Lloyd's Register Quality Assurance – tScheme Report

tScheme Report

This report relates to the assessment of the Electronic Trust Service known as:

BT Managed PKI Security
(Formerly BT Assure PKI)

Provided By:

British Telecommunications plc

LRQA reference	**LRQ0961984**
Assessment dates	**March 2017**
Assessment criteria	**tScheme**
Assessment location	**Cardiff**
Assessment team	**Colin Robbins** **Jeff Northam**
LRQA office	**Birmingham**

©LRQA **2017** All rights reserved. LRQA and **British Telecommunications plc** permits *tScheme* Limited to copy the contents in whole or part for all purposes relating to application for, processing of, publication of and investigation of Grant of Approval for the Service which is the subject of this report, notwithstanding the undertaking given in §0.5 of tSd 0238 Model Assessment Report (Service)

Lloyd’s Register Quality Assurance – tScheme Report

Contents **Page**

2.0 Certification Statement **Page 3**

3.0 Method and evidence employed **Page 6**

tSd 0111 Base **Page 6**

tSd 042 Registration services **Page 8**

tSd 0102 Certification Authority [QC] **Page 9**

tSd 0103 Signing Key Pair Management **Page 11**

tSd 0104 Certificate Generation **Page 12**

tSd 0105 Certificate Dissemination **Page 13**

tSd 0106 Certificate Status Management **Page 14**

tSd 0107 Certificate Status Validation **Page 15**

4.0 Assessor comments **Page 16**

Lloyd’s Register Quality Assurance – tScheme Report

Certification Statement

We:

Lloyd’s Register Quality Assurance Limited (LRQA)

of:

LRQA UK,
1 Trinity Park,
Bickenhill Lane,
Birmingham
B37 7ES

certify that the management system used to deliver:

BT Assure PKI

PUBLIC SERVICE DESCRIPTION

Version 1.9 (27 March 2017).

BT Managed Public Key Infrastructure (PKI) Security is a managed service that provides the technology and processes required to issue digital certificates. The service is suitable for any organisation that needs to issue certificates - these can be issued under either the Symantec Trust Network (STN) public hierarchy and the STN CPS or the Customer's own self-signed root and the non-STN CPS.

Within Managed PKI Security, the Registration Authority (RA) and Certification Authority (CA) functions are separated. The customer organisation performs the RA function and BT performs the CA function.

This arrangement allows the customer RA function to apply validation criteria that are based on its local business knowledge and approve or reject certificate requests using its own business rules. It also allows the organisation to delegate the complex and difficult CA management function to a specialist organisation that has the infrastructure and practices required to protect and manage sensitive CA Keys and PKI records. Specific CA functions managed by BT are:

CA Key Generation and Management
Certificate Status Management and Validation

BT uses its own RA to validate requests for the service, confirming that the applicant company is registered and that the Managed PKI Security Administrator has the organisational authority required to operate the RA and enter into the Managed PKI Security contract on the applicant company's behalf.

Following acceptance of the request a new CA Certificate is issued and the CA signing keys installed at the secure CA facility operated by BT.

The service is built using Symantec technology and utilises industry standard protocols to protect order information and to deliver certificates. Employees, or customers, of the subscribing organisation apply for end user certificates from a local web site using their browser. Requests are validated by the local RA, digitally signed & encrypted and then sent to the CA, where certificates are constructed and signed using the organisations CA Digital Certificate.

BT provides the Managed PKI Security customer with certificate status data, either in the form of a Certificate Revocation List or through the use of the Online Certificate Status Protocol (OCSP), to validate certificates within their application(s). (Note: OCSP is not available to Managed PKI Security FastTrack customers). BT also provides status information to relying parties.
For further information, please see the Service Policy Disclosure Statement. This can be found by clicking on the Service Policy Disclosure Statement link in the How Can Help section at:

http://www.globalservices.bt.com/uk/en/products/managed-pki-security

as supplied by:

British Telecommunications plc

81, Newgate Street, London, EC1A 7AJ

meets the requirements of ISO/IEC 27001:2005 and the criteria defined in the *tScheme* Approval Profiles:

tSd 0111 Base approval profile	Issue	**3-00**
tSd 0042 Registration services	Issue	**3-02**
tSd 0102 Certificate authority **Excluding** Qualified Certificates	Issue	**3-01**
tSd 0103 Signing key pair management **Excluding/** Qualified Certificates	Issue	**3-02**
tSd 0104 Certificate generation **Excluding** Qualified Certificates	Issue	**3-01**
tSd 0105 Certificate dissemination	Issue	**3-01**
tSd 0106 Certificate status management	Issue	**3-01**
tSd 0107 Certificate status validation	Issue	**3-01**

in accordance with:

ISO/IEC 27001:2013 and tScheme

as at the date of this report being;

30 March 2017

declaration made by:

Jeff Northam **27001 Assessor**

Colin Robbins **tScheme Assessor**

on behalf of LRQA.

2.1 Qualifications to the Certification

Previous tScheme approval has included Qualified Certificates.

Qualified Certificates have been taken out of scope for this approval.

BT does not issue qualified certificates with this service.   A customer of the Managed PKI Services does issue qualified certificate; this is subject to a separate audit in the customer’s host country.

3.0 Method and evidence employed

The assessment involved comparing the evidence presented against the criteria specified in the *tScheme* Approval Profiles and reviewing working practices to verify compliance. Compliance against each profile heading is detailed below. Acceptability of evidence and establishment of compliance with the criteria was verified by examination of the evidence and/or interview of relevant personnel.

tSd 0111 Base

3.1	Business probity and management competence Enterprise level criteria	The organisational structure is fully defined and the management roles and responsibilities are specified. BT Global Services, a division of BT Telecommunications plc, registered in England No.1800000 is the Operational Enterprise. The service is covered by ISO 27001 certification – different elements of the service fall under different 27001 certificates.
3.2	Management and security policies and procedures	Security policies, procedures and security management structure was reviewed and found to be compliant with the tScheme requirements. Document control, risk management and internal audