BT

Certification Practice Statement

Version: 5.4a

Effective Date: 12 December 2020

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the BT Certification Practices Statement (CPS) that outlines the principles and practices related to BT's certification services. This CPS applies to all entities participating in or using BT's certificate services, excluding participants in BT's Private PKI services, which are not cross-certified or publicly trusted. This CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

Name of Policy/Guideline/Requirement Standard	**Location of Source Document/Language**
DigiCert Certificate Policy	https://www.digicert.com/legal-repository/
The Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")	https://cabforum.org/baseline-requirements-documents/
Microsoft Trusted Root Store (Program Requirements)	https://docs.microsoft.com/en-us/security/trustedroot/program-requirements
Mozilla Root Store Policy	https://www.mozilla.org/en-US/about/governance/policies/securitygroup/certs/policy/
Mozilla CA/Forbidden or Problematic Practices	https://wiki.mozilla.org/CA/Forbidden_or_Problematic_Practices
Apple Root Store Program	https://www.apple.com/certificateauthority/ca_prog ram.html
Chromium Project Root Store Certificate Policy	https://www.chromium.org/Home/chromiumsecurity/root-ca-policy

If any inconsistency exists between this CPS and the normative provisions of the foregoing policies, guidelines, and requirements ("Applicable Requirements"), then the Applicable Requirements take precedence over this CPS.

This CPS is only one of several documents that control BT's certification services. Other important documents include both private and public documents, such as the DigiCert CP, BT's agreements with its customers, Relying Party agreements, and BT's privacy policy. BT may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CPS is divided into nine parts that cover the security controls and practices and procedures for certificate services within the BT PKI. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation."

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the BT Certification Practices Statement and is based on the DigiCert Certification Practices Statement (version 5.1). BT has not assigned this CPS an object identifier value.

Date	Changes	Version
12-December-2020	Various amendments relating to points raised during previous audits	5.4a
14-October-2020	Various changes following review of DigiCert CPS	5.4
20-April-2020	Various changes following review by DigiCert compliance team	5.1
31-March-2020	Initial Acceptance – versioning aligning with DigiCert reference	5.0
16-January-2020	Amended 4.9.5 to specify "within 12 hours"	3.13a
06-September-2019	Amended to maintain link with new DigiCert CPS	3.13
25-February-2019	Version in line with DigiCert CPS and will be maintained as such	3.8.11
11-October-2018	Various changes to align with latest STN CP	3.8.9

The OID for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412). The OID-arc for this version 4 of the CPS is 2.16.840.1.114412.0.2.4. Subsequent revisions to this CPS might have new OID assignments. The following OID arcs are also included in this CPS, but are considered deprecated: 2.16.840.1.113733.1.7, 2.23.140.1.1,1.3.6.1.4.1.14370, 1.3.6.1.4.1.14370.1, and 2.16.840.1.113733.1.7.48.

OIDs found in Certificates reliant upon CAB Forum requirements and guidelines include the designated reserved policy identifiers in the Certificate Policy extension as of September 30, 2020.

BT issues Certificates containing the following OIDs / OID arcs:

Digitally Signed Object	Object Identifier (OID)
Level 1 Certificates - Enterprise	2.16.840.1.114412.4.1.2 or 2.16.840.1.114412.5.2 (maps to 2.16.840.1.113733.1.7.23.2)

All OIDs mentioned above belong to their respective owners. The specific OIDs used when objects are signed pursuant to this CPS are indicated in the object's respective Certificate Policies extension.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

DigiCert operates offline root and offline intermediate certification authorities (CAs) that issue subordinate CAs for BT and its customers. As the operator of several CAs, BT performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

BT and BT enterprise customers may operate their own CAs as subordinate CAs to a DigiCert PCA. Such a customer enters into a contractual relationship with BT to abide by all the requirements of the CP and the BT CPS. These subordinate CAs may however implement more restrictive practices based on their internal requirements.

1.3.2. Registration Authorities and Other Delegated Third Parties

A Registration Authority is an entity that performs identification and authentication of certificate Applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of an Issuer CA on identity management systems (IdMs). BT may act as an RA for certificates it issues.

BT and customers of BT who manage their own subordinate Issuer CAs may act as RAs for certificates they issue.
Validation of domains for S/MIME Certificates cannot be delegated to a third party and is only validated by the RA of the Issuer CA.

For subordinate CAs to be used to issue email certificates, in which BT is the named Organisation, verification of email domain ownership is carried out by DigiCert and the subordinate CA certificates are technically constrained by DigiCert using name constraint extensions. BT RAs are only permitted to issue certificates containing email addresses within the verified domain(s).

For subordinate CAs to be used to issue email certificates, in which a customer of BT is the named Organisation, verification of email domain ownership is carried out by DigiCert and the subordinate CA certificates are technically constrained by DigiCert using name constraint extensions. Customers' RAs are only permitted to issue certificates containing email addresses within the verified domain(s).

The only exception to this is where BT Customer Subordinate CAs are used without such name constraints. In this case the customer's RA performs the email validation and their RA operation is subject to its own separate ETSI audit.

1.3.3. Subscribers

Subscribers use BT's services and PKI to support transactions and communications. Subscribers under this CPS include all end users (including entities) of certificates issued by an Issuer CA. A Subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals or organisations. Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an organization's employees. The *Subject* of a Certificate is the party named in the Certificate. A *Subscriber*, as used herein, may refer to the Subject of the Certificate and the entity that contracted with BT for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

CAs are technically also subscribers of certificates within the DigiCert Public PKI, either as the primary Certificate Authority issuing a self- signed Certificate to itself, or as an Issuer CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CPS, however, apply only to end-user Subscribers.

In some cases, certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organisation may require certificates for its employees to allow them to represent the organisation in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CPS to distinguish between these two roles: "Subscriber", is the entity which contracts with BT for the issuance of credentials and; "Subject", is the person to whom the credential is bound.

The Subscriber bears ultimate responsibility for the use of the credential, but the Subject is the individual that is authenticated when the credential is presented.

When 'Subject' is used, it is to indicate a distinction from the Subscriber. When "Subscriber" is used it may mean just the Subscriber as a distinct entity but may also use the term to embrace the two. The context of its use in this CPS will invoke the correct understanding.

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by BT. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate. A Relying party may or may not also be a Subscriber of the Public PKI hierarchy.

1.3.5. Other Participants

None

1.4. CERTIFICATE USAGE

A digital Certificate (or Certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by this CPS, by any CPS under which the certificate has been issued and any agreements with Subscribers.

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS.

This CPS covers several different types of end entity Certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificate	Appropriate Use
Level 1 Client Certificates - Enterprise and Class 1 and 2 Certificates	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.

1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified in accordance with this CPS when the Certificate issued.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

BT periodically rekey Intermediate CAs. Third party applications or platforms that have an Intermediate CA embedded as a root certificate may not operate as designed after the Intermediate CA has been rekeyed. BT therefore does not warrant the use of Intermediate CAs as root certificates and recommends that Intermediate CAs not be embedded into applications and/or platforms as root certificates.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

British Telecommunications plc
81 Newgate Street
London
EC1A 7AJ

1.5.2. Contact Person

The Certificate Policy Manager
BT Trust Services
pp2 Ty Cynnal
Watkiss Way
Cardiff
CF11 0SW

cps.mpki@bt.com

1.5.2.1. Revocation Reporting Contact Person

The Certificate Policy Manager
BT Trust Services
pp2 Ty Cynnal
Watkiss Way
Cardiff
CF11 0SW

To request that a Certificate be revoked, please email support.mpki@bt.com.

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. BT or an RA will authenticate and log each revocation request according to Section 4.9 of the CP and this CPS. BT will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Organisation listed in the Certificate. If revocation is requested by someone other than an authorised representative of the Subscriber or Organisation, BT or an RA will investigate the alleged basis for the revocation request prior to taking action in accordance with Section 4.9.1 and 4.9.3.

1.5.3. Person Determining CPS Suitability for the Policy

The BT Policy Management Authority (BTPMA) is responsible for determining whether this CPS and other documents in the nature of certification practice statements that supplement or are subordinate to this CPS are suitable under the CP and this CPS.

1.5.4. CPS Approval Procedures

Approval of this CPS and subsequent amendments shall be made by the BT Policy Management Authority (BTPMA). Amendments shall either be in the form of a document containing an amended form of the CPS or an update notice. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. *See also* Section 9.10 and Section 9.12 below.

1.6. DEFINITIONS AND ACRONYMS

See Appendix A for a table of acronyms, definitions and references.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

BT is responsible for the repository functions for its own CAs and the CAs of its Enterprise Managed PKI Customers. BT publishes Certificates they issue in the repository in accordance with Section 2.2.

Upon revocation of an end-user Subscriber's Certificate, BT publishes notice of such revocation in the repository. BT issues CRLs for its own CAs and the CAs of Enterprise Customers within its Subdomain, pursuant to the provisions of this CPS. In addition, for Enterprise Customers who have contracted for Online Certificate Status Protocol (OCSP), BT provides OCSP service pursuant to the provisions of this CPS.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

BT maintains a web-based repository that permits Relying parties to make online enquires regarding the revocation and other Certificate Status Information. BT provides Relying parties with information on how to find the appropriate repository to check Certificate status and, if Online Certificate Status Protocol (OCSP) is available, how to find the right OCSP responder.

BT publishes the Certificates it issues on behalf of its own CAs within its Subdomain of the DigiCert PKI. Upon Revocation of an end-user Subscriber's Certificate, BT shall publish notice of such revocation in the repository. In addition, BT issues Certificate Revocation Lists (CRLs) and, if available, provides OCSP services for its own CAs within its Subdomain of the DigiCert PKI.

BT will at all times publish a current version of:

- The CP,
- This CPS,
- Its Subscriber Agreements,
- Its Relying Third Party Charters, and
- Publicly available copy of the auditor report that contains the necessary information as required in the CABF BR section 8.

