs and/or End User Certificate(s) may be issued.

"Seat" means an unexpired, unrevoked End User Certificate held by an individual End User.

"Secure Signature-Creation Device" means a signature-creation device that meets the requirements laid down in Annex III of the Directive.

"Set Up" means the installation and Set Up Service listed on the Charges List which is provided with this BT Managed PKI Security Service.

2 Service Overview

BT Managed PKI Security ("the Service") allows the Customer to become a LRA and manage End User enrolments for End User Certificate(s) and provides the Customer with the number of CAs, as agreed on the Order , under a Public or Private Hierarchy as follows:

(a) a LRA manages registrations, approves registrations as enrolments, performs authentication and instructs BT to issue End User Certificates to End Users on behalf of the Customer in accordance with the terms of this Service Annex;

(b) BT is the IA responsible for issuing End User Certificate(s) in accordance with the Customer's instructions; and

(c) End User Certificates will contain the Customer's legal name and department or project name, the End User's name (or alias) and e-mail address and such other Customer Data as BT determines at its absolute discretion. This combination of information uniquely identifies the End User Certificate(s).

2.1 Service Description

The Service comprises:

2.1.1 the number of CAs ordered by the Customer as stated on the Order, under which the Customer in its capacity as a LRA may request BT to issue End User Certificates;

2.1.2 a RA Kit provided to the Administrator and any additional RA Kit(s) ordered by the Customer and agreed by BT in writing. The BT Equipment needs a power supply for its operation (which must be be provided by the Customer at its expense);

2.1.3 End User Page(s) for the purpose of registration of End Users for each CA, and End User Page(s) that enable End Users to download the Root Key of each of the CAs provided as part of the Service. These End User Pages will be hosted by BT on a BT web server that is allocated a URL notified from time to time by BT to the Customer. The Customer may make changes to the End User Pages within the boundaries of the functionality provided by the software packages detailed in the on-line Administrator handbook provided by BT as amended from time to time;

2.1.3.1 for certificates issued under the PCS, the registration End User Page will inform End Users that by submitting their registration for an End User Certificate to the Administrator, they will have entered into a contract with the Customer for End User Certificates;

2.1.4 a Helpdesk which provides telephone and email support and advice to the Administrator(s) (but not directly to End Users), as follows:

- setting up of, and general configuration issues relating directly to Service components;
- assistance during initial and subsequent Administrator enrolment(s) relating directly to Service components ;
- assistance with End User registration problems relating directly to components of BT Managed PKI Security;
- any questions regarding the RA Kits; and
- manual revocation of End User Certificates in accordance with instructions given to BT by the Customer.

2.1.5 use of the Control Centre for each CA.

2.1.6 use of the on-line Administrator handbook as amended from time to time.

2.1.7 the issue of End User Certificates on a request made to BT by the Administrator providing it will not exceed the maximum number of Seats that BT has confirmed may be issued during a Period.

2.1.8 BT Managed PKI Security FastTrack is an entry-level service that can support a maximum of 1,000 End Users. The minimum licence is for 50 End Users. It is supplied without Local Hosting or Automated Administration and so the customer administrator will be required to manually authenticate all certificate requests.

2.2 Access to the Service

The Customer can access the Service as follows:

(1) Administrators: Access is available via internet facing web servers using HTTPS protocol. The web servers and application implement x.509 digital certificate based access control and role assignment.

(2) Automated RA applications: Access is available via internet facing web servers using HTTP protocol. The message content is protected x.509 digital certificate based signatures and encryption.

(3) Certificate Users: Access is available via internet facing web servers using HTTPS protocol. Any certificate requests are authenticated and approved by Customer Administrators.

(4) Relying Parties: Access to certificate revocation information is available via Online Certificate Status Protocol (OCSP) and Certificate Revocation Lists (CRLs). These are publicly available via HTTP and HTTPS protocols. The message content is signed to ensure authenticity.

2.3 Uses & Restrictions for the Service

The Service allows the Customer to instruct BT to issue End User Certificates to End Users.

- Within a Private Hierarchy, an End User Certificate may only be used within the Customer's organisational intranet or extranet environment. The Customer may place some restrictions on and alter some elements of the content of End User Certificates via the Control Centre.
- Within a Public Hierarchy, an End User Certificate may be used in a corporate or other organisational intranet or extranet environment or on the Internet. The Customer may place some restrictions on and alter some elements of the content of End User Certificates via the Control Centre.

2.4 Periods

2.4.1 The first Administrator Certificate for each CA is valid for the Minimum Period from and including the Operational Service Date, after which it will expire. If additional Administrator(s) for that CA are appointed by the Customer during the Minimum Period, their Administrator Certificate(s) will expire at the end of that Minimum Period. Where an Administrator Certificate(s) has been revoked pursuant to sections 5.1(d) and 5.1(e) a replacement Certificate may be ordered from BT and will expire at the same time as the revoked Administrator Certificate(s) would have expired. On or before expiry of an Administrator Certificate, the Customer may order a renewal Administrator Certificate by completing another Order and complying with any additional checks BT may operate to ensure that the Customer's details are correct and up to date. A renewal Administrator Certificate is valid until the end of the next Period following the Period in which it was issued. Administrator Certificates may be revoked before expiry by the earlier of the following: expiry or sooner termination of the Agreement, or this Service Annex, or otherwise in accordance with the Agreement.

