BT Managed Public Key Infrastructure Security Schedule to the General Terms

Contents

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

Words that are capitalised but have not been defined in this Schedule have the meanings given to them in the General Terms.

Part A – The Service

1 Service Summary

BT will provide you with a set of managed services that will enable you to become a Local Registration Authority (LRA) and manage End User enrolments for End User Certificate(s) under a Public or Private Hierarchy, comprising:

1.1 the Standard Service Components; and

1.2 any of the Service Options as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 (the "**PKI Security Service**").

2 Standard Service Components

BT will provide you with all the following standard service components ("**Standard Service Components**") in accordance with the details as set out in any applicable Order

2.1 **CAs**: BT will provide you with the number of CAs as set out in any applicable Order.

2.2 **RA Kit**: BT will provide you with a RA Kit for the Administrator and any additional RA Kit(s) as set out in any applicable Order.

2.3 **End User Page(s)**:

2.3.1 BT will provide you with End User Page(s) for the purposes of:

(a) registering End Users for each CAs; and

(b) enabling End Users to download the Root Key of each of the CAs provided as part of the PKI Security Service.

2.3.2 BT will host the End User Pages on a BT web server that is allocated a URL.

2.3.3 You may make changes to the End User Pages within the boundaries of the functionality provided by the software packages as set out in the Administrator Handbook.

2.4 **Certificate Revocation List (CRL)**: BT will provide you with a daily update to the CRL.

2.5 **Support Service**: BT will provide you with a Service Desk to support and advice you on:

2.5.1 set up and general configuration of the PKI Security Service;

2.5.2 Administrator and AA Certificate enrolment(s);

2.5.3 End User registration issues

2.5.4 questions regarding the PKI Security Service; and

2.5.5 manual revocation of End User Certificates or AA Certificates in accordance with BT's instructions.

2.6 **Control Centre**: BT will provide you with a Control Centre for each CA;

2.7 **Administrator Handbook**: BT will make available in the Control Centre a handbook containing information and guidance on how to administer the PKI Security Service.

2.8 **End User Certificates**:

2.8.1 BT will, on request by the Administrator, issue End User Certificates within the maximum number of Seats that BT has confirmed may be issued during the Minimum Period of Service or Renewal Period.

2.8.2 Within a Private Hierarchy:

(a) you will only use End User Certificates within your organisational intranet or extranet environment; and

(b) you may place some restrictions on and alter some elements of the content of End User Certificates via the Control Centre.

2.8.3 Within a Public Hierarchy:

(a) you may use an End User Certificate in a corporate or other organisational intranet or extranet environment or on the Internet; and

(b) you may place some restrictions on and alter some elements of the content of End User Certificates via the Control Centre; and

(c) any End User Certificate issued will contain your legal name, department or project name, the End User's name (or alias) and e-mail address and such other Customer Data as BT may determine. This combination of information uniquely identifies the End User Certificate.

3 Service Options

BT will provide you with any of the following options as set out in any applicable Order ("**Service Options**") and in accordance with the details as set out in that Order:

3.1 **Local Hosting**

3.1.1 BT will provide you with a service that allows you to:

(a) use your software with the PKI Security Service to design the visual appearance of End User Pages by including your text and branding images;

(b) host the End User Pages produced under this Paragraph 3.1 on a server that you select; and

(c) use the End User Pages produced under this Paragraph 3.1 in addition to the standard End User Pages provided and hosted by BT as part the PKI Security Service.

3.1.2 BT will give you a right to access and use the LH Software and to make copies of the LH Software for back-up purposes only.

3.2 **Automated Administration**

3.2.1 BT will provide you with Automated Administration that allows you to:

(a) automatically authenticate End User registrations directly against a single table database of Customer Data using matching rules as set out in this Schedule, within the parameters of the Automated Administration functionality;

(b) automatically request BT to issue 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 Paragraph 3.2.1(a).

3.2.2 BT will provide you with a right to access and use the AA Software and to make copies for back-up purposes only.

3.2.3 Automated Administration:

(a) will only be provided to you if you have Local Hosting service in place; and

(b) cannot be used with Passcode Authentication on a single CA at the same time.

3.2.4 You may, at an additional Charge, migrate any CA from Passcode Authentication to Automated Administration.

3.3 **Premium Revocation**

BT will:

3.3.1 provide you with an updated CRL every hour, which you will be able to download from the Repository and use for the purposes of validating the status of Certificates issued to you and your End Users; and

3.3.2 use reasonable endeavours to ensure the accuracy of the information on the CRL.