BT is responsible for the repository function for BT's CAs, and Enterprise Customers' CAs, which issue Certificates within BT's Subdomain of the DigiCert PKI.

BT publishes the CP, this CPS, Subscriber Agreements, and the Relying Third Party Charters in the repository section of BT's web site at https://www.trustwise.com/legal-repository/

BT publishes Certificates in accordance with Table 2 below.

Certificate Type	***Publication Requirements***
BT Issuing CA Certificates	Available to Relying Parties as part of a Certificate Chain that can be obtained with the End User Certificate through the query functions described below.

Certificate of the BT CA supporting Client Managed PKI Lite Certificates and CA Certificates of Client Managed PKI Customers	Available to relying parties as part of a Certificate Chain that can be obtained with the End User Certificate through query functions in the BT repository at: https://www.trustwise.com/services/client/searchSubscriberBT.html
End User Certificates	Optionally published and available to relying parties through query functions in the BT repository at: https://www.trustwise.com/services/client/searchSubscriberBT.html
End User Certificates issued through Client Managed PKI Customers	Made available through the query functions listed above, although at the discretion of the Client Managed PKI Customer, the Certificate may be accessible only via a search using the Certificate's serial number.

Table 2 – Certificate Publication Requirements

2.3. TIME OR FREQUENCY OF PUBLICATION

CA Certificates are published in a repository as soon as possible after issuance. CRLs for end-user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least every 6 months, and also within 18 hours if a CA Certificate is revoked. Under special circumstances, BT may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

BT does not issue certificates that are subject to baseline requirements.

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards except that BT may issue a Level 1 Certificate with a null subject DN if it includes at least one alternative name form that is marked critical. When DNs are used, common names must respect namespace uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates, except where stated otherwise under Section 3.1.3.

3.1.2. Need for Names to be Meaningful

BT uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. BT only allows directory information trees that accurately reflect organization structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, BT does not issue anonymous or pseudonymous Certificates; however, for IDNs, BT may include the Punycode version of the IDN as a subject name. BT may also issue other pseudonymous end-entity Certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

The uniqueness of each subject name in a Certificate shall be enforced as follows:

Client Certificates – Requiring a unique email address or a unique organization name combined/associated with a unique serial number.

The names of Subscribers shall be unique within a subordinate Issuer CA's or Customer's Sub-domain for a specific type of Certificate. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6. Recognition, Authentication, and Role of Trademarks

Certificate Applicants are prohibited from using names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. BT, however, does not verify whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. BT is entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2. INITIAL IDENTITY VALIDATION

BT may use any legal means of communication or investigation to ascertain the identity of an organisational or individual Applicant. BT may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

The Certificate Applicant must demonstrate that it rightfully holds the private key corresponding to the public key listed in the certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another BT approved method. This requirement does not apply where a key pair is generated by a CA on behalf of an End User, for example where pre-generated keys are placed on smart cards.

3.2.2. Authentication of Organization and Domain/Email Control

Whenever a Certificate contains an Organisation name, the identity of the organisation and other enrolment information provided by Certificate Applicants (except for Non-Verified Subscriber Information) is confirmed in accordance with the procedures set forth in BT's documented Validation Procedures.

As a minimum BT shall:
Determine that the organisation exists by using at least one third party identity proofing service or database, or alternatively, organisational documentation issued or filed with the applicable government or competent authority that confirms the existence of the organisation; and,
Confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organisation, that the organisation has authorised the
Certificate Applicant, and that the person submitting the Certificate application on behalf of the Certificate Applicant is authorised to do so. When a Certificate includes the name of an individual as an authorised representative of an Organisation, the employment of that individual and, his/her authority to act on behalf of the Organisation shall also be confirmed.

Where BT and BT Customer subordinate CA's are to be used to issue email certificates, the normal practice is for DigiCert to verify the right of BT or its customer to use or control an email address to be contained in a Certificate by doing one of the following:
1. By verifying domain control over the email domain using one of their standard procedures for validation of DV SSL/TLS Server Certificates or
2. by sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response through use of the Random Value to indicate that the Applicant and/or Organization owns or controls that same email address.
The verified email domains are then included in the name constraints extension of the Subordinate CA. As well as this 'Technical Constraint', BT and BT Customer RAs are only permitted to issue email certificates containing email addresses within the verified domains.
The only exception to this is where customer RAs operate their own subordinate CAs without name constraints. In this case the customer's RA performs the email validation and their RA operation is subject to its own separate ETSI audit.

3.2.3. Authentication of Individual Identity

If a Certificate will contain the identity of an individual, then BT or an RA validates the identity of the individual using the following procedures:

Certificate	Validation
Level 1 Client Certificates – Enterprise	Authenticate identity by: • manual check performed by the enterprise administrator customer for each subscriber requesting a certificate, "in which the subscriber receives the certificate via an email sent to the address provided during enrolment"; • Passcode-based authentication where a randomly-generated passcode is delivered out of band by the enterprise administrator customer to the subscriber entitled to enrol for the certificate, and the subscriber provides this passcode at enrolment time; or • comparing information provided by the subscriber to information contained in business records or databases (customer directories such as Active Directory or LDAP).

Internal Admin Certificates	The authentication of Internal Administrator certificates is based on authentication of the organisation and a confirmation from the organisation of the employment and authorisation of the person to act as Administrator. BT may also have occasion to approve Certificate Applications for their own Administrators. Administrators are "Trusted Persons" within an organisation. In this case, authentication of their Certificate Applications shall be based on confirmation of their identity in connection with their employment or retention as an independent contractor and background checking procedures.

3.2.3.1. Authentication for Role-based Client Certificates

BT does not issue Role-based Certificates

3.2.3.2. Authentication of Devices with Human Sponsors

BT does not issue certificates to Devices with Human Sponsors

3.2.4. Non-verified Subscriber Information

Non-verified subscriber information includes:

- Organisational Unit,
- Any other information designated as non-verified in the certificate

3.2.5. Validation of Authority

Whenever an individual's name is associated with an Organisation name in a certificate in such a way to indicate the individual's affiliation or authorisation to act on behalf of the Organisation BT or the RA:

- Determines that the organisation exists by using at least one third party identity proofing service or database, or alternatively, organisational documentation issued or filed with the applicable government that confirms the existence of the organisation; and,

- Uses information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals or confirms by telephone, confirmatory postal mail, or comparable procedure to the organisation, the employment with the Organisation of the individual submitting the Certificate Application, and where appropriate, his/her authority to act on behalf of the Organisation.

3.2.6. Criteria for Interoperation

Interoperation with the BT Subdomain of the DigiCert PKI is permitted pursuant to the CP.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, BT creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, BT or an RA may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
Level 1 Client Certificates	Username and password or a challenge phrase	At least every nine years

BT does not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

BT does not re-key after revocation. The Subscriber must undergo initial validation as specified in section 3.2.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

BT or an RA authenticates all revocation requests. BT may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

Prior to the revocation of a Certificate, BT verifies that the revocation has been requested by the Certificate's Subscriber or the entity that approved the Certificate Application.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the End User submit the End User's Challenge Phrase (or equivalent thereof) and revoking the Certificate automatically if it matches the Challenge Phrase (or equivalent thereof) on record,
- Receiving a message purporting to be from the End User that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the End User providing reasonable assurances in light of the Class of Certificate that the person or organisation requesting revocation is, in fact the End User.
  Depending on the circumstances, such communication may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

BT Administrators are entitled to request the revocation of End User Certificates within BT's Subdomain. BT authenticates the identity of Administrators via access control using SSL and client authentication before permitting them to perform revocation functions.

RAs using an Automated Administration Software Module may submit bulk revocation requests to BT. Such requests are authenticated via a request digitally signed with the private key in the RA's Automated Administration hardware token.

The requests of Client Managed PKI Customers to revoke a CA Certificate are authenticated by BT to ensure that the revocation has in fact been requested by the CA.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Either the Applicant or an individual authorised to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to BT.

4.1.2. Enrolment Process and Responsibilities

In no particular order, the enrolment process includes:

1. Submitting a certificate application;
2. Generating a Key Pair;
3. Delivering the Public Key of the Key Pair to BT;
4. Agreeing to the applicable Subscriber Agreement

4.1.2.1. End-user Subscriber Certificates

All end-user Certificate Subscribers shall manifest assent to the relevant Subscriber Agreement that contains representations and warranties described in Section 9.6.3 and undergo an enrolment process consisting of:

- completing a Certificate Application and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to BT,
- demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to BT.

4.1.2.2. CA and RA Certificates

Subscribers of CA and RA Certificates enter into a contract with BT. CA and RA Applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process. During this contracting process or, at the latest, prior to the Key Generation Ceremony to create a CA or RA key pair, the applicant shall cooperate with BT to determine the appropriate distinguished name and the content of the Certificates to be issued by the applicant.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

After receiving a certificate application, BT or an RA verifies the application information and other information in accordance with Section 3.2.

4.2.2. Approval or Rejection of Certificate Applications

BT or an RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2, and
- Payment has been received.

BT or an RA will reject a certificate application if:

- Identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed,
- The Subscriber fails to furnish supporting documentation upon request,
- The Subscriber fails to respond to notices within a specified time,
- Payment has not been received, or
- The RA believes that issuing a certificate to the Subscriber may bring the DigiCert PKI into disrepute.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, BT will approve the certificate application and issue the Certificate. BT is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

BT begins processing certificate applications within five working days of receipt. Processing of an application will be completed within two weeks, subject to the provision by the customer of the necessary information, unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between DigiCert PKI participants. A certificate application remains active until rejected. BT will usually complete the validation process and issue or reject a certificate application within five working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of BT can delay the issuance process

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by BT or following receipt of an RA's request to issue the Certificate. BT creates and issues to a Certificate Applicant a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

BT shall, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available. Certificates shall be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2. Publication of the Certificate by the CA

BT publishes the Certificates it issues in a publicly accessible repository

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

RAs may receive notification of the issuance of certificates they approve.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate is only permitted once the Subscriber agrees to the Subscriber Agreement and accepted the certificate. The certificate shall be used lawfully in accordance with BT's Subscriber Agreement, the terms of this CPS and the relevant CP.