2.4.2 An End User Certificate is valid for 365 days, unless otherwise limited by the Administrator at the time of instruction to BT to issue, at the end of which the End User Certificate will expire. An End User Certificate may be revoked in the event of any of the following:

(a) instructions given to BT by the End User concerned and the Customer hereby confirms End Users are authorised to give such instructions on behalf of the Customer;

(b) instructions given to BT by the Customer;

(c) termination for whatever reason of the Service provided under this Service Annex; or

(d) in accordance with the provisions of the End User's contract with the Customer for the End User Certificate.

2.4.3 At any time within a Minimum Period or a Period, End User Certificates may be issued up to the maximum number of Seats ordered by the Customer.

2.4.4 If BT or the Customer terminates Service provided under this Service Annex, Administrator(s) will be unable to carry out LRA responsibilities as described in section 5 of this Service Annex. In these circumstances, the Customer may, at its discretion, make a reasonable request to BT to revoke all the End User Certificates associated with the Customer's BT Managed PKI Security.

2.5 Reports

The Service will allow the Administrator(s) access to reporting capabilities.

2.6 Additional Services (Options)

2.6.1 Local Hosting

Local Hosting allows the Customer to:

(a) design the visual appearance of End User Pages by including the Customer's own text and branding images by use of the Customer's own software for use in conjunction with the Service; and

(b) to host those End User Pages on a server of the Customer's choice.

The customised End User Pages produced pursuant to this section 2.6.1 may be used in addition to the standard End User Pages provided and hosted by BT pursuant to the Service.

Local Hosting comprises the following elements:

2.6.1.1 Software Licence

(a) BT will provide the LH Software to the Customer by allowing the Customer to download it from a URL notified from time to time by BT.

(b) The Customer acknowledges that its licence rights and other such uses of the LH Software are contained in this Service Annex.

(c) All rights, title and interest in the LH Software and any rights, title and interest in any adaptations and anything derived from the provision of support for the LH Software; and all rights, title and interest created in the provision of Software Support shall remain the exclusive property of BT or its licensors as appropriate except as expressly provided otherwise by BT in the Agreement

2.6.1.2 Services

The following services are provided as part of Local Hosting:

(a) configuration of the Service to work in conjunction with Local Hosting;

(b) Local Hosting Support. The Helpdesk provides telephone and email support and advice only to the Administrator and System Administrator but not directly to End Users, as follows:

- assistance during initial setting up of, and subsequent, configuration issues relating directly to components of the Local Hosting as listed in this section 2.6.1;
- assistance with End User registration problems relating directly to components of the Local Hosting as listed in this section 2.6.1; and
- any questions regarding Local Hosting;

(c) use of the Control Centre in respect of Local Hosting;

(d) use of the on-line Administrator handbook in respect of Local Hosting as amended by BT from time to time.

2.6.2 Automated Administration

Automated Administration allows the Customer, without manual intervention by the Administrator, to:

(a) automatically authenticate End User registrations directly against a single table database of Customer Data provided by the Customer, using matching rules defined by the Customer in accordance with the Customer Responsibilities set out in this Service Annex, within the parameters of the Automated Administration functionality;

(b) automatically request the issue by BT of End User Certificates to End Users, where the enrolments are found to match; and

(c) refer to the Administrator all End User enrolments which are not automatically approved in accordance with section 2.6.2 (a).

The Automated Administration Services comprises the following elements:

(a) configuration of the Service to work in conjunction with Automated Administration;

(b) Automated Administration support which provides telephone and email support to the Administrator and System Administrator (but not directly to End Users) as followss:

- assistance during initial setting up of, and subsequent, configuration issues relating directly to components of the Automated Administration as listed in this section 2.6.2;
- assistance during AA Certificate enrolment(s) for Automated Administration;
- assistance with End User problems relating directly to the use of the AA Software and AA Kit as described in this section 2.6.2;
- any questions regarding the Automated Administration; and
- manual revocation of AA Certificate(s) in accordance with instructions given to BT by the Customer.

(c) use of the Control Centre in respect of Automated Administration; and

(d) use of the on-line handbook in respect of Automated Administration as amended by BT from time to time.

2.6.2.1 AA Software Performance

- BT does not warrant that the AA Software will operate uninterrupted or that it will be free from minor errors or defects which do not materially affect its performance.

- Other than as expressly provided in the Agreement, no warranties are given or assumed by BT regarding the AA Software and are hereby excluded to the extent permitted by law.

- In the event that an error or defect in the AA Software is due to faulty design, manufacture, and / or materials, and provided that the Customer reports a fault within ninety (90) days from and including the date of acceptance,
- BT shall, at its absolute discretion, and in the following order:
  (a) repair the AA Software;
  (b) replace the AA Software; or
  (c) refund the appropriate charges for Automated Administration, in which case this Service Annex shall be terminated.