3.4 **Online Certificate Status Protocol Service (OCSP)**: BT will provide you with access to an OCSP responder via the Internet to validate the status of Certificates issued to you or your End Users against the CRL in Real Time.

3.5 **Passcode Authentication**

3.5.1 BT will provide you with Passcode Authentication that allows you to:

(a) automatically check and approve End User enrolments against your data in the CSV file based upon matching rules defined by you, within the parameters of the Passcode Authentication functionality;

(b) automatically request BT to issue 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 Paragraph 3.5.1(a).

3.6 **Key Manager**: BT will provide you with a key manager that allows for the centralised generation, distribution and back-up of the private keys associated with encryption certificates enabling you to recover encrypted data where the original key is lost or corrupted.

3.7 Service Options may not be available in all countries.

3.8 You will only use Service Options for the number of CAs purchased as part of the PKI Security Service.

4 Service Management Boundary

4.1 BT will provide and manage the PKI Security Service in accordance with Parts B and C of this Schedule and as set out in any applicable Order up to the front-end firewall on the PKI Security Service platform ("**Service Management Boundary**").

4.2 BT will have no responsibility for the PKI Security Service outside the Service Management Boundary.

4.3 BT does not make any representations, whether express or implied, about whether the PKI Security Service will operate in combination with any Customer Equipment or other equipment and software.

5 Associated Services

5.1 You will have the following services in place that will connect to the PKI Security Service and are necessary for the PKI Security Service to function and will ensure that these services meet the minimum technical requirements that BT specifies;

5.1.1 Internet connectivity

(an "**Enabling Service**").

5.2 If BT provides you with any services other than the PKI Security Service (including, but not limited to any Enabling Service) this Schedule will not apply to those services and those services will be governed by their separate terms.

6 Equipment

6.1 **Purchased Equipment**

6.1.1 **Consumer Regulations**

Where you place an Order acting for purposes that are related to your trade, business or profession, this is a business to business transaction to which the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013 do not apply.

6.1.2 **Sale of Goods**

The UN Convention on Contracts for the International Sale of Goods will not apply to the Contract.

6.1.3 **Delivery and Installation of Purchased Equipment**

(a) You will provide BT with the name and contact details of at least one individual who is responsible for receiving the Purchased Equipment at the Site(s).

(b) Where a Site is located within the EU, BT will dispatch any Purchased Equipment for delivery to the applicable Site as set out in any applicable Order.

(c) Where a Site is located outside the EU:

(i) you will act as the importer of record, clear the Purchased Equipment through the applicable customs authority in the destination country and be liable for any import tax, duty or excise duty incurred, and, if requested by BT, provide authorisation as soon as practicable, authorising BT or BT's agent to carry out BT's obligations as shipping agent. If you cannot give BT such authorisation, you are responsible for fulfilling the shipping agent obligations on BT's behalf at your own cost; and

(ii) subject to your compliance with Paragraph 6.1.3(c)(i):

i. BT will deliver any Purchased Equipment to the applicable port of entry in the destination country in accordance with Paragraph 6.1.4(b); or

ii. if agreed between both of us in any applicable Order, BT will arrange shipping services to deliver the Purchased Equipment to the final destination address(es) as set out in any applicable Order.

(d) Where a Site is located within the EU, if agreed between both of us in any applicable Order, BT will, subject to Paragraph 6.1.3(e), install any Purchased Equipment at the applicable Site(s), and:

(i) test Purchased Equipment to ensure that it is ready for use; and

(ii) on the date that BT has completed those tests, confirm to you that the Purchased Equipment is available for you to carry out any Acceptance Tests.

(e) Where a Site is located within a country in the EU other than the Territory, BT will not:

(i) sell you the Purchased Equipment if you are not VAT-registered in the delivery country; and

(ii) install the Purchased Equipment unless the Reverse Charge Mechanism applies to such services in that country.

(f) Where a Site is located outside the EU, BT will, subject to your compliance with Paragraph 6.1.3(c)(i), only sell you Purchased Equipment and not any associated installation.

(g) In order to provide you with the Purchased Equipment and any installation services as set out in the Order, BT may transfer the provision and installation of Purchased Equipment outside the Territory to a BT Affiliate or a third party in accordance with Clause 26 of the General Terms.

6.1.4 **Transfer of Title and Risk**

(a) Where the Purchased Equipment is delivered to a Site that is located within the Territory:

(i) title in the Purchased Equipment (except for the Intellectual Property Rights) will pass to you when you have paid for the Purchased Equipment in full;

(ii) where BT delivers or installs the Purchased Equipment, risk will pass to you on delivery of the Purchased Equipment, but you will not be liable for any loss or damage that is caused by BT's negligence; and

(iii) where BT does not deliver or install the Purchased Equipment, risk will pass to you when you take possession of the Purchased Equipment.