Certificate use must be consistent with the *KeyUsage* field extensions included in the certificate (e.g., if Digital Signature is not enabled then the certificate must not be used for signing).
Subscribers shall protect their private keys from unauthorised use and shall discontinue use of the private key following expiration or revocation of the certificate. Subscribers shall use Certificates in accordance with their intended purpose. Parties other than the Subscriber shall not archive the Subscriber Private Key except as set forth in section 4.12

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. BT does not warrant that any third-party software will support or enforce the controls and requirements found herein.
Relying parties shall assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by BT are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the BT repository.

A Relying Party should rely on a digital signature only if:

1. the digital signature was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked, and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

Before relying on a time-stamp token, a Relying Party must:

1. verify that the time-stamp token has been correctly signed and that the Private Key used to sign the time-stamp token has not been compromised prior to the time of the verification,
2. take into account any limitations on the usage of the time-stamp token indicated by the relevant time-stamp policy, and
3. take into account any other precautions prescribed in this CPS or elsewhere.

4.6. CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new certificate to the Subscriber without changing the public key or any other information in the certificate. Certificate Renewal is not supported by BT and any renew operations will use the Re-key process (see Section 4.7)

4.6.1. Circumstance for Certificate Renewal

Not Supported by BT

4.7. CERTIFICATE RE-KEY

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same.

4.7.1. Circumstance for Certificate Rekey

Prior to the expiration of an existing Subscriber's Certificate it is necessary for the Subscriber to re-key the certificate to maintain continuity of certificate usage. A certificate may also be re-keyed after expiration. Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

4.7.2. Who May Request Certification of a New Public Key

Only the Subscriber for an individual certificate may request certificate re-key.

4.7.3. Processing Certificate Rekey Requests

Agreed re-key procedures ensure that the person seeking to re-key an end-user Subscriber Certificate is in fact the Subscriber (or authorised by the Subscriber) of the Certificate.

One acceptable procedure is using a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrolment information a Challenge Phrase (or the equivalent thereof). Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrolment information, and the enrolment information has not changed, a renewal Certificate is automatically issued. Subject to the provisions of Section 3.3.1, after re-keying in this fashion, and on at least alternative instances of subsequent re-keying thereafter, BT or an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in this CPS for the authentication of an original Certificate Application.

Other than this procedure or another BT-approved procedure, the requirements for the authentication of an original Certificate Application shall be used for re-keying an end-user Subscriber Certificate.

4.7.4. Notification of Certificate Rekey to Subscriber

See section 4.3.2

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Conduct constituting Acceptance of a re-keyed certificate is in accordance with Section 4.4.1.
Issued Certificates are considered accepted 30 days after the Certificate is rekeyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.7.6. Publication of the Issued Certificate by the CA

See section 4.4.2.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstances for Certificate Modification

Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the Subscriber's private key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2. Who May Request Certificate Modification

See section 4.1.1

4.8.3. Processing Certificate Modification Requests

BT or an RA shall perform identification and authentication of all required Subscriber information in terms of Section 3.2.

4.8.4. Notification of Certificate Modification to Subscriber

See section 4.3.2.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6. Publication of the Modified Certificate by the CA

See section 4.4.2.

4.8.7. Notification of Certificate Modification by the CA to Other Entities

See section 4.4.3.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, BT and Subscribers verify that the revocation request was made by either the organization or individual that made the certificate application or by an entity with the legal jurisdiction and authority to request revocation. Subscribers are required to provide evidence of the revocation authorization to BT upon request.

4.9.1. Circumstances for Revocation

BT will revoke a Certificate within 24 hours after receipt and on confirming one or more of the following occurred:

1. The Subscriber requests in writing that BT revoke the Certificate;
2. The Subscriber notifies BT that the original Certificate request was not authorized and does not retroactively grant authorization;
3. BT obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. BT obtains evidence that the validation of domain authorization should not be relied upon.

BT may revoke a certificate within 24 hours and will revoke a Certificate within 5 days after receipt and on confirming that one or more of the following occurred:

1. The Certificate no longer complies with the requirements of any section of the Mozilla Root Store policy;
2. BT obtains evidence that the Certificate was misused and/or used outside the intended purpose as indicated by the relevant agreement;
3. The Subscriber breached a material obligation under the CP, this CPS, or the relevant agreement;
4. BT confirms any circumstance indicating that use of an email address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name registrant's right to use the

Domain Name, a relevant licensing or services agreement between the Domain Name registrant and the Applicant has terminated, or the Domain Name registrant has failed to renew the Domain Name);

5. BT confirms a material change in the information contained in the Certificate;
6. BT determines or confirms that any of the information appearing in the Certificate is inaccurate;
7. Revocation is required by the DigiCert CP and/or this CPS; or
8. BT confirms a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

BT may revoke any Certificate in its sole discretion, including if BT believes that:

1. Either the Subscriber's or BT's obligations under the CP or this CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
2. BT received a lawful and binding order from a government or regulatory body to revoke the Certificate;
3. BT ceased operations and did not arrange for another Certificate authority to provide revocation support for the Certificates;
4. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;

BT always revokes a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

4.9.2. Who Can Request Revocation

Individual Subscribers can request the revocation of their own individual Certificates through an authorised representative of BT or an RA. A duly authorised representative of BT or a RA shall be entitled to request the revocation of an RA Administrator's Certificate. The entity that approved a Subscriber's Certificate Application shall also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only BT is entitled to request or initiate the revocation of the Certificates issued to its own CAs. RAs are entitled, through their duly authorised representatives, to request the revocation of their own Certificates, and their Superior Entities shall be entitled to request or initiate the revocation of their Certificates.

4.9.3. Procedure for Revocation Request

BT processes a revocation request as follows:

1. BT logs the identity of entity making the request or problem report and the reason for requesting revocation based on the list in section 4.9.1. BT may also include its own reasons for revocation in the log.
2. BT may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, BT revokes the Certificate based on the timeframes listed in 4.9.1 as listed for the reason for revocation.
4. For requests from third parties, BT personnel begin investigating the request within 24 hours after receipt and within 7 days decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate,
    c. the identity of the complainants, and
    d. relevant legislation.

5. If BT determines that revocation is appropriate,
    a. In the case of an end-entity certificate, BT personnel revoke the Certificate and update the CRL. If BT deems appropriate, BT may forward the revocation reports to law enforcement.
    b. In the case of a Subordinate CA certificate, BT disables the CA, preventing any further certificate issuance, and contacts DigiCert to instigate revocation procedures which will include notifying Mozilla as appropriate.

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. DigiCert may grant and extend revocation grace periods on a case-by-case basis. DigiCert reports the suspected compromise of its CA Private Key and requests revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

4.9.5. Time within which CA Must Process the Revocation Request

BT takes commercially reasonable steps to process revocation requests without delay. BT will revoke a certificate within twelve hours of receiving clear instructions to do so.

4.9.6. Revocation Checking Requirement for Relying Parties

Relying Parties shall check the status of Certificates on which they wish to rely. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL published by the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable web-based repository, or OCSP responder (where available) to check revocation status. CAs shall provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

Due to the numerous and varying locations for CRL repositories, relying parties are advised to access CRLs using the URLs(s) embedded in the certificate CRL Distribution Points extension. The proper OCSP responder for a given certificate is placed in its Authority Information Access extension.

4.9.7. CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates shall be issued at least annually, but also whenever a CA is revoked.

If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

4.9.8. Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. In addition to publishing CRLs, BT provides Certificate status information through query functions in the BT repository.

Certificate status information is available through web-based query functions accessible through the BT Repository at: https://www.trustwise.com/services/client/searchSubscriberBT.html

BT also provides OCSP Certificate status information. Enterprise Customers who contract for OCSP services may check Certificate status through the use of OCSP. The URL for the relevant OCSP Responder is communicated to the Enterprise Customer.

Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time, usually within ten seconds. OCSP responses conform to RFC 5019 and/or RFC 6960. OCSP responses either:

1. Are signed by the CA that issued the Certificates whose revocation status is being checked, or

2. Are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960

4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.
If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party shall check Certificate status by consulting the applicable repository or requesting Certificate status using the applicable OCSP Responder (where OCSP services are available).

For Publicly Trusted Subscriber Certificates:
Prior to 2020-09-30:
BT update information was provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service have a maximum expiration time of ten days.

Effective 2020-09-30:
1. OCSP responses have a validity interval greater than or equal to eight hours;
2. OCSP responses have a validity interval less than or equal to ten days;
3. For OCSP responses with validity intervals less than sixteen hours, then BT updates the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then BT updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder should not respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with Section 7.1.5 of the Baseline Requirements, this CPS and the CP, the responder must not respond with a "good" status for such requests.

BT may monitor the OCSP responder for requests for “unused” serial numbers as part of its security response procedures.

The OCSP responder may provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC6962]. A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by (a) the Issuing CA; or (b) a Precertificate Signing Certificate [RFC6962] associated with the Issuing CA; or
3. "unused" if neither of the previous conditions are met.

4.9.11. Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12. Special Requirements Related to Key Compromise

BT uses commercially reasonable efforts to notify potential Relying Parties if it discovers, or has reason to believe, that there has been a Compromise of the private key of one its own CAs or one the CAs within its subdomain. The primary means for notifying replying parties is through revocation of the compromised CA and subsequent publication of the revocation details in the superior CA CRL.

BT will instruct DigiCert to carry out the revocation as a matter of urgency. Customer Administrators of the affected CA's will also be contacted by email

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder.

The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period. CRLs for end-entity certificates are updated at least every 24 hours and the value of the nextUpdate field is no greater than 7 days after the thisUpdate field.

OCSP information for subscriber Certificates is updated for every OCSP request. Cached responses are not used. OCSP responses include a defined value in the nextUpdate field which is no more than 24 hours after the thisUpdate field.