2.6.2.2 Hardware

- If a material fault develops in the BT Equipment provided as a part of the Automated Administration, BT will provide a replacement and the Customer must return the faulty BT Equipment to BT. Any such replacement of BT Equipment remains the property of BT at all times.

- In event of any loss or theft of the BT Equipment, provided as part of Automated Administration, the Customer must notify BT immediately via the Helpdesk. The Customer agrees that it will pay BT for the replacement BT Equipment.

2.6.2.3 Indemnity

- the Customer must fully indemnify BT against any claims or legal proceedings which are brought or threatened against BT for or in respect of any fault or inaccuracy in the Customer Data, or the single table database.

2.6.3 Premium Revocation

The Premium Revocation Service provides the Customer with an updated CRL every hour, which will be made available in the Repository for download and use by the Customer for the purposes of validating the status of Certificates issued to the Customer and the Customer's End Users.

The Premium Revocation Service comprises :

- the provision of CRLs which will be updated hourly and immediately made available to the Customer via the Repository.
- the Premium Revocation Service support which provides telephone and email support to the Administrator(s) (but not directly to End Users) as follows:
  - assistance during initial setting up of, and subsequent configuration issues relating directly to use of the Premium Revocation Service; and,
  - answering any questions regarding the Premium Revocation Service.
- use of the Control Centre in respect of the Premium Revocation Service; and
- use of the on-line handbook in respect of the Premium Revocation Service as amended by BT from time to time.

2.6.4 Online Certificate Status Protocol Service (OCSP)

The OCSP Service provides an online access service via the Internet which enables the Customer to validate the status of Certificates issued to the Customer or the Customer's End Users against the CRL in Real Time.

The OCSP Service comprises:

- Access to an OCSP responder via the Internet enabling Real Time certificate status checking against the current CRL by customers.
- OCSP Service Support comprising telephone and email support to the Administrator and System Administrator (but not directly to End Users) in the following areas:
  - assistance during initial setting up of, and subsequent configuration issues relating directly to use of, the OCSP Service; and
  - answering any questions regarding the OCSP Service.
- use of the Control Centre in respect of OCSP Service; and
- use of the on-line handbook in respect of the OCSP Service as amended by BT from time to time.

2.6.5 Passcode Authentication

Passcode Authentication allows the Customer, without manual intervention by the Administrator , to:

(a) check and approve End User enrolments against the Customer Data contained in the CSV file based upon matching rules defined by the Customer, within the parameters of the Passcode Authentication functionality;
(b) automatically request the issue by BT of End User Certificates to End Users, where the enrolments are found to match; and
(c) refer to the Administrator all End User enrolments which are not automatically approved in accordance with section 2.6.5 (a).

The Passcode Authentication Service comprises :

(a) configuration of the Service to work in conjunction with Passcode Authentication;
(b) Passcode Authentication support which provides telephone and email support to the Administrator and System Administrator (but not directly to End Users), as follows:
- assistance during initial setting up of, and subsequent, configuration issues relating directly to components of the Passcode Authentication as listed in this section 2.6.5;
- assistance with End User problems relating directly to the use of the Passcode Authentication; and
- any questions regarding the Passcode Authentication.

(c) use of the Control Centre in respect of Passcode Authentication; and
(d) use of the on-line handbook in respect of Passcode Authentication as amended by BT from time to time.

2.6.5 Key Manager

The Key Manager option allows for the centralised generation, distribution and back-up of the private keys associated with encryption certificates so that, in the event the original key is lost or corrupted, encrypted data can be recovered. Key Manager combines software that runs on the Customer Site with a key recovery service operated by BT. The software generates the encryption key pair, requests the corresponding certificate and delivers the key and certificate to the End User. Each private key is also encrypted under a unique session key, which is then itself encrypted using a BT public key.

When a key is recovered, the Key Manager software sends the encrypted symmetric key to BT, which is decrypted and returned so that locally held private key can be recovered. This ensures that there is a clear audit trail of all key recovery transactions.

2.7 Usage & Restrictions for Additional Services

(a) The additional services must only be used for the purpose specified in this Service Annex in conjunction with the Service.

(b) The Customer shall only use the additional services for the number of CAs purchased as part of the Service.

2.7.1 Local Hosting

(a) The Customer may make copies of the LH Software for back-up purposes only. The copyright notice(s) that appear in original programs and/or on the original media on which the LH Software is delivered must be reproduced on all copies.

(b) The Customer shall not modify or enhance the LH Software or use Local Hosting in conjunction with any other software or hardware or service under any circumstances, except as specified by BT from time to time.

(c) Notwithstanding paragraph 2.7.1(d) and paragraph 2.7.1(e), the Customer acknowledges and accepts that it is the Customer's responsibility, prior to installation, and throughout the duration of this Service Annex, to ensure that its systems, software and hardware are compatible with the current Local Hosting compatibility specification as published by BT from time to time.

(d) The Customer must fully implement, within a reasonable time of instruction by BT, all maintenance releases, patches or other upgrades. .

(e) Where the Customer has requested BT to install Local Hosting, the Customer accepts that prior to installing the Local Hosting, BT shall require confirmation that the Customer has satisfied the requirements of section 2.7.1(c) above. BT shall be under no obligation to install the Local Hosting if BT considers, at its absolute discretion that the provisions of section 2.7.1(c) have not been complied with to its entire satisfaction.