(b) Where the Purchased Equipment is delivered to a Site that is not located within the Territory:

(i) title in the Purchased Equipment (except for the Intellectual Property Rights) will pass to you upon dispatch from the final shipping point in the Territory (or in transit where shipped from outside the Territory); and

(ii) risk in the Purchased Equipment will pass to you in accordance with Incoterms® 2010 DAP, but you will not be liable for any loss or damage that is caused by BT's negligence.

6.1.5 **Acceptance of Purchased Equipment**

(a) Where a Site is located within the Territory, we will treat the Purchased Equipment as accepted:

(i) where BT does not install the Purchased Equipment, when you take delivery or possession of the Purchased Equipment; and

(ii) where BT installs the Purchased Equipment, the earlier of:

i. the Service Start Date; and

ii. where you notify BT in writing that the Purchased Equipment has not passed the Acceptance Tests but that is due to minor Incidents that do not affect the Purchased Equipment's performance, the date of that Notice.

(b) Where a Site is not located within the Territory, we will treat the Purchased Equipment as accepted on signature for the delivery at the port of entry, or at the final delivery address(es) that BT has agreed with you where BT are shipping the Purchased Equipment.

6.1.6 **Warranty**

(a) During the period of three consecutive months following the Service Start Date (or any other period that BT advises you in a Notice), if you report to BT in accordance with Paragraph 10 that there is an Incident in the Purchased Equipment due to faulty design, manufacture or materials, or BT's negligence, BT will, or will arrange for the manufacturer or other third party to, replace or (at BT's option) repair the part affected by, or causing, the Incident free of charge, unless:

(i) the Purchased Equipment has not been properly kept, used or maintained in accordance with the manufacturer's or BT's instructions, if any;

(ii) the Purchased Equipment has been modified without BT's written consent;

(iii) the Incident is due to damage, interference with or maintenance of Purchased Equipment by persons other than BT or a third party authorised by BT;

(iv) the Incident is due to faulty design by you where the Purchased Equipment has been customised or integrated into your systems to your design; or

(v) the Incident is due to fair wear and tear.

(b) If requested by BT, you will return the Purchased Equipment affected by an Incident to BT or to the manufacturer or other third party, in accordance with BT's instructions, for repair or replacement in accordance with Paragraph 6.1.6(a).

(c) BT does not warrant that the Software supplied in accordance with the Contract is free from Incidents, but BT will remedy any defects that materially impair performance (where necessary, by arrangement between both of us) within a reasonable time.

6.1.7 **Security**

(a) You are responsible for the proper use of any user names, personal identification numbers and passwords used with the Purchased Equipment, and you will take all necessary steps to ensure that they are kept confidential, secure and not made available to unauthorised persons.

(b) BT does not guarantee the security of the Purchased Equipment against unauthorised or unlawful access or use.

6.1.8 **Software Licence**

On and from the Service Start Date, or, where BT installs any Purchased Equipment, from the date of installation, you will comply with the provisions of any Software licences provided with or as part of any Purchased Equipment.

6.2 **WEEE Directive**

6.2.1 You are responsible under Article 13 of the Waste Electrical and Electronic Equipment Directive 2012 ("**WEEE Directive**") for the costs of collection, treatment, recovery, recycling and environmentally sound disposal of any equipment supplied under the Contract that has become waste electrical and electronic equipment ("**WEEE**").

6.2.2 For the purposes of Article 13 of the WEEE Directive this Paragraph 6.2 is an alternative arrangement to finance the collection, treatment, recovery, recycling and environmentally sound disposal of WEEE.

6.2.3 You will comply with any information recording or reporting obligations imposed by the WEEE Directive.

7 Specific Terms

7.1 **Minimum Period of Service**

7.1.1 Unless one of us gives Notice to the other of an intention to terminate the PKI Security Service at least 90 days before the end of the Minimum Period of Service or a Renewal Period, at the end of the Minimum Period of Service or Renewal Period the PKI Security Service will automatically extend for a Renewal Period and both of us will continue to perform each of our obligations in accordance with the Contract.

7.1.2 In either of us gives Notice of an intention to terminate the PKI Security Service, BT will cease delivering the PKI Security Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period.