OCSP service is not available for status information of subordinate CA Certificates.

4.10.2. Service Availability

Certificate Status Services are available 24 x 7 with no scheduled interruption.

4.10.3. Optional Features

OCSP is an optional status service feature that needs to be specifically enabled.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

Except for enterprises deploying Managed PKI Key Management Services no BT subdomain of the DigiCert PKI participant may escrow CA, RA or end-user Subscriber private keys.

Enterprise customers using Managed PKI Key Management Service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. BT does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process.

4.12.1. Key Escrow and Recovery Policy Practices

BT never escrows CA Private Keys under this CPS.

Enterprise customers using the Managed PKI Key Management service (or an equivalent service approved by DigiCert) are permitted to escrow end-user Subscribers' private key. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for enterprise customers using the Managed PKI Key Manager Service (or an equivalent service approved by Symantec), the private keys of CAs or end-user Subscribers shall not be escrowed.

End-user Subscriber private keys shall only be recovered under the circumstances permitted within the Managed PKI Key Management Service Administrator's Guide, under which:

- Enterprise customers using Managed PKI Key Manager shall confirm the identity of any person purporting to be the Subscriber to ensure that a purported Subscriber request for the Subscriber's private key is, in fact, from the Subscriber and not an impostor,
- Enterprise customers shall recover a Subscriber's private key without the Subscriber's authority only for their legitimate and lawful purposes, such as to comply with judicial or administrative process or a search warrant, and not for any illegal, fraudulent, or other wrongful purpose, and
- Such Enterprise customers shall have personnel controls in place to prevent Key Management Service Administrators and other persons from obtaining unauthorised access to private keys.

It is recommended that Enterprise Customers using the Key Management Service:

- Notify the subscribers that their private keys are escrowed,
- Protect subscribers' escrowed keys from unauthorised disclosure,
- Protect all information, including the administrator's own key(s) that could be used to recover subscribers' escrowed keys,
- Release subscribers' escrowed keys only for properly authenticated and authorised requests for recovery,

- Revoke the Subscriber's Key pair prior to recovering the encryption key under certain circumstances such as to discontinue the use of a lost certificate,
- Not be required to communicate any information concerning a key recovery to the subscriber except when the subscriber him/herself has requested recovery,
- Not disclose or allow to be disclosed escrowed keys or escrowed key-related information to any third party unless required by the law, government rule, or regulation.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

BT has implemented the BT Security Policy, which supports the security requirements of this CPS. Compliance with these policies is included in BT's independent audit requirements described in Section 8. BT's Security Policy contains sensitive security information and is only available on agreement with BT. An overview of the requirements are described below.

5.1.1. Site Location and Construction

BT's CA and RA operations are conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of sensitive information and systems whether covert or overt. BT also maintains disaster recovery facilities for its CA operations. BT's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of BT's primary facility.

5.1.2. Physical Access

5.1.2.1. Data Centres

Systems providing online certificate issuance (e.g. Issuer CAs) are located in secure data centres. BT protects such online equipment (including certificate status servers and CMS equipment) from unauthorized access and implements physical controls to reduce the risk of equipment tampering. Access to the data centres housing the CA and TSA platforms requires two-factor authentication by BT staff in trusted roles to meet two-person physical access control. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer BT's Private Keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

BT's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

5.1.2.2. RA Operations Areas

BT's RA operations are protected against access from non-authorized individuals. BT securely stores all removable media and paper containing sensitive plain-text information related to its CA or RA operations in secure containers.

5.1.2.3. Offline CA Key Storage Rooms

BT securely stores the cryptomodules used to generate and store offline CA Private Keys. Access to the rooms used for key storage is controlled and logged. When not in use during a key ceremony, CA cryptomodules are

locked in a safe that provides two-person physical access control. Activation data is protected in accordance with section 6.4. Cryptomodule activation keys are stored under dual control in a secured environment when not in use.

5.1.2.4. CA Key Generation and Signing Rooms

CA key generation and signing occurs either in the secure storage room described in section 5.1.2.3 or in a room of commensurate security in close proximity thereto. BT's CA Administrators retrieve cryptographic materials necessary to perform key generation and certificate signing. At no time are cryptographic materials left unattended by fewer than two persons serving in trusted roles as specified in section 5.2.2.

5.1.3. Power and Air Conditioning

BT's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4. Water Exposures

BT has taken reasonable precautions to minimise the impact of water exposure to BT's systems.

5.1.5. Fire Prevention and Protection

BT has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. BT's fire prevention and protection measures have been designed to comply with local fire safety regulations

5.1.6. Media Storage

All media containing production software and data, audit, archive, or backup information is stored within BT facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7. Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroised in accordance with manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with BT's normal waste disposal requirements.

5.1.8. Off-site Backup

BT performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner.

5.1.9. Certificate Status Hosting, CMS and External RA Systems

All physical control requirements under Section 5.1 apply equally to any Certificate Status Hosting.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Personnel acting in trusted roles include CA and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by

persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations.

BT considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position must successfully complete the screening requirements set out in this CPS.

A list of personnel appointed to trusted roles is maintained and reviewed annually.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue Certificates to Subscribers.

5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking Certificates.

5.2.1.3. System Administrators/ System Engineers (Operator)

The System Administrator / System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / System Engineer also keeps critical systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DigiCert is operating in accordance with this CPS or an RA's Registration Practices Statement.

5.2.1.5. RA Administrators

RA Administrators are responsible for the RA software.

5.2.2. Number of Persons Required per Task

BT requires that at least two people acting in a trusted role take action for the most sensitive tasks, such as activating BT's Private Keys, generating a CA Key Pair, or backing up a BT Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access. Physical access to the CAs does not constitute a task as defined in this section, but is defined in section 5.1.

5.2.3. Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:
1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and

4. Those performing duties related to CA key management or CA administration.

To accomplish this separation of duties, BT specifically designates individuals to the trusted roles defined in Section 5.2.1 above Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. BT processes identify individuals acting in trusted roles, restricting an individual from assuming multiple roles at the same time

5.3. PERSONNEL CONTROLS

Personnel seeking to become Trusted Persons must present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government Contracts. Background checks are repeated at least every 10 years for personnel holding Trusted Positions.

5.3.1. Qualifications, Experience, and Clearance Requirements

BT requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily, as well as proof of any government clearances, if any, necessary to perform certification services under government contracts.

5.3.2. Background Check Procedures

Prior to commencement of employment in a Trusted Role, BT conducts background checks which include the following:

- confirmation of previous employment,
- check of professional reference,
- confirmation of the highest or most relevant educational qualification obtained,
- search of criminal records, and
- check of credit/financial records
-

To the extent that any of the requirements imposed by this section cannot be met due to a prohibition or limitation in local law or other circumstances, BT will utilise a substitute investigative technique permitted by law that provides substantially similar information, including but not limited to obtaining a background check performed by the applicable governmental agency.

The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person generally include (but are not limited to) the following:

- Misrepresentations made by the candidate or Trusted Person,
- Highly unfavourable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.
-

Reports containing such information are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behaviour uncovered by the background check. Such actions may include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

The use of information revealed in a background check to take such actions is subject to the applicable local laws.

5.3.3. Training Requirements

BT provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. BT maintains records of such training. BT periodically reviews and enhances its training programs as necessary.

BT's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- BT security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4. Retraining Frequency and Requirements

BT provides refresher training and updates to its personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily. Periodic security awareness training is provided on an on-going basis.

5.3.5. Job Rotation Frequency and Sequence

Not applicable.

5.3.6. Sanctions for Unauthorized Actions

Appropriate disciplinary actions are taken for unauthorised actions or other violations of BT policies and procedures. Disciplinary actions may include measures up to and including termination and are commensurate with the frequency and severity of the unauthorised actions.

5.3.7. Independent Contractor Requirements

In limited circumstances, independent contractors or consultants may be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a BT employee in a comparable position. Independent contractors and consultants who have not completed or passed the background check procedures specified in section 5.3.2 of this CPS are permitted access to BT's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.8. Documentation Supplied to Personnel

BT provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

BT's systems require identification and authentication at system logon with a unique username and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

BT enables all essential event auditing capabilities of its CA applications in order to record the events listed below. If BT's applications cannot automatically record an event, BT implements manual procedures to satisfy the requirements. For each event, BT records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. All event records are available to auditors as proof of BT's practices.

BT records at least the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, re-key requests, and revocation;
    b. All verification activities stipulated in the DigiCert CP and this CPS;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;
    e. Firewall and router activities; and
    f. Entries to and exits from the CA facility.

Log entries include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

5.4.2. Frequency of Processing Log

The CA system is continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

5.4.3. Retention Period for Audit Log

Audit logs shall be retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4. Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5. Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed weekly.

5.4.6. Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by BT personnel.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

BT performs annual risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorised access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. BT also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that BT has in place to control such risks. BT's Internal Auditors review the security audit data checks for continuity. BT's audit log monitoring tools alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. RECORDS ARCHIVAL

BT complies with all record retention policies that apply by law and retrieved as necessary by request of authorised parties. BT includes sufficient detail in all archived records to show that a Certificate was issued in accordance with this CPS.

5.5.1. Types of Records Archived

BT retains the following information in its archives (as such information pertains to BT's CA operations):

1. Accreditations of BT,
2. CP and CPS versions,
3. Audits,
4. Contractual obligations and other agreements concerning the operation of the CA,
5. System and equipment configurations, modifications, and updates,
6. Rejection or acceptance of a certificate request,
7. Certificate issuance, rekey, renewal, and revocation requests,
8. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
9. Any documentation related to the receipt or acceptance of a Certificate or token,
10. Subscriber Agreements,
11. Issued Certificates,
12. A record of certificate re-keys,
13. Data or applications necessary to verify an archive's contents,
14. Compliance auditor reports,
15. Changes to BT's audit parameters,
16. Any attempt to delete or modify audit logs,
17. CA Key generation and destruction,
18. Access to Private Keys for key recovery purposes,
19. Changes to trusted Public Keys,
20. Export of Private Keys,
21. Approval or rejection of a revocation request,
22. Appointment of an individual to a trusted role,
23. Destruction of a cryptographic module,
24. Certificate compromise notifications,
25. Remedial action taken as a result of violations of physical security, and
26. Violations of the CP or CPS.