(f) BT excludes all liabilities, losses and expenses relating to the Customer failing to comply with sections 2.7.1(c), 2.7.1(d) and 2.7.1(e) above, or to any corrections or restorations directly or indirectly relating to such failure to comply. The Customer acknowledges that any changes to the configuration may result in poor or non-performance of Local Hosting, and that the Customer is solely responsible, and must at its own expense, correct or restore its software and hardware configuration using its back up copies or otherwise to ensure future compliance with sections 2.7.1(c), 2.7.1(d) and 2.7.1(e).

2.7.2 Automated Administration

(a) The Customer shall not use the AA Kit other than for the specific purpose of providing secure key generation, storage and signing for the AA Certificate as part of the Automated Administration.

(b) Automated Administration requires the prior installation of Local Hosting.

(c) The Customer may make copies of the AA Software for back-up purposes only. The copyright notice(s) that appear in original programs and/or on the original media on which the AA Software is delivered must be reproduced on all copies.

(d) The Customer shall not modify or enhance the AA Software or use Automated Administration in conjunction with any other software or hardware or service under any circumstances, except as specified by BT from time to time.

(e) The Customer cannot use Automated Administration and Passcode Authentication on a single CA at the same time, and must select one at the time of installation. Following installation, the Customer may at any time choose to migrate any CA from Passcode Authentication to Automated Administration. An additional Set Up fee will be payable to BT for this work.

(f) Automated Administration must only be installed by BT or any person who is authorised by BT in writing to install Automated Administration.

(g) Automated Administration is provided as part of the Service as described in this Service Annex. No reduction of charge shall be given if the Customer chooses not to implement Automated Administration.

(h) An AA Certificate may be revoked in the event of any of the following:

- a reasonable request given to BT by the Customer;
- termination for whatever reason of this Service Annex; or
- where BT has reason to believe that there may be a compromise of the integrity of the Private Keys held on the HSM.

2.7.3 Premium Revocation

(a) BT will use reasonable endeavours to ensure the accuracy of the information in each CRL on an hourly update basis. Subsequent revocation of End User Certificates made by the Customer via the Control Centre, or subsequent revocation by End Users via the End User Pages will not be recorded until the next CRL is produced.

2.7.4 OCSP

(a) BT will ensure that information provided by the OCSP Service will reflect in Real Time the most up to date CRL listing made available by the Customer.

(b) Revocation of End User Certificates made by the Customer via the Control Centre, or subsequent revocation by End Users via the End User Pages will be recorded on the CRL in Real Time.

2.7.5 Passcode Authentication

(a) The Customer shall not use Passcode Authentication in conjunction with any other software or hardware or service under any circumstances, except as specified by BT from time to time.

(b) The Customer cannot use Automated Administration and Passcode Authentication in conjunction with a single CA at the same time, and must select one at the time of installation. Following

installation, the Customer may at any time choose to migrate any single CA from Passcode Authentication to Automated Administration. An additional Set Up fee will be payable to BTfor this work.

(c) Passcode Authentication is provided as part of the Service as described in this Service Annex. No reduction of charge shall be given if the Customer chooses not to implement Passcode Authentication.

3. Service Delivery

BT will provide the Service, configuring it to use the services selected on the Order and setting up the initial Administrator account. BT will also provide the Customer Administrator with training on the use of the Service, as set out on the Order.

3.1 Set Up comprises:

(a) Activation of the Service;
(b) Set Up of the Service, the Local Hosting and the Automated Administration or Passcode Authentication as applicable and confirmed by BT in writing on the Order;
(c) where applicable, use of the Pre-Production Service by BT on behalf of the Customer for the purposes of Set Up of the Automated Administration with the Service as detailed on the Order . Pre-Production Service comprises use of:
- a pre-production environment on which BT will perform Set Up of the Service;
- pre-production environment Certificates; and
- Software which is used for Set Up in conjunction with Pre-Production Service.

3.1.1 BT will perform Set Up at the Customer's Site, and Activation of the Service as follows:

(a) enrol onto Pre-Production Service;
(b) download and install the Pre-Production Service Administrator Certificate;
(c) configure the Service, Local Hosting, Automated Administration, Passcode Authentication, as applicable, using the Control Centre on Pre-Production Service;
(d) assist the Administrator on implementing the configuration options required by the Customer for the Service which will appear in the End User Pages hosted by BT;
(e) install the LH Software on the server chosen by the Customer;
(f) test Local Hosting using the Customer's End User Pages where available, or using the test template pages for Local Hosting, in accordance with section 3.1.3;
(g) where a server Certificate has not previously been installed on the server chosen by the Customer for use with the Service, a trial server Certificate will be installed and valid only for the purposes of Set Up and acceptance by the Customer;
(h) install the AA Kit where applicable and either install the AA Software on the server chosen by the Customer and configure for Automated Administration, or configure Passcode Authentication;
(i) enrol for, download and install the Pre-Production Service AA Certificate, where applicable, onto the server chosen by the Customer;
(j) either test Automated Administration against a test file provided by BT; or test Passcode Authentication;
(k) where applicable, install the Directory Integration, configure the Directory Integration interface which shall be an LDAP or ODBC interface, to retrieve data from the Customer's existing LDAP directory or ODBC compatible database, or where this is not provided, against a test file;
(l) install the RA Kit;
(m) assist the Administrator in enrolling for the Service on behalf of the Customer;
(n) download and install the Administrator Certificate onto the RA Kit;
(o) download and install the AA Certificate onto the AA Kit;