7.1.3 BT may propose changes to this Schedule or the Charges (or both) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

7.1.4 Within 21 days of any Notice to Amend, you will provide BT Notice:

(a) agreeing to the changes BT proposed, in which case those changes will apply from the beginning of the following Renewal Period;

(b) requesting revisions to the changes BT proposed, in which case both of us will enter into good faith negotiations for the remainder of that Minimum Period of Service or Renewal Period, as applicable, and, if agreement is reached, the agreed changes will apply from the beginning of the following Renewal Period; or

(c) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

7.1.5 If we have not reached agreement in accordance with Paragraph 7.1.4(b) by the end of the Minimum Period of Service or the Renewal Period, the terms of this Schedule will continue to apply from the beginning of the following Renewal Period unless you give Notice in accordance with Paragraph 7.1.4(c) or BT may give Notice of termination, in which case BT will cease delivering the PKI Security Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

7.2 **Customer Committed Date**

7.2.1 If you request a change to the PKI Security Service or any part of the PKI Security Service, including any IP Address location, then BT may revise the Customer Committed Date to accommodate that change.

7.2.2 BT may expedite delivery of the PKI Security Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

7.3 **Invoicing**

7.3.1 Unless set out otherwise in any applicable Order, BT will invoice you for the following Charges in the amounts set out in any applicable Order:

(a) Installation Charges, on the Service Start Date, or where the installation period is estimated to be longer than one month, monthly in arrears starting from when you place an Order until the Service Start Date;

(b) Recurring Charges, annually in advance on the first day of the relevant year and for any period where the PKI Security Service is provided for less than one month, the Recurring Charges will be calculated on a daily basis. Recurring Charges will be charged from the Service Start Date;

(c) any Charges for any Purchased Equipment from the Service Start Date, and those Charges that will apply from the date you take delivery or possession of that Purchased Equipment; and

(d) any Termination Charges incurred in accordance with Paragraph 7.4 upon termination of the relevant Service.

7.3.2 BT may invoice you for any of the following Charges in addition to those set out in any applicable Order:

(a) Charges for investigating Incidents that you report to BT where BT finds no Incident or that the Incident is caused by something for which BT is not responsible under the Contract;
(b) Charges for commissioning the PKI Security Service in accordance with Paragraph 8.2 outside of Business Hours;
(c) Charges for expediting provision of the PKI Security Service at your request after BT has informed you of the Customer Committed Date; and
(d) late payment Charges set out in the BT Price List or notified to you by BT; and
(e) any other Charges as set out in any applicable Order or the BT Price List or as otherwise agreed between both of us.

7.4 **Termination Charges**

7.4.1 If you terminate the Contract, the PKI Security Service or any applicable Order for convenience in accordance with Clause 17 of the General Terms you will pay BT:

(a) all outstanding Charges for service rendered;
(b) any remaining Charges outstanding with regard to Purchased Equipment;
(c) any additional amounts due under the Contract;
(d) any other Charges as set out in any applicable Order; and
(e) any charges reasonably incurred by BT from a supplier as a result of the early termination.

7.4.2 In addition to the Charges set out at Paragraph 7.4.1 above, if you terminate during the Minimum Period of Service or any Renewal Period, you will pay BT:

(a) for any parts of the PKI Security Service that were terminated during the first 12 months of the Minimum Period of Service, Termination Charges, as compensation, equal to:

(i) 100 per cent of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service;
(ii) 20 per cent of the Recurring Charges for the remaining months, other than the first 12 months of the Minimum Period of Service; and
(iii) any waived Installation Charges; and

7.4.3 for any parts of the PKI Security Service that were terminated after the first 12 months of the Minimum Period of Service or during a Renewal Period, Termination Charges, as compensation, equal to 20 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service or Renewal Period; and

7.4.4 BT will refund to you any money you have paid in advance after deducting any Charges or other payments due to BT under the Contract.

7.5 **Service Amendment**

7.5.1 You may request, by giving BT Notice, a change to:

(a) an Order for the PKI Security Service (or part of an Order) at any time before the applicable Service Start Date; or
(b) the PKI Security Service at any time after the Service Start Date.

7.5.2 If you request a change in accordance with Paragraph 7.5.1, except where a change results from BT's failure to comply with BT's obligations under the Contract, BT will, within a reasonable time, provide you with a written estimate, including:

(a) the likely time required to deliver the changed PKI Security Service; and
(b) any changes to the Charges due to the changed PKI Security Service.

7.5.3 BT has no obligation to proceed with any change that you request in accordance with Paragraph 7.5.1, unless and until the necessary changes to the Charges, implementation timetable and any other relevant terms of the Contract to take account of the change are agreed between both of us in writing.

7.5.4 If BT changes a PKI Security Service prior to the Service Start Date because you have given BT incomplete or inaccurate information, BT may, acting reasonably, apply additional Charges.