5.5.2. Retention Period for Archive

BT retains archived data associated with Level 3 or Level 4 Certificates for at least 10.5 years. BT archives data for other certificate types for at least 7.5 years.

5.5.3. Protection of Archive

Archive records are stored at a secure location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the BT PMA or as required by law. BT maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If BT needs to transfer any media to a different archive site or equipment, BT will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive Backup Procedures

BT incrementally backs up electronic archives of its issued Certificate information on a daily basis. Copies of paper-based records shall be maintained in an off-site secure facility.

5.5.5. Requirements for Time-stamping of Records

BT automatically time-stamps archived records with system time (non-cryptographic method) as they are created. BT synchronizes its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6. Archive Collection System (internal or external)

BT's archive collection systems are internal, except for enterprise RA Customers. BT assists its enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorised Trusted Personnel are able to access the archive. The integrity of the information is verified when it is restored.

5.6. KEY CHANGEOVER

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, BT ceases using the expiring CA Private Key to sign Certificates and uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

BT maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. BT reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

BT makes regular system backups on a weekly basis and maintains backup copies of its CA Private Keys, which are stored in a secure, separate location. If BT discovers that any of its computing resources, software, or data operations have been compromised, BT assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If BT determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, BT suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity Private Key Compromise Procedures

If BT suspects that one of its CA Private Keys has been comprised or lost then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. Specifically, BT will:

1. Collect information related to the incident;
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. Make information available that can be used to identify which Certificates are affected, unless doing so would breach the privacy of a BT user or the security of BT's services;
6. Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
7. Isolate, contain, and stabilise its systems, applying any short-term fixes needed to return the system to a normal operating state;
8. Prepare and circulate an incident report that analyses the cause of the incident and documents the lessons learned; and
9. Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

BT may generate a new Key Pair and sign a new Certificate. If a disaster physically damages BT's equipment and destroys all copies of BT's signature keys then BT will provide notice to affected parties at the earliest feasible time.

5.7.4. Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, BT implements data backup and recovery procedures as part of its Business Continuity Disaster Recovery Plan (BCDRP). Stated goals of the BCDRP are to ensure that certificate status services be only minimally affected by any disaster involving BT's primary facility and that BT be capable of maintaining other services or resuming them as quickly as possible following a disaster. BT reviews, tests, and updates the BCDRP and supporting procedures at least annually.

BT's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes BT's primary CA operations to become inoperative, BT will re-initiate its operations at its secondary location giving priority to the provision of certificate status information capabilities, if affected.

5.8. CA OR RA TERMINATION

Before terminating its CA activities, BT will:

1. Provide notice and information about the termination by sending notice by email to its customers, and Application Software Vendors by posting such information on BT's web site; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, BT will:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CPS.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

All keys are generated using a FIPS-approved method or equivalent international standard.

BT's CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony. The cryptographic hardware is evaluated to FIPS 140-2 Level 3. Activation of the hardware requires the use of two-factor authentication tokens. BT creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process.

Subscribers must generate their keys in a manner that is appropriate for the certificate type.

6.1.2. Private Key Delivery to Subscriber

When end-user Subscriber key pairs are generated by the end-user, private key delivery to a Subscriber is not applicable.

Where RA or end-user Subscriber key pairs are pre-generated by BT on hardware tokens or smart cards, such devices are distributed to the RA or End User using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or End User using an out of band process. The distribution of such devices is logged by BT.

Where end-user Subscriber key pairs are pre-generated by Managed PKI Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Managed PKI Customer.

For Managed PKI Customers using Managed PKI Key Manager for key recovery services, the Customer may generate encryption key pairs (on behalf of End Users whose Certificate Applications they approve) and transmit such key pairs to End Users via a password protected PKCS # 12 file.

S/MIME email signature certificates are not distributed as PKCS#12 packages. S/MIME encryption certificates may be distributed as PKCS#12 packages using secure channels and sufficiently secure passwords sent out of band from the package.

6.1.3. Public Key Delivery to Certificate Issuer

End Users and RAs submit their public key to BT for certification electronically through the use of a Certificate Signing Request (CSR) or other digitally signed package in a session secured by Secure Sockets Layer (SSL). Where CA, RA, or End User key pairs are generated by BT, this requirement is not applicable.

6.1.4. CA Public Key Delivery to Relying Parties

DigiCert's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs. All accreditation authorities supporting DigiCert Certificates and all application software providers are permitted to redistribute DigiCert's root anchors.

BT generally provides the full certificate chain (including the issuing CA and any CAs in the chain) to the End User upon Certificate issuance.
BT CA Certificates may also be downloaded with the End User Certificate through query functions in the BT repository at
https://www.trustwise.com/services/client/searchSubscriberBT.html

6.1.5. Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using crypto-analysis during the period of expected utilisation of such key pairs. The BT Standard for minimum key sizes is the use of key pairs equivalent in strength to 2048 bit RSA for PCAs and CAs (ensuring that the modulus size, in bits, is evenly divisible by 8).
DigiCert's third and fifth generation (G3 and G5) PCAs have 2048 bit RSA key pairs.
BT issues a minimum key size equivalent in strength to 2048 bit RSA for RAs and end entity certificates key pairs.
All BT Sub-domain PCAs and CAs, and RAs and end entity certificates use SHA-2 for digital signature hash algorithm CAs (ensuring that the modulus size, in bits, is evenly divisible by 8).

6.1.6. Public Key Parameters Generation and Quality Checking

BT uses a cryptomodule that conforms to FIPS 186-2 and provides random value generation and on- board generation of Public Keys and a wide range of ECC curves.

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

BT's Certificates include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.

The use of a specific key is determined by the key usage extension in the X.509 Certificate.

BT does not operate Root CAs.

Subscriber Certificates assert key usages based on the intended application of the Key Pair and cannot include anyExtendedKeyUsage.

Key usage bits and extended key usages are specified in the certificate profile for each type of Certificate. BT's CA Certificates have at least two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the digitalSignature bit is also set.

Except for legacy applications using Level 1 and requiring a single key for dual use with both encryption and signature, BT does not issue Certificates with key usage for both signing and encryption. Instead, BT issues Subscribers two Key Pairs—one for key management and one for digital signature and authentication. For Certificates at Levels 1 that are used for signing and encryption in support of legacy applications, they must:

- be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CPS,
- never assert the non-repudiation key usage bit, and
- not be used for authenticating data that will be verified on the basis of the dual-use Certificate at a future time.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

BT has implemented a combination of physical, logical, and procedural controls to ensure the security of BT, and Enterprise Customer CA private keys. Subscribers are required by Contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorised use of private keys.

6.2.1. Cryptographic Module Standards and Controls

For PCA and Issuing Root CA key pair generation and CA private key storage, DigiCert and BT use hardware cryptographic modules that are certified at or materially meet the requirements of FIPS 140-2 Level 3.

6.2.2. Private Key (n out of m) Multi-person Control

BT has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. BT uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with CPS § 6.4.2.

6.2.3. Private Key Escrow

CA, private keys are not escrowed. Escrow of private keys for end-user Subscribers is explained in Section 4.12.

6.2.4. Private Key Backup

BT creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CPS. CA private keys are copied to backup hardware cryptographic modules in accordance with this CPS.

Modules containing on site backup copies of CA private keys are subject to the requirements of this CPS. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CPS.

BT does not store copies of RA private keys. For the backup of end-user Subscriber private keys, see Section 6.2.3 and Section 4.12.

6.2.5. Private Key Archival

Upon expiry of a BT CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CPS. The CA key pairs shall not be used for signing events after the expiration date, unless the CA certificate has been renewed in terms of this CPS.

BT does not archive copies of RA and Subscriber private keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

BT generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, BT makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

6.2.7. Private Key Storage on Cryptographic Module

CA or RA private keys held on hardware cryptographic modules shall be stored in an encrypted form

6.2.8. Method of Activating Private Keys

BT's Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. Subscribers should also take commercially reasonable measures for the physical protection of their workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization. When deactivated, private keys shall be kept in encrypted form only and secured. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys. See also Section 6.4.

6.2.9. Method of Deactivating Private Keys

BT CA private keys are deactivated upon removal from the token reader. BT RA private keys (used for authentication to the RA application) are deactivated upon system log off. BT RAs are required to log off their workstations when leaving their work area.

Client Administrators, RA, and end-user Subscriber private keys may be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, End Users have an obligation to adequately protect their private key(s) in accordance with this CPS.

6.2.10. Method of Destroying Private Keys

Where required, BT destroys CA private keys in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key. BT utilises the zeroisation function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

BT CA, RA and End User Certificates are backed up and archived as part of BT's routine backup procedures.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

BT Certificates have maximum validity periods of:

Type	Private Key Use	Certificate Term
Publicly Trusted Root CAs	No stipulation	25 years [1]

Publicly Trusted Sub CAs / Issuer CAs	No stipulation	15 years
End Entity / Client for all other purposes	No Stipulation	60 months

[1] *Certificates issued prior to 8th September 2017 may have a validity period of 37 years*

Participants shall cease all use of their key pairs after their usage periods have expired. Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

BT may voluntarily retire its CA Private Keys before the periods listed above to accommodate key changeover processes. BT does not issue Subscriber Certificates with an expiration date that exceeds the Issuer CA's public key term stated in the table above or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, represents an additional day.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

Activation data (Secret Shares) used to protect tokens containing BT CA private keys is generated in accordance with the requirements of Section 6.2.2 and the Key Ceremony Reference Guide. The creation and distribution of Secret Shares is logged.