(p) modify the Local Hosting, Automated Administration or Passcode Authentication and URLs associated with the Service to point at the production platform instead of the Pre-Production Service, and demonstrate its functionality;
(q) advise the Customer how to use the Control Centre provided as part of the Service;
(r) configure the HTML pages to the Customer's URL and install the Customer's logo;
(s) enrol for a server Certificate and install on Customer's server where this has been ordered in advance and is available to install. Where such a Certificate is not available a trial server Certificate, with limited validity, will be installed for acceptance testing purposes and the System Administrator will be responsible for installing the server Certificate when it is available;
(t) demonstrate Certificate management functionality provided to the Administrator in the Control Centre to the Customer, and demonstrate the part that the Control Centre plays in this process; and
(u) advise the Customer of the recovery process that should be in place in the event of server failure. BT may provide assistance with recovery subject to mutual agreement with the Customer on the scope of the recovery, however BT will not assist with recovery if the recovery process is not in place.

3.1.2 **Enrolment Information and Confirmation**

The Customer must provide the following information for each subordinate CA and for the superior IA:

(a) the name and contact details of the Administrator completing the Order for the CA on behalf of the Customer and any additional Administrator(s);
(b) the Customer's legal name;
(c) the Customer's department or project name;
(d) the Customer's registered address (including country and post code) and contact details;
(e) details of the Customer's billing contact person(s);
(f) the reference number of the Customer's relevant purchase order (if any) for invoicing purposes;
(g) a challenge phrase (to later authenticate the Customer to BT);
(h) proof of the Customer's legal status (to be verified via third-party database checks or comparable alternative measures, at BT's discretion);
(i) the number of Seats required; and
(j) sufficient information, as requested by BT, to allow BT to approve the designated Administrator(s) and issue the Administrator Certificate(s) for each CA.

The Customer may also opt to provide its Dun and Bradstreet D-U-N-S Number to speed processing of the Order .

3.1.3 Acceptance

3.1.3.1 The Customer must sign an acceptance form to confirm that:
(a) the Service has been installed and tested to the Customer's reasonable satisfaction;
(b) the Service is functioning free from errors at the time of testing;
(c) the End User Pages, in accordance with section 3.1.1(f), are installed and are interfacing with the Service; and
(d) BT has fully met all its obligations relating to Set Up of the Service.

3.1.3.2 Activation of all CAs associated with the Service, and Set Up of all associated Software and BT Equipment must take place during a single Set Up Period which shall end on the Operational Service Date. If a Customer wishes Activation of a CA or service associated with the Service after that time, the Customer must purchase additional Set Up from BT.

3.1.3.3 All charges for Set Up of the Service will be invoiced after the Customer confirms acceptance in accordance with section 3.1.3.

3.1.3.4 The Minimum Period will commence on the Operational Service Date for the Service. Use of Pre-Production Service is included within that Minimum Period.

3.1.3.5 Pre-Production Service must only be used by BT or any person who is authorised by BT in writing. The Customer acknowledges that Pre-Production Service will be withdrawn after the Customer confirms acceptance in accordance with section 3.1.3.

3.2 **Third-Party Confirmation of Customer Information**

3.2.1 Upon receipt of the completed Order supplied by the Customer, BT or it's agent will verify that data with information held in third-party databases, by making appropriate inquiries with those third parties, including at BT's discretion government entities and credit vetting agencies. BT will use a telephone number listed with a third-party database to confirm certain information with the Customer.

3.2.2 If the databases or other applicable resources available to BT or its agents do not contain all the information required, the Customer may be required to provide additional information and proof.

3.2.3 BT will not provide the Service to the Customer and this Service Annex will be terminated if;

(a) the Customer fails to provide any information or any further information requested by BT or BT's agent; or

(b) any information is not verified or verifiable to BT's complete satisfaction; or

(c) the Customer fails or refuses to co-operate with BT's efforts to verify the Customer's details.

4 BT Service Management Boundary (SMB)

The SMB for the Service is the front-end firewall on the Service platform. Connection to the Service platform and the hardware and software used to access the Service are the responsibility of the Customer.