7.6 **Expiry and Revocation of Certificates**

7.6.1 **Administrator Certificates:**

(a) All Administrator Certificates for each CA will expire at the end of the Minimum Period of Service.
(b) You may make a request to BT to renew an Administrator Certificate on or before the expiry of the Administrator Certificate.
(c) Any Administrator Certificate that you renew will expire at the end of the Renewal Period.
(d) BT may revoke Administrator Certificates from you upon receipt of a request from you and in accordance with the Contract.

7.6.2 **End User Certificates:**

(a) End User Certificates will expire at the end of the 365 days from the date that BT receives a request from the Administrator to issue the End User Certificate:

(b) BT may revoke an End User Certificate upon receipt of reasonable request from the End User or from you acting on behalf of the End User to revoke the End User Certificate.

7.6.3 **AA Certificates:**

(a) BT may revoke an AA Certificate upon receipt of a request from you to revoke the AA Certificate or where BT reasonably believes that there may be a Compromise of the integrity of the Private Keys held on the hardware security module (HSM).

(b) You will inform BT to revoke an AA Certificate within four hours from the time you become aware of or reasonably believe that there has been a Compromise of an AA Certificate Private Key.

7.7 **Third Party Confirmation of Your Information**

7.7.1 BT will:

(a) verify information that you provide with your Order with information held in third-party databases;

(b) will use a telephone number listed with a third-party database to confirm certain information with you; and

(c) require you to provide additional information and proof where the databases and other resources available to BT do not contain all the information that BT requires.

7.7.2 BT will not provide the PKI Security Service to you if:

(a) you fail to provide any information or additional information that BT request;

(b) BT cannot verify any information that you provide to BT's complete satisfaction; or

(c) you do not cooperate with BT to verify the information.

Part B – Service Delivery and Management

8 BT's Obligations

8.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the PKI Security Service, BT:

8.1.1 will provide you with contact details for the Service Desk;

8.1.2 will comply with all reasonable health and safety rules and regulations and reasonable security requirements that apply at the Site(s) and that you have notified to BT in writing, but BT will not be liable if, as a result of any such compliance, BT is in breach of any of obligations under this Contract; and

8.1.3 will provide you with a Customer Committed Date and will use reasonable endeavours to meet any Customer Committed Date;

8.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

8.2.1 configure the PKI Security Service;

8.2.2 conduct a series of standard tests on the PKI Security Service to ensure that it is configured correctly;

8.2.3 connect the PKI Security Service to the Enabling Service;

8.2.4 Set Up the PKI Security Service; and

8.2.5 on the date that BT has completed the activities in this Paragraph 9.2, confirm to you that the PKI Security Service is available for performance of any Acceptance Tests in accordance with Paragraph 9.2.

8.3 **During Operation**

On and from the Service Start Date, BT:

8.3.1 will respond and use reasonable endeavours to remedy an Incident without undue delay and in accordance with the Service Care Levels in Part C of the Contract;

8.3.2 will maintain a web portal and server to provide you with online access to performance reports; and

8.3.3 may carry out Maintenance from time to time and will use reasonable endeavours to inform you at least five Business Days before any Planned Maintenance on the PKI Security Service, however, BT may inform you with less notice than normal where Maintenance is required in an emergency.

8.4 **The End of the Service**

On termination of the PKI Security Service by either one of us, BT will revoke all Certificates.

9 Your Obligations

9.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the PKI Security Service, you will:

9.1.1 provide BT with the names and contact details of Customer Contact, but BT may also accept instructions from a person who BT reasonably believes is acting with your authority;

9.1.2 provide BT with any information reasonably required without undue delay;

9.1.3 provide BT with access to any Site(s) during Business Hours, or as otherwise agreed, to enable BT to Set Up, deliver and manage the PKI Security Service;

9.1.4 complete any preparation activities that BT may request to enable you to receive the PKI Security Services promptly and in accordance with any reasonable timescales;

9.1.5 provide BT with Notice of any health and safety rules and regulations and security requirements that apply at the Site(s); and

9.1.6 complete enrolment forms for each CA and for the superior IA and provide these when you place an Order.

9.2 **Acceptance Tests**

9.2.1 You will carry out the Acceptance Tests for the PKI Security Service within five Business Days after receiving Notice from BT in accordance with Paragraph 8.2.5 ("**Acceptance Test Period**").

9.2.2 The PKI Security Service is accepted by you if you confirm acceptance in writing during the Acceptance Test Period or is treated as being accepted by you if you do not provide BT with Notice to the contrary by the end of the Acceptance Test Period.