BT RAs are required to select strong passwords to protect their private keys. BT's password selection guidelines require that passwords:

- be generated by the user;
- have at least eight characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

BT strongly recommends that Managed PKI Administrators, RAs, and End Users choose passwords that meet the same requirements. BT also recommends the use of two factor authentication mechanisms (e.g., token and pass phrase, biometric and token, or biometric and pass phrase) for private key activation.

6.4.2. Activation Data Protection

BT Shareholders are required to safeguard their Secret Shares and sign a Contract acknowledging their Shareholder responsibilities.

BT RAs are required to store their Administrator/RA private keys in encrypted form using password protection and their browser's "high security" option.

BT strongly recommends that Client Administrators, RAs and End Users store their private keys in encrypted form and protect their private keys through the use of a hardware token and/or strong pass phrase. The use of two factor authentication mechanisms (e.g., token and pass phrase, biometric and token, or biometric and pass phrase) is encouraged.

6.4.3. Other Aspects of Activation Data

No Stipulation.

6.5. COMPUTER SECURITY CONTROLS

BT performs all CA and RA functions using Trustworthy Systems that meet the requirements of this CPS. Managed PKI Customers must use Trustworthy Systems. BT recommends that Managed PKI customers follow the guidelines provided in the Enterprise Security Guide.

6.5.1. Specific Computer Security Technical Requirements

BT ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorised access. In addition, BT limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

BT's production network is logically separated from other components. This separation prevents network access except through defined application processes. BT use firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that may access production systems.

BT requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. BT requires that passwords be changed on a periodic basis.

Direct access to BT databases supporting the BT repository is limited to Trusted Persons in BT's operations group having a valid business reason for such access.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

Applications are developed and implemented by BT in accordance with BT systems development and change management standards. BT also provides software to its Managed PKI Customers for performing RA and certain CA functions. Such software is developed in accordance with BT system development standards.

DigiCert developed software, when first loaded, provides a method to verify that the software on the system originated from DigiCert, has not been modified prior to installation, and is the version intended for use.

6.6.2. Security Management Controls

BT has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. BT creates a hash of all software packages and BT software updates. This hash is used to verify the integrity of such software manually. Upon installation and periodically thereafter, BT validates the integrity of its CA systems.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

BT performs all its CA and RA functions using networks secured to prevent unauthorised access and other malicious activity. BT protects its communications of sensitive information through the use of encryption and digital signatures.

6.8. TIME-STAMPING

The system time on BT's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to a real time value

distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body. BT maintains an internal NTP server that synchronizes with cellular telephone networks and maintains the accuracy of its clock within one second or less.

Certificates, CRLs and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

7. CERTIFICATE, CRL, AND OCSP PROFILES

BT uses the ITU X.509, version 3 standard to construct digital Certificates for use within the BT subdomain of the DigiCert PKI. BT adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. BT generates non-sequential Certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All Certificates are X.509 version 3 Certificates.

7.1.2. Certificate Extensions

For Root CA, Subordinate CA, and Subscriber certificates that are publicly-trusted, BT abides by section 7.1.2 of the Baseline Requirements and configure the Certificate extensions to those requirements. Certificates must contain the ExtendedKeyUsage extension, aligning to Application Software Supplier granted trust bits and private PKI use cases. Certificates may not contain the anyEKU value. Subordinate CA Certificates created after January 1, 2019 for publicly trusted certificates will contain an EKU extension; and cannot include the anyExtendedKeyUsage KeyPurposeId.

BT's Subordinate CA Certificates created after January 1, 2019 are Technically Constrained by inclusion of one of or both of id-kp-emailProtection and/or id-kp-clientAuth Extended Key Usage (EKU) extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue certificates. The anyExtendedKeyUsage KeyPurposeId does not appear in the EKU extension of publicly trusted certificates. For Subordinate CA Certificates the value id-kp-serverAuth [RFC5280] is not present.

Other than in the case of the exception described in section 1.3.2, Subordinate CA certificates that include the id-kp-emailProtection extended key usage also include a name constraint extension as described in section 7.1.5.1.

7.1.3. Algorithm Object Identifiers

BT Certificates are signed using one of the following algorithms:

sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]

BT does not currently sign Certificates using RSA with PSS padding.

BT and Subscribers may generate Key Pairs using the following:

RsaEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1]
Dhpublicnumber	[iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1]

id-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]

For publicly-trusted certificates, BT uses the keys and hash algorithms specified in the CAB forum baseline requirements and Mozilla root store policy.

7.1.4. Name Forms

Each Certificate includes a unique serial number that is never reused.

For CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuer CA to support name chaining as specified in RFC 5280, section 4.1.2.4. Certificates are populated with the Issuer Name and Subject Distinguished Name required under Section 3.1.1. For publicly trusted certificates, Issuer DNs meet the CAB forum baseline requirements.

7.1.5. Name Constraints

BT may include name constraints in the nameConstraints field when appropriate. For publicly-trusted certificates, BT will follow the requirements of section 7.1.5 of the Baseline Requirements and as the following sections specify.

7.1.5.1. Name-Constrained serverAuth CAs

BT does not operate serverAuth CAs.

7.1.5.2. Name-Constrained emailProtection CAs

If the technically constrained Subordinate CA certificate includes the id-kp-emailProtection extended key usage, it also includes the Name Constraints X.509v3 extension with constraints on rfc822Name, with at least one name in permittedSubtrees, each such name having its ownership validated according to section 3.2.2 of this CPS.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by BT are listed in Section 1.2.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

BT includes brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension. Those Certificates may contain a CPS pointer qualifier that points to the applicable Relying Party Agreement or the applicable CPS.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

For revoked issuing CAs, the CRLReason indicated cannot be unspecified (0) or certificateHold(6). If the reason for revocation is unspecified, BT will omit the reasonCode entry extension, when not technically not

capable of issuance. If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate. BT specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

• unspecified (0), (*Reason code (0)_unspecified is only used if it is omitted from the CRL and OCSP in accordance with the baseline requirements*)
• keyCompromise (1),
• cACompromise (2),
• affiliationChanged (3),
• superseded (4), (*When a reason code is not specified, BT will log the revocation as (4) superseded or (5) Cessation of Operation*)
• cessationOfOperation (5), (*When a reason code is not specified, BT will log the revocation as (4) superseded or (5) Cessation of Operation*)

7.2.1. Version number(s)

BT issues version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	Subject DN of the issuing CA
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2. CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Specify reason for revocation in list of reason codes in section 7.2, if included.

7.3. OCSP PROFILE

Effective 2020-09-30, if an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus is present and asserted.

Effective 2020-09-30, the CRLReason indicated contains a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1. Version Number(s)

BT's OCSP responders conform to version 1 of RFC 6960.

7.3.2. OCSP Extensions

Not applicable.

The singleExtensions of an OCSP response does not contain the reasonCode (OID 2.5.29.21) CRL entry extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest versions of the ETSI Programs for Certification Authorities as required by the Mozilla Root Store policy and other programs listed in section 1.1 and 1.6.3.

In addition, an annual tScheme audit is performed for BT's Data Centre operations and key management operations supporting BT's public and Managed PKI CA services. Customer-specific CAs are not specifically audited as part of the audit of BT's operations unless agreed by BT with the Customer. BT shall be entitled to require that Managed PKI Customers undergo a compliance audit under this CPS and audit programs for these types of Customers.

In addition to compliance audits, BT shall be entitled to perform other reviews and investigations to ensure the trustworthiness of BT's Subdomain of the DigiCert PKI, which include, but are not limited to:

- BT or its authorised representative shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event BT or its authorised representative has reason to believe that the audited entity has failed to meet DigiCert PKI Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity's failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to security or integrity.
- BT or its authorised representative shall be entitled to perform "Supplemental Risk Management Reviews" on a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

BT or its authorised representative shall be entitled to delegate the performance of these audits, reviews, and investigations to a third-party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable co-operation with BT and the personnel performing the audit, review, or investigation.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

Compliance audits are performed at least annually at the sole expense of the audited entity.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The tScheme audits are performed by a UKAS accredited assessment body that demonstrates proficiency in public key infrastructure technology, information security tools and techniques, security auditing, and the third-party attestation function.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Compliance audits of BT's operations are performed by an assessment body that is independent of BT.

8.4. TOPICS COVERED BY ASSESSMENT

The scope of BT's annual tScheme audit covers BT's business practices disclosure, the integrity of BT's PKI operations, and compliance with this CPS and referenced requirements.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

With respect to compliance audits of BT's operations, significant exceptions or deficiencies identified during the Compliance Audit will result in a determination of actions to be taken. This determination is made by BT management with input from the auditor. BT management is responsible for developing and implementing a corrective action plan. If BT determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of the operation, a corrective action plan will be developed within 30 days and implemented within a commercially reasonable period of time agreed with the auditor. For less serious exceptions or deficiencies, BT Management, with input from the auditor, will evaluate the significance of such issues and determine the appropriate course of action.

8.6. COMMUNICATION OF RESULTS

Results of the compliance audit of BT's operations may be released at the discretion of BT management. For CAs that are not Technically Constrained, BT makes the results of its audits publicly available no later than three months after the end of the audit period as required in the CABF BR. In the event of a delay greater than three months, BT will provide an explanatory letter signed by the Qualified Auditor.

Details of audit reports can be found at https://www.trustwise.com/audit-repository/

8.7. SELF-AUDITS

On at least a quarterly basis, BT performs regular internal audits against a randomly selected sample of at least three percent of its Certificates issued since the last internal audit.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

BT and Customers are entitled to charge End Users for the issuance, management, and renewal of Certificates.

9.1.2. Certificate Access Fees

BT and Customers do not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3. Revocation or Status Information Access Fees

BT does not charge a fee as a condition of making the CRLs required by CPS available in a repository or otherwise available to Relying Parties. BT does, however, charge a fee for providing customised CRLs, OCSP services, or other value-added revocation and status information services. BT does not permit access to revocation information, Certificate status information, or time stamping in its repository by third parties that provide products or services that utilise such Certificate status information without BT's prior express written consent.