5. The Customer's Responsibilites

5.1 For each CA, the Customer must:

(a) appoint one or more Administrator(s), who will operate the LRA on behalf of the Customer, provide BT with the Administrator(s) contact details and inform BT immediately of any changes to this Customer Data. For the benefit of End Users, the Customer warrants to BT that the Administrator consents to the publishing of these details as the End User support contact. The Customer also warrants that all Administrators have consented to the holding, processing and disclosing of all personal data of the Administrator in accordance with this Service Annex;

(b) ensure that any Administrator is a trustworthy individual deemed appropriate to perform End User Certificate management duties, including without limitation security administration, human resource or personnel management, and network administration. The Customer must ensure that the Administrator has adequate training in these and any other relevant areas as recommended in the on-line Administrator handbook;

(c) require and ensure that the Administrator(s) comply fully with the terms of the Agreement;

(d) appoint a new Administrator and promptly request BT to revoke the original Administrator's Certificate, where that Administrator ceases to have the Customer's authority or fully satisfy section 5.1(b) of this Service Annex;

(e) within 4 hours of the Customer becoming aware or having reason to believe that there has been a Compromise of an Administrator's Private Key; or an Administrator being no longer entitled to act as an Administrator, the Customer or any other Administrator will request BT to revoke that Administrator Certificate;

(f) if relevant ensure that an Administrator Certificate and corresponding key pair is promptly erased from the BT Equipment within 4 hours of the revocation of that Administrator Certificate;

(g) provide helpdesk support to End Users who have applied for Certificates via the Customer; and

(h) notify End Users of revocation of their End User Certificates. This is the sole responsibility of the Customer.

5.2 The Customer acknowledges that by purchasing the Service, the Customer agrees to undertake LRA responsibilities for each CA which will materially affect the content and use of End User Certificates. LRA responsibilities include the obligation to validate registration and enrolment data submitted by End Users, management of End User Certificates, and to comply with this paragraph 5. In its capacity as a LRA, the Customer must:

(a) approve or reject requests for End User Certificates, based on the criteria determined by the Customer, including criteria requirements notified by BT from time to time;

(b) ensure as a minimum that all End Users are either officers, directors, employees, or (if the Customer is an unincorporated partnership) partners of the Customer; or persons maintaining a prior legal or contractual relationship with the Customer which does not solely relate to the provision of End User Certificates. In all cases the Customer must have business records to demonstrate the relationship with End Users;

(c) request BT to revoke an End User Certificate in the event that the End User no longer meets the Customer's qualifying criteria (including those matters set out in section 5.2(b)) to have an End User Certificate. The Customer must obtain authority to act as the End User's agent for this purpose and will produce such authority at BT's request; and

(d) before the Customer may request BT to issue an End User Certificate, fully comply with sections 5.2(a) and 5.2(b) of this Service Annex.

5.2.1 In addition, PCS Customers must:

(a) ensure End Users enter into an agreement with the Customer that binds them to the terms of this Service Annex and ensures that End Users:

- submit accurate and complete enrolment information;
- exercise reasonable care to avoid the unauthorised disclosure of the Private Key;
- notify the Customer without any unreasonable delay if:
  - the Private Key is lost, stolen or compromised;
  - control over the Private Key has been lost due to a compromise of activation data; or,
  - they are notified of any inaccuracy or change to the certificate content.

(b) act in accordance with all instructions and notices from BT in connection with the PCS.

5.2.2 End Users applying for Qualified Certificates must:

- ensure that the Public and Private Keys:
  - are generated within a Secure Signature-Creation Device;

- are generated using an algorithm recognised as being fit for the purpose of a Qualified Electronic Signature; and,
- uses a key length and algorithm that is recognised as being fit for the purpose of a Qualified Certificate.

- acknowledge that BT may suspend or terminate a Qualified Certificate if BT reasonably suspects that a Qualified Certificate has been stolen or compromised.
- consent to the passage of data to a third party for the provision of the Qualified Certificate.

5.3 The Customer warrants that the Administrator for each CA will:

(a) comply fully with the terms of the Agreement;

(b) at all times act in a competent and professional manner;

(c) use only BT Equipment, hardware and software which have from time to time been designated by BT in connection with the Service;

(d) use the Service (including any hardware, Software, or information provided by BT in relation to the Service) only for its authorised and intended purpose;

(e) retain at all times personal responsibility for the control of, and not permit unauthorised, unattended or shared access to, any information, documentation, BT Equipment or software provided to the Customer by BT under this Contract. This includes without limitation the RA Kit, the associated Public Key and Private Key pair, or any similarly sensitive information relating to the Service;

(f) store the BT Equipment in a secure, lockable container (when not in use) accessible only by the applicable Administrator;

(g) follow guidance on the detailed LRA procedures set out in the on-line Administrator handbook. Additionally, for PCS Customers, follow guidance set out in the BT CPS. BT strongly recommends that the Administrator reads and follows these documents;

(h) act as support in respect of the Customer's End Users; and

(i) return as directed by BT the BT Equipment on termination of Service provided under this Service Annex.

5.4 The Customer warrants that the Administrator for each CA will, in respect of the validation of End User registrations:

(a) Confirm:

- that the End User requesting an End User Certificate is the person identified on the application;
- that the End User rightfully holds the Private Key corresponding to the Public Key to be listed in the End User Certificate; and
- that the information provided is accurate;

(b) confirm the End User's suitability to receive an End User Certificate on the basis of the criteria determined by the Customer, including criteria from time to time notified by BT;

(c) request BT to revoke an End User Certificate:

- within 8 hours of the Administrator(s) knowing or having reason to believe that there has been Compromise of the End User's Private Key; or
- where the End User is no longer entitled to have the End User Certificate (including where section 5.2.1 is applicable).