9.2.3 Subject to Paragraph 9.2.4, the Service Start Date will be the earlier of the following:

(a) the date that you confirm acceptance of the PKI Security Service in writing in accordance with Paragraph 9.2.2; or
(b) the date of the first day following the Acceptance Test Period.

9.2.4 if, during the Acceptance Test Period, you provide BT Notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide you Notice that BT has remedied the non-conformance and inform you of the Service Start Date.

9.3 **During Operation**

On and from the Service Start Date, you will:

9.3.1 ensure that End Users report Incidents to the Customer Contact and not to the Service Desk;

9.3.2 ensure that the Customer Contact will take Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between both of us, and will be available for all subsequent Incident management communications;

9.3.3 monitor and maintain any Customer Equipment connected to the PKI Security Service or used in connection with a PKI Security Service;

9.3.4 ensure that any Customer Equipment that is connected to the PKI Security Service or that you use, directly or indirectly, in relation to the PKI Security Service is:

(a) connected using the applicable BT Network termination point, unless you have BT's permission to connect by another means;
(b) adequately protected against viruses and other breaches of security;
(c) technically compatible with the PKI Security Service and will not harm or damage BT Equipment, the BT Network, or any of BT's suppliers' or subcontractors' network or equipment; and
(d) approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment;

9.3.5 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment does not meet any relevant instructions, standards or Applicable Law;

9.3.6 ensure that the copyright notices that appear on the original program and media on which the LH Software or AA Software is delivered to you is reproduced on any back-up copies that you produce;

9.3.7 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.

9.3.8 for each CA:

(a) appoint Administrator(s) that are competent to perform End User Certificate duties to operate the LRA on your behalf;
(b) immediately inform BT of any changes to the name and contact details of the Administrator(s);
(c) ensure that the Administrator has adequate training in all relevant areas as set out in Administrator Handbook;
(d) ensure that the Administrator will follow guidance on the detailed LRA procedures as set out in the Administrator handbook, and for PCS Customers, the BT CPS;
(e) appoint a new Administrator and request BT to revoke the original Administrator's Certificate within four hours from the time you become aware or reasonably believe that:

(i) there has been a Compromise of an Administrator's Private Key; or
(ii) an Administrator is no longer entitled to act as an Administrator.

(f) where applicable, ensure that an Administrator Certificate and corresponding key pair is promptly erased from the Purchased Equipment within 4 hours of the revocation of that Administrator Certificate;
(g) provide helpdesk support to End Users who have applied for Certificates through you; and
(h) notify End Users of revocation of their End User Certificates.
(i) ensure and be able to demonstrate that End Users are your officers, directors, employees, partners(in the case of unincorporated partnership) or persons maintaining a prior legal or contractual relationship with you which does not solely relate to the provision of End User Certificates;

9.3.9 for PCS:

(a) enter into an agreement with End Users that will ensure that they comply with this Schedule;
(b) ensure that End Users:

(i) submit accurate and complete enrolment information;
(ii) take all reasonable steps to prevent unauthorised disclosure of the Private Key; and
(iii) immediately inform you where:

i. the Private Key is lost, stolen or compromised;

ii. control over the Private Key is lost due to a compromise of activation data; or
iii. they are informed of any inaccuracy or change to the certificate content.

(c) for the purpose of validation of End User registrations: confirm that:

(i) the End User requesting an End User Certificate is the person identified on the application;
(ii) the End User rightfully holds the Private Key corresponding to the Public Key to be listed in the End User Certificate;
(iii) the information provided is accurate; and
(iv) the End User is suitable to receive an End User Certificate in accordance with your criteria and any BT's criteria.

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

(i) within eight hours after the Administrator becomes aware or reasonably believes that there has been Compromise of the End User's Private Key; or
(ii) where the End User is no longer entitled to have the End User Certificate.

9.3.10 agree that End User Certificate(s) and Administrator Certificate(s) are issued by BT on your instructions and that the contractual relationship with respect to End User Certificates is between you and the End User.

9.3.11 agree that the information on the Repository will be made publicly available via the Repository or otherwise.

9.3.12 where applicable, ensure that:

(a) you download the CRLs that BT makes available to you to your server;
(b) the OCSP Service remains online in order for the CRL information produced by OCSP to be made available for use in Real Time; and
(c) the information on the CRL is accurate and up to date.

9.3.13 If you select **Automated Administration**:

(a) ensure that you have Local Hosting in place;
(b) inform BT to revoke an AA Certificate, within four hours from the time you become aware of or reasonably believe that there has been a Compromise of an AA Certificate Private Key;
(c) only use the AA Kit to for the purposes of providing secure key generation, storage and signing for the AA Certificate as part of the Automated Administration; and
(d) not use Automated Administration together with other software or hardware or service unless you have BT's permission to do so.