9.1.4. Fees for Other Services

BT does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, is subject to a Contract with the entity holding the copyright to the document.

9.1.5. Refund Policy

BT's refund policy is set out in its various customer contracts.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

Customers are encouraged to maintain a commercially reasonable level of cover for errors and omissions either through errors and omissions insurance or self-insured retention. BT maintains such errors and omissions insurance coverage.

9.2.2. Other Assets

No Stipulation

9.2.3. Insurance or Warranty Coverage for End-Entities

Not Applicable.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

The following records of End Users shall, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

1. CA application records, whether approved or disapproved,
2. Certificate Application records,
3. Private keys held by Enterprise Customers using Managed PKI Key Manager and information needed to recover such private keys,
4. Transactional records (both full records and the audit trail of transactions),
5. STN audit trail records created or retained by VeriSign, BT, or a Customer,
6. Audit reports created by BT or their respective auditors (whether internal or public). Results of the audit are distributed in alignment with specified requirements where relevant, but other system sensitive details are not disclosed publicly.
7. Contingency planning and disaster recovery plans, and
8. Security measures controlling the operations of BT hardware and software and the administration of Certificate services and designated enrolment services.

9.3.2. Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, BT's repository, and information contained within them are not considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3. Responsibility to Protect Confidential Information

BT secures private information from compromise and disclosure to third parties.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

BT has implemented a privacy policy, which is located at:
https://www.bt.com/privacy-policy/ in compliance with this CPS.

9.4.2. Information Treated as Private

BT treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. BT protects private information using appropriate safeguards and a reasonable degree of care.

9.4.3. Information Not Deemed Private

Subject to local laws, private information does not include Certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

BT employees and contractors are expected to handle personal information in strict confidence and meet the requirements of UK law concerning the protection of personal data.

9.4.5. Notice and Consent to Use Private Information

Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom the information applies. This section is subject to applicable privacy laws.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

BT Subdomain Participants acknowledge that BT shall be entitled to disclose Confidential/Private Information if, in good faith, BT believes disclosure is necessary in response to subpoenas and search warrants. This section is subject to applicable privacy laws.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

The allocation of Intellectual Property Rights among BT Subdomain Participants other than End Users and Relying Parties is governed by the applicable Contracts among such BT Subdomain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to End Users and Relying Parties.

9.5.1. Property Rights in Certificates and Revocation Information

CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. BT and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Third Party Charter referenced in the Certificate. BT and Customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, the Relying Third Party Charters, or any other applicable Contracts.

9.5.2. Property Rights in the CPS

BT Subdomain Participants acknowledge that BT retains all intellectual property rights in and to this CPS.

9.5.3. Property Rights in Names

A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4. Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and Subscribers are the property of the CAs and Subscribers that are the respective Subjects of these Certificates, subject to the rights of Customers using Managed PKI Key Manager, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs.

Notwithstanding the foregoing, DigiCert's root public keys and the root Certificates containing them, including all PCA public keys and self-signed Certificates, are the property of DigiCert. DigiCert licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software.

Finally, without limiting the generality of the foregoing, a CA's private key is the property of the CA, and the CA retains all Intellectual Property Right in and to its private key.

9.5.5. Violation of Property Rights

BT Subdomain Participants shall not knowingly violate the intellectual property rights of any third party.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

BT's Contracts warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to this CPS in all material aspects.

9.6.2. RA Representations and Warranties

BT's Contracts require RAs to warrant that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS, and
- Revocation services and use of a repository conform to this CPS in all material aspects.

9.6.3. Subscriber Representations and Warranties

BT's Contracts require Subscribers to warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the End User and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created,
- Their private key is protected and no unauthorised person has ever had access to the End User's private key,
- All representations made by the Subscriber in the Certificate Application the End User submitted are true,
- All information supplied by the End User and contained in the Certificate is true,
- The Certificate is being used exclusively for authorised and legal purposes, consistent with this CPS, and
- The End User is an End User and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

9.6.4. Relying Party Representations and Warranties

Relying Third Party Charters require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in this CPS.
Any unauthorized reliance on a Certificate is at a party's own risk.

Relying Party Agreements may include additional representations and warranties.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, BT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. BT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. BT DOES NOT GUARANTEE THE AVAILABILITY OF ANY PRODUCTS OR SERVICES AND MAY MODIFY OR DISCONTINUE ANY PRODUCT OR SERVICE OFFERING AT ANY TIME.

9.8. LIMITATIONS OF LIABILITY

To the extent permitted by applicable law, BT's Contracts and Relying Third Party Charters limit, and other Contracts shall limit BT's liability. Limitations of liability include an exclusion of indirect, special, incidental, and consequential damages. Liability caps limiting BT's damages concerning a specific Certificate are detailed in specific Contracts.

9.9. INDEMNITIES

9.9.1. Indemnification by Subscribers

To the extent permitted by applicable law, BT's Contracts require, and other Contracts shall require, End Users to indemnify BT and any non-BT CAs or RAs for:

- Falsehood or misrepresentation of fact by the End User on the End User's Certificate Application,

- Failure by the End User to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The End User's failure to protect the End User's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the End User's private key, or
- The End User's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

9.9.2. Indemnification by Relying Parties

To the extent permitted by applicable law, BT's Contracts and Relying Third Party Charters require, and other Contracts shall require, Relying Parties to indemnify BT and any non-BT CAs or RAs for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10. TERM AND TERMINATION

9.10.1. Term

This CPS and any amendments to the CPS are effective when published to BT's online repository and remain in effect until replaced with a newer version.

9.10.2. Termination

This CPS as amended from time to time, shall remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

BT will communicate the conditions and effect of this CPS's termination via the BT Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

BT accepts notices related to this CPS at the locations specified in Section 1.5.2. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from BT. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 1.5.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested.

BT will notify Mozilla (via DigiCert) if:

1. Ownership or control of the CA certificates changes;
2. An organization other than the CA obtains control of an unconstrained intermediate certificate (as defined in section 5.3.2 of the Mozilla Root Store policy) that directly or transitively chains to DigiCert's included certificate(s);
3. Ownership or control of BT's operations changes; or
4. There is a material change in BT's operations (e.g., when the cryptographic hardware related to a certificate in Mozilla's root store is consequently moved from one secure location to another).

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This CPS is reviewed annually. Amendments to this CPS shall be made by BT and approved by the BT Policy Management Authority (PMA). Amendments shall either be in the form of a document containing an amended form of the CPS or an update. Amended versions or updates will be published at:
https://www.trustwise.com/legal-repository/

Updates supersede any designated or conflicting provisions of the referenced version of the CPS. The PMA shall determine whether changes to the CPS require a change to the Certificate policy object identifiers of the Certificate policies corresponding to each Class of Certificate.

9.12.2. Notification Mechanism and Period

BT reserves the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. BT's decision to designate amendments as material or non-material shall be within BT's sole discretion.

BT will post amendments to the CPS in the BT Repository, which is located at:
https://www.trustwise.com/legal-repository/

Notwithstanding anything in the CPS to the contrary, if BT believes that material amendments to the CPS are necessary immediately to stop or prevent a breach of the security, BT shall be entitled to make such amendments by publication in the BT Repository.

Such amendments will be effective immediately upon publication.

9.12.3. Circumstances under which OID Must Be Changed

If the PMA determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each Class of Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13. DISPUTE RESOLUTION PROVISIONS

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Disputes between BT and one of its Customers shall be resolved pursuant to provisions in the applicable Contract between the parties.

9.14. GOVERNING LAW

Subject to any limits appearing in applicable law, English Law shall govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of Contract or other choice of law provisions and without the requirement to establish a commercial nexus in England. This choice of law is made to ensure uniform procedures and interpretation for all BT Subdomain Participants, no matter where they are located.

This governing law provision applies only to this CPS. Contracts incorporating the CPS by reference may have their own governing law provisions, provided that this Section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such Contracts, subject to any limitations appearing in applicable law.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. BT meets the requirements of the European data protection laws and has established

appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

Not Applicable

9.16.2. Assignment

Not Applicable.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

Not Applicable.

9.16.5. Force Majeure

To the extent permitted by applicable law, BT's Contracts and Relying Third Party Charters includes, and other Contracts shall include, a force majeure clause protecting BT.

9.17. OTHER PROVISIONS

No stipulation.

APPENDIX A: Acronyms, Definitions and References

Table of Acronyms

Acronym	*Term*
AATL	*Adobe Approved Trust List*
BR	*Baseline Requirements*
CA	*Certificate Authority or Certification Authority*
CAA	*Certification Authority Authorization*
CAB	*"CA/Browser" as in "CAB Forum"*
CABF	*CAB Forum*
CMS	*Card Management System*
CP	*Certificate Policy*
CPS	*Certification Practice Statement*
CRL	*Certificate Revocation List*
CSPRNG	*Cryptographically Secure Pseudo-Random Number Generator*
CSR	*Certificate Signing Request*
CSU	*Cryptographic Storage Unit.*
CT	*Certificate Transparency*
DBA	*Doing Business As (also known as "Trading As")*
DCPA	*DigiCert Policy Authority*
DNS	*Domain Name Service*
DV	*Domain Validated*
ETSI	*European Telecommunications Standards Institute*
EU	*European Union*
EV	*Extended Validation*
FIPS	*(US Government) Federal Information Processing Standard*
FQDN	*Fully Qualified Domain Name*
FTP	*File Transfer Protocol*
GLEIF	*Global Legal Entity Identifier Foundation*
HISP	*Health Information Service Provider*

HSM	***Hardware Security Module***
HTTP	***Hypertext Transfer Protocol***
IANA	***Internet Assigned Numbers Authority***
ICANN	***Internet Corporation for Assigned Names and Numbers***
IdM	***Identity Management System***
IDN	***Internationalized Domain Name***
IETF	***Internet Engineering Task Force***
IGTF	***International Grid Trust Federation***
ISSO	***Information System Security Officer***
ITU	***International Telecommunication Union***
IV	***Individual Validated***
KRB	***Key Recovery Block.***
LEI	***Legal Entity Identifier***
LSVA	***Logical security vulnerability assessment.***
MICS	***Member-Integrated Credential Service (IGTF)***
NIST	***National Institute of Standards and Technology***
OCSP	***Online Certificate Status Protocol***
OID	***Object Identifier***
ONC	***Office of the National Coordinator for Healthcare (U.S.)***
OSU	***Online Sign-Up (Wi-Fi Alliance Hotspot 2.0)***
OV	***Organization Validated***
PCA	***Primary Certification Authority.***
PIN	***Personal Identification Number (e.g. a secret access code)***
PKCS	***Public-Key Cryptography Standard.***
PKI	***Public Key Infrastructure***
PKIX	***IETF Working Group on Public Key Infrastructure***
PMA	***Policy Management Authority.***
RA	***Registration Authority***
RFC	***Request for Comments (at IETF.org)***

S/MIME	***Secure multipurpose Internet mail extensions.***
SAN	***Subject Alternative Name***
SHA	***Secure Hashing Algorithm***
SSL	***Secure Sockets Layer***
STN	***Symantec Trust Network***
TLD	***Top-Level Domain***
TLS	***Transport Layer Security***
TSA	***Time Stamping Authority***
TST	***Time-Stamp Token***
TTL	***Time To Live***
UTC	***Coordinated Universal Time***
X.509	***The ITU-T standard for Certificates and their corresponding authentication framework***

Definitions

Term	*Definition*
Administrative CA	A type of BT CA that issues Certificates to BT RAs, Managed PKI Customer personnel (Managed PKI Administrators), Affiliate Administrators, and Automated Administration servers.
Administrator	A Trusted Person within the organisation of a Processing Centre, Service Centre, or Managed PKI Customer, that performs validation and other CA or RA functions.
Administrator Certificate	A Certificate issued to an Administrator that may only be used to perform CA or RA functions.
Applicant	An entity applying for a certificate
Application Software Vendor	A software developer whose software displays or uses DigiCert Certificates and distributes DigiCert's Root Certificates
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrolment information matches information contained in a database.
Automated Administration Software Module	Software that performs Automated Administration.
BT Repository	BT's database of Certificates and other relevant VeriSign Trust Network information accessible on-line.
BT Security Policy	The highest-level document describing BT's security policies.
BT Subdomain Participants	An individual or organisation that is one or more of the following within the BT's Subdomain of the STN: BT, a Customer, a Reseller, an End User, or a Relying Party.
CAB Forum	Defined in the EV Guidelines
Certificate	A message that, at least, states a name or identifies the CA, identifies the End User, contains the End User's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organisation that requests the issuance of a Certificate by a CA.
Certificate Application	A request from a Certificate Applicant (or authorised agent of the Certificate Applicant) to a CA for the issuance of a Certificate.
Certificate Approver	Defined in the EV Guidelines
Certificate Chain	An ordered list of Certificates containing an End User Certificate and CA Certificates, which terminates in a root Certificate.

Certificate Policies (CP)	The document entitled "Symantec Trust Network Certificate Policies" and is the principal statement of policy governing the STN.
Certificate Requestor	Defined in the EV Guidelines
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation.
Certificate Signing Request	A message conveying a request to have a Certificate issued.
Certification Authority (CA)	An entity authorised to issue, manage, revoke, and renew Certificates in the STN.
Certification Practice Statement (CPS)	This document, which is a statement of the practices that BT employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates, and requires its Managed PKI Customers to employ.
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrolment for a Certificate. When issued a Certificate, the Certificate Applicant becomes an End User and a CA or RA can use the Challenge Phrase to authenticate the End User when the End User seeks to revoke or renew the End User's Certificate.
Class	A specified level of assurances as defined within the CP. See STN CP Section 1.1.1. The distinctions are summarised in CPS Section 1.1.1.
Client Managed PKI Customer	An organisation that has obtained Managed PKI services from BT, whereby the organisation becomes a CA within the STN to issue client Certificates. Client Managed PKI Customers outsource back-end functions of issuance, management, and revocation to BT, but retain for themselves the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
Client Managed PKI Lite Customer	An organisation that has obtained Managed PKI Lite services from BT, whereby the organisation becomes a Registration Authority within the STN to assist BT to issue client Certificates. This CA delegates to Client Managed PKI Lite Customers the RA functions of approving or rejecting Certificate Applications and initiating revocations and renewals of Certificates.
Compliance Audit	A periodic audit that a Processing Centre, Service Centre, or Managed PKI Customer undergoes to determine its conformance with STN Standards that apply to it.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorised disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorised use, or other compromise of the security of such private key.

Confidential/Private Information	Information required to be kept confidential and private pursuant to STN CP Section 2.8.1.
Contract	An agreement used by a CA or RA setting forth the terms and conditions under which an individual or organisation acts as an End User. Within the BT Subdomain, this is the BT Customer Contract.
Contract Signer	Defined in the EV Guidelines
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used.
Customer	An organisation that is a Managed PKI Customer
End User	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organisational Certificate, an organisation that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. An End User is capable of using, and is authorised to use, the private key that corresponds to the public key listed in the Certificate.
Enterprise Security Guide	A document setting forth security recommendations for Managed PKI Customers.
EV Guidelines	Defined in Section 1.1.
Exigent Audit/Investigation	An audit or investigation by BT, where BT has reason to believe that an entity's failure to meet STN Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of the STN posed by the entity has occurred.
Infrastructure Certification Authority (Infrastructure CA)	A type of BT CA that issues Certificates to components of the BT infrastructure supporting certain BT services. Infrastructure CAs do not issue CA, RA, or End User Certificates.
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights.
Intermediate Certification Authority (Intermediate CA)	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the End User's Certificate.
Key Ceremony Reference Guide	A document describing Key Generation Ceremony requirements and practices.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Client Managed PKI Customer using Managed PKI Key Manager.

Key Recovery Block (KRB)	A data structure containing an End User's private key that is encrypted using an encryption key. KRBs are generated using Managed PKI Key Manager software.
Key Recovery Service	A VeriSign service provided by BT that provides encryption keys needed to recover a Key Recovery Block as part of a Client Managed PKI Customer's use of Managed PKI Key Manager to recover an End User's private key.
Managed PKI	Symantec's fully integrated managed PKI service offered by BT that allows enterprise Customers of BT to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI permits enterprises to secure messaging, intranet, extranet, virtual private network, and ecommerce applications.
Managed PKI Administrator	An Administrator that performs validation or other RA functions for a Managed PKI Customer.
Managed PKI Administrator's Handbook	A document setting forth the operational requirements and practices for Managed PKI Customers.
Managed PKI Certificate	A Certificate whose Certificate Application was approved by a Managed PKI Customer.
Managed PKI Contract	A Contract under which an organisation becomes a Managed PKI Customer and agrees to be bound by this CPS.
Managed PKI Control Centre	A web-based interface that permits Managed PKI Administrators to perform Manual Authentication of Certificate Applications.
Managed PKI Customer	An organisation that is a Client Managed PKI Customer or a Client Managed PKI Lite Customer.
Managed PKI Key Management Service Administrator's Guide	A document setting forth the operational requirements and practices for Client Managed PKI Customers using Managed PKI Key Manager.
Managed PKI Key Manager	A key recovery solution for those Client Managed PKI Customers choosing to implement key recovery under a special Managed PKI Contract.
Managed PKI Lite	A type of Managed PKI service that permits an organisation to become a Registration Authority within the STN to assist the BT CA to issue client Certificates.
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.

Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a STN Certificate may provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation.
Non-verified End User Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by the CA or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant.
Online Certificate Status Protocol (OCSP)	A protocol for providing Relying Parties with real-time Certificate status information.
OCSP Responder	An online software application operated under the authority of BT and connected to its repository for processing certificate status requests
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked.
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Policy Management Authority (PMA)	The organisation within BT responsible for promulgating this policy
Primary Certification Authority (PCA)	A CA that acts as a root CA for a specific Class of Certificates, and issues Certificates to CAs subordinate to it.
Processing Centre	An organisation such as BT that creates a secure facility housing, among other things, the cryptographic modules used for the issuance of Certificates. In the Consumer and Web Site lines of business, Processing Centres act as CAs and perform all Certificate lifecycle services of issuing, managing, revoking, and renewing Certificates. In the Enterprise line of business, Processing Centres provide lifecycle services on behalf of their Managed PKI Customers or the Managed PKI Customers of the Service Centres subordinate to them.

Public Key Infrastructure (PKI)	The architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Qualified Certificate	A Certificate that meets the requirements of EU law and is provided by an Issuer CA meeting the requirements of EU law
Registration Authority (RA)	An entity approved by a CA to assist Certificate Applicants in applying for Certificates, and to approve or reject Certificate Applications, revoke Certificates, or renew Certificates.
Relying Party	An individual or organisation that acts in reliance on a certificate and/or a digital signature.
Relying Party Agreement	An agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using BT's Repository.
Relying Third Party Chart	A policy statement used by a CA setting forth the terms and conditions under which an individual or organisation acts as a Relying Party.
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement.
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CPS Section 6.2.2.
Secure Sockets Layer (SSL)	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.
Subdomain	The portion of the DigiCert PKI under control of an entity and all entities subordinate to it within the DigiCert hierarchy.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organisational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	The entity identified as the subject in the Certificate
Subscriber Agreement	An agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

Supplemental Risk Management Review	A review of an entity by BT following incomplete or exceptional findings in a Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business.
Trusted Person	An employee, contractor, or consultant of an entity responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CPS § 5.2.1.
Trusted Position	The positions within an entity that must be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognised in classified government nomenclature.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol, the Registry Data Access Protocol, or an HTTPS website