In addition, for PCS Customers the Administrator will:

(d) require End Users receiving End User Certificates to enter into a contract with the Customer.

In addition, for End Users registering for Qualified Certificates, the Administrator will:

(e) confirm:

- that the End User requesting an End User Certificate has been authenticated to the policy requirements for Certificate Authorities issuing Qualified Certificates as set out in Section 7.3.1 of the European Telecommunications Standards Institute Document TS 101 456 V1.2.1 April 2002 or the corresponding section in the then current version of the same, and;
- that the Private Key corresponding to the Public Key to be included in the End User Certificate has been generated on and is solely stored on a Secure Signature-Creation Device.

5.5 The Customer must fully indemnify BT against any claims or legal proceedings which are brought or threatened against BT by an End User or any other third party:

(a) in relation to any act or omission of the Customer; or

(b) in connection with any relationship between the Customer and the End User or any other third party.

5.6 The Customer acknowledges that End User Certificate(s) and Administrator Certificate(s) are issued by BT on the Customer's instructions and that the contractual relationship with respect to End User Certificates is between the Customer and End User.

5.7 The Customer agrees that the information on the Repository will be made publicly available via the Repository or otherwise.

5.8 The Customer warrants that it has obtained all rights, consents and permission required from all End Users, for the copying, disclosure, use and transmission of all Customer Data to BT or it's agents.

5.9 Where applicable, it is the responsibility of the Customer to ensure that:

5.9.1 the CRLs made available by BT under the Premium Revocation Service are downloaded to the Customer server, and BT accepts no responsibility for failure of the Customer to perform this operation.

5.9.2 the OCSP Service remains online in order for the CRL information produced by OCSP to be made available for use in Real Time; and

5.9.3 the information on the CRL is accurate and up to date.

5.10 BT accepts no responsibility for failure of either the Customer or the Customer server to perform the requirements in paragraphs 5.9.2 and 5.9.3.

5.11 Local Hosting (Optional)

The provision of support for the LH Software as described in section 5.11.3 is subject to the Customer complying with all of the following:

(a) providing adequate information to enable BT to diagnose any errors in the LH Software;
(b) implementing the latest maintenance releases, patches or other upgrade instructions as required by section 2.7.1(d); and
(c) complying with the terms of this Service Annex.

5.11.1 BT does not warrant that the LH Software will operate uninterrupted or that it will be free from minor errors or defects which do not materially affect its performance.

5.11.2 Other than as expressly provided in the Agreement, no warranties are given or assumed by BT regarding the LH Software and are hereby excluded to the extent permitted by law.

5.11.3 In the event that an error or defect in the LH Software is due to faulty design, manufacture, and / or materials, and provided that the Customer reports a fault within ninety (90) days from and including the date of acceptance, BT shall, at its absolute discretion, and in the following order:

(a) repair the LH Software;
(b) replace the LH Software; or
(c) refund the appropriate charges for Local Hosting which shall terminate this Service Annex.

5.12 Automated Administration (Optional)

5.12.1 The Customer must appoint a System Administrator(s) who should:

(a) be present throughout Set Up to familiarise themselves with any configuration processes that may assist them during the performance of the Customer's System Administrator functions;
(b) be responsible for installing such maintenance releases, patches and other upgrades released by BT from time to time in accordance with instructions provided by BT; and
(c) be responsible for removing and replacing the BT Equipment if it becomes faulty, and returning it to BT.

5.12.2 The Customer is solely responsible, and must at its own expense, correct or restore its software and hardware configuration using its back up copies or otherwise to ensure future compliance with sections 2.7(b), 2.7.2(d) and 5.12.4.

5.12.3 Within 4 hours of the Customer becoming aware or having reason to believe that there has been a Compromise of an AA Certificate Private Key, the Customer or any other Administrator, or System Administrator will notify BT to revoke that AA Certificate.

5.12.4 Notwithstanding sections 2.7.2(d) and 5.12.1, it is the Customer's responsibility, prior to installation, and throughout the duration of this Service Schedule, to ensure that its systems, software and hardware are compatible with the current Automated Administration compatibility specification as published by BT from time to time.

5.12.5 Prior to installation of the Automated Administration, BT shall require confirmation that the Customer has complied with the requirements of section 5.12.4 above. BT shall be under no obligation to install the Automated Administration if BT considers, at its absolute discretion, that the provisions of paragraph 5.12.4 have not been complied with to its entire satisfaction.

5.12.6 BT excludes all liabilities, losses and expenses incurred by the Customer failing to comply with this Service Annex, or relating to any corrections or restorations directly or indirectly relating to such failure to comply.

5.12.7 The Customer acknowledges that failure to comply may adversely affect the performance of Automated Administration.

5.12.8 AA Software Performance

The provision of support for the AA Software as described in section 2.6.2.1 is subject to the Customer complying with all of the following:

(a) providing adequate information to enable BT to diagnose any errors in the AA Software;
(b) implementing the latest maintenance releases, patches or other upgrade instructions as required by section 5.12.1(b); and
(c) complying with the terms of this Service Annex.