9.3.14 If you select for **Passcode Authentication**:

(a) ensure that the CSV file is produced to the specification described from time to time in the Administrator's Handbook;
(b) If you select for Passcode Authentication, use your software to design your own End User Pages and ensure the End User Pages are available at the time of installation of Local Hosting; and
(c) not use Passcode Authentication together with other software or hardware or service unless you have BT's permission to do so.

10 Notification of Incidents

Where you become aware of an Incident:

10.1 Your Customer Contact will report it to the Service Desk;

10.2 BT will give you a Ticket;

10.3 BT will inform you when it believes the Incident is cleared and will close the Ticket when:

10.3.1 you confirm that the Incident is cleared within 24 hours after having been informed; or

10.3.2 BT has attempted unsuccessfully to contact you, in the way agreed between both of us, in relation to the Incident and you have not responded within 24 hours following BT's attempt to contact you.

10.4 If you confirm that the Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and BT will continue to work to resolve the Incident; and

10.5 Where BT becomes aware of an Incident, Paragraphs 10.2, 10.3 and 10.4 will apply.

Part C – Service Levels

11 Service Availability

11.1 **Availability Service Level**

From the Service Start Date, BT will provide the PKI Security Service with a target availability of 99.5 per cent of the total hours during every month you use the PKI Security Service ("**Availability Service Level**").

Part D – Defined Terms

12 Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Schedule). BT has repeated some definitions in this Schedule that are already defined in the General Terms. This is to make it easier for you to find the definitions when reading this Schedule.

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

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

"**Acceptance Test Period**" has the meaning given in Paragraph 9.2.1.

"**Acceptance Tests**" means those objective tests conducted by you that when passed confirm that you accept the PKI Security Service and that the PKI Security Service is ready for use save for any minor non-conformities that will be resolved as an Incident in accordance with Paragraph 8.3.1.

"**Activation**" means the preparation of the Control Centre and associated PKI Security Service(s) for your Service Desk and the activation of the CA(s) as part of the PKI Security Service

"**Administrator**" means any of the Individuals authorised to act on your behalf for Service Management matters and who is responsible for the technical and system related matters relating to the PKI Security Service.

"**Automated Administration**" or "**AA**" means the service option that allows you to automatically authenticate End User registrations and to automatically request BT to issue End User Certificates to End Users.

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

"**Administrator Handbook**" has the meaning given to it in Paragraph 2.7

"**Availability**" means the period of time when the PKI Security Service is functioning.

"**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.

"**BT Price List**" means the document containing a list of BT's charges and terms that may be accessed at: www.bt.com/pricing (or any other online address that BT may advise you).

"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.

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

"**Certificate**" means electronic data which is used to prove procession of a Public Key and which;

(a) includes information on the owner of the Public Key;
(b) contains their Public Key;
(c) specifies the operational period and serial number of the Certificate; and
(d) identifies the issuer of the Certificate.

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

"**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.

"**Circuit**" means any line, conductor, or other conduit between two terminals by which information is transmitted, and that is provided as part of the PKI Security Service.

"**Compromise**" means a violation or suspected violation of BT's or your security policy designed to prevent unauthorised disclosure of, or loss of control over, sensitive information pertaining to Private Keys or Public Keys.

"**Content**" means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

"**Control Centre**" means a set of tools and facilities to manage or enhance the PKI Security Service, which is accessed via web pages, hosted by BT to enable your Administrator(s) to manage and monitor the PKI Security Service.

"**Core Network**" means BT's network infrastructure between and including the POP, but does not include the Access Line between your Site(s) and the POP.

"**COS**" means class of service, which is a categorisation of traffic based on a process for managing a network by giving certain types of traffic priority over others.

"**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 Committed Date**" means the date provided by BT on which delivery of the PKI Security Service (or each part of the PKI Security Service, including to each Site) is due to start.

"**Customer Contact**" means any the Administrator(s) individuals authorised to act on your behalf for PKI Security Service management matters, including the Administrator(s) and System Administrator.

"**Customer Data**" means information about you, the Administrator, or End User, which may include personal data subject to laws or regulations that you provide on the Order Form or enrolment form.
"**Customer Equipment**" means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with a PKI Security Service.
"**CVM**" means Certificate Validation Module which is a Software patch provided by BT to validate Certificates.
"**DAP**" means Delivered at Place as defined in Incoterms® 2010.
"**Device**" means any mobile handset, laptop, tablet or other item of handheld equipment, including all peripherals, excluding SIM Cards and applications, which are in scope of the PKI Security Service, as set out in the Order
"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.
"**Enabling Service**" has the meaning given in Paragraph 5.1.
"**End User Certificate**" means the Certificate provided by BT to End User(s).
"**End User Page**" means an HTML coded page(s) for use by you and your End Users.
"**End User**" means you, or a person who applies through for an End User Certificate(s).
"**EU**" means European Union.
"**General Terms**" means the general terms that this Schedule is attached to, or where not attached to this Schedule, can be found at www.bt.com/terms, and form part of the Contract.
"**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). BT is the IA responsible for issuing End User Certificate(s) in accordance your instructions.
"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the PKI Security Service or particular element of the PKI Security Service.
"**Incoterms® 2010**" means the International Commercial Terms, which are a series of pre-defined commercial terms published by the International Chamber of Commerce and are a trademark of the International Chamber of Commerce.
"**Installation Charges**" means those Charges set out in any applicable Order in relation to installation of the PKI Security Service or any Purchased Equipment, Customer Equipment or BT Equipment as applicable.
"**Internet Protocol**" or "**IP**" means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.
"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.
"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.
"**LDAP**" means Lightweight Directory Access Protocol, a directory architecture protocol which operates over TCP/IP.
"**Local Hosting**" or "**LH**" means the service option where BT that allows you to use your software with the PKI Security Service to design the visual appearance of End User Pages and to host the End User Pages on a server.
"**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 PKI Security Service.
"**LRA**" or "**Local Registration Authority**" means the function that approves Certificate requests from End Users. The LRA manages registrations, approves registrations as enrolments, performs authentication and gives BT instructions to issue End User Certificates to End Users on your behalf.
"**Minimum Period of Service**" means a period of 12 consecutive months beginning on the Service Start Date, unless set out otherwise in any applicable Order.
"**ODBC**" means Open Database Connectivity, which is a standard or open application programming interface for accessing a database.
"**Online Certificate Status Protocol Service**" or "**OCSP**" means the online access service that enables you to validate the status of Certificates issued to you or your End Users in Real Time.
"**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 you and End Users in accordance with the BT CPS.
"**PIN**" means an alphanumeric pass code.
"**PKI**" means Public Key Infrastructure.
"**PKI Security Service**" has the meaning given in Paragraph 1.
"**Planned Maintenance**" means any Maintenance BT has planned to do in advance.
"**POP**" means a point of presence, which is the point where the Access Line terminates and is the demarcation point between the Access Line and BT's Core Network.
"**Pre-Production Service**" means the service provided by BT on which BT will perform Set Up of the PKI Security Service, enabling you to integrate and test the PKI Security Service.

"**Private Hierarchy**" means a single CA or hierarchy of CAs chained up to a common Root Key which belongs to you and is not generally available in the public domain.
"**Private Key**" means a mathematical key (kept secret by you, 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.
"**RA**" or "**Registration Authority**" means a person or a function empowered in accordance with the Service Schedule(s) to carry out the verification of End User enrolments.
"**RA Kit**" means 'the Purchased Equipment, comprising a cryptographic USB token to store the Administrator Certificate and the Administrator Certificate.
"**Real Time**" means the level of computer responsiveness that an End User senses as immediate.
"**Recurring Charges**" means the Charges for the PKI Security Service or applicable part of the PKI Security Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Repository**" means a database, accessible on-line, containing Certificates, Public Keys, Customer Data and other information relating to the PKI Security Service.
"**Renewal Period**" means for each PKI Security Service, the initial 12 month period following the Minimum Period of Service, and each subsequent 12 month period.
"**Reverse Charge Mechanism**" means the method by which Customers within the European Union may self-assess for domestic VAT on cross-border purchases in accordance with Articles 194 – 199 of Council Directive 2006/112/EC.
"**Root Key**" means the Public Key of the CA at the top of your 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.
"**Service Desk**" means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the PKI Security Service.
"**Service Level**" means the Availability Service Level.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Options**" has the meaning given in Paragraph 3.
"**Set Up**" means the installation and Set Up PKI Security Service listed on the BT Price List including:

(a) Activation of the PKI Security Service;
(b) Set Up of the PKI Security Service;
(c) where applicable, use of the Pre-Production Service

"**Site**" means a location at which the PKI Security Service is provided.
"**Standard Service Components**" has the meaning given in Paragraph 2.
"**Territory**" means the country in which BT is registered as resident for corporate income tax purposes.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".
"**Validity Period**" means a period of 365 days or other period specified by you.
"**WEEE**" has the meaning given in Paragraph 6.2.1.
"**WEEE Directive**" has the meaning given in Paragraph 6.2.1.