5.13 Passcode Authentication

It is the responsibility of the Customer to ensure that the CSV file is produced to the specification described from time to time in the Administrator's handbook.

5.14 Set Up

The Customer must appoint a Administrator(s) who should:

(a) be present throughout the Set Up of the Service to familiarise themselves with any configuration processes that may assist them during the performance of the Customer's System Administrator functions.
(b) be responsible for installing such maintenance releases, patches and other upgrades released by BT from time to time in accordance with instructions provided by BT; and
(c) be responsible for removing and replacing the BT Equipment if it becomes faulty as instructed by BT.

The Customer is responsible for designing its own End User Pages for use with Local Hosting, using the Customer's own software. These End User Pages must be available at the time of installation if the Customer wishes these End User Pages to be tested in accordance with section 3.1.1 (f).

5.15 End User Certificates

End User Certificates are for issue to End Users only as follows:

(a) End User registrations to BT for End User Certificates are made through an BT Managed PKI Security Customer. The issue of an End User Certificate is subject to this Service Annex;
(b) any End User Certificate issued will contain the BT Managed PKI Security Customer's legal name, department or project name, the End User's name (or alias) and e-mail address and such other Customer Data as BT determines at its absolute discretion. This combination of information uniquely identifies the End User Certificate.

5.15.1 Uses

Within a Public Hierarchy, End User Certificates may be used in corporate or other organisational Intranet or extranet environment or on the Internet. The BT Managed PKI Security Customer may place some restrictions and alter some elements of the content of End User Certificates via the Control Centre.

5.15.2 Periods

- An End User Certificate is valid for 365 days from the date that the Customer Administrator requests BT to issue the Certificate to the End User unless otherwise limited by the Customer at

the time of request to BT to issue, at the end of which the End User Certificate and this Service Annex will expire. An End User Certificate may be revoked in the event of any of the following:

(a) a reasonable request given to BT by the End User;
(b) instructions given to BT by the Customer, and the End User hereby confirms the Customer is authorised to give such instructions on behalf of the End User;
(c) termination for whatever reason of the Service; or
(d) in accordance with the provisions of this Service Annex.

5.15.3 End User Certificate Registration

The registration process for End User Certificates is as follows:

(a) the End User will complete the registration End User Page. This page will inform the End User that by submitting their registration for an End User Certificate to the Administrator, they will have entered into a contract with the Customer for End User Certificates issued under the PCS;
(b) the Customer receives End User registrations for End User Certificates, approves the registrations as enrolments, performs authentication of these enrolments and requests issuance of an End User Certificate by BT to the Customer; and
(c) the authentication of an enrolment for an End User Certificate will only be approved by the Customer if the End User is able to demonstrate certain specific criteria to BT's satisfaction. This includes:
- the End User's affiliate relationship with the Customer; and
- the validation of the End User's enrolment information.

The End User must provide the following information when applying for an End User Certificate:

(a) name (or alias);
(b) Private Key;
(c) e-mail address;
(d) challenge phrase (to later authenticate the End User to BT); and
(e) other information which may be required by the BT Managed PKI Security Customer with which the End User is affiliated, and such other information as reasonably required by BT.

An End User Certificate will not be issued to the End User, and this Service Annex will be terminated, if any of this information is either not provided by the End User, or is not verified or verifiable to the Customer's and BT's complete satisfaction.

The End User acknowledges that the Customer Data will be made available to the Customer.

5.15.4 Certificate Delivery Process

- On or after the Operational Service Date, BT will send the End User a PIN at the e-mail address specified by the End User on the registration End User Page.
- To collect the End User Certificate, the End User enters their PIN on the download End User Page, together with the presentation of their correctly corresponding Private Key by the End User's browser.
- A copy of the End User's Public Key will be made publicly available via the Repository or otherwise.
- The End User agrees that the information on the Repository will be made publicly available via the Repository or otherwise.

6 Charges and Payment Terms

The charges for the Service will comprise some or all of the following components, depending on the option selected on the Order:

Product	One-time Charge	Recurring Charge	Notes
BT Managed PKI Security		Annual Charge	Payable on the Operational Service Date and each anniversary thereafter.
Local Hosting			Included as part of the Service (excluding BT Managed PKI Security FastTrack)
Automated Administration			Included as part of the Service (excluding BT Managed PKI Security FastTrack)
Premium Revocation		Annual Charge	Optional Service
OCSP		Annual Charge	Optional Service. The OCSP annual licence includes Premium Revocation if required.
Key Manager		Annual Charge	Optional Service
Password Authentication			Included as part of the Service (excluding BT Managed PKI Security FastTrack)
Set Up	Install		Payable on the Operational Service Date

7 Service Levels

The Service is provided on a resilient platform within BT data centres, which is scheduled to be available 24 hours per day, 7 days per week, 365 days per year. The Service has a target of 99.5% availability within any calendar month. This target excludes all periods of Planned Maintenance or any emergency maintenance or updates. Whilst BT will make all reasonable efforts to meet and exceed this monthly target availability, it accepts no liability whatsoever for any failure to meet this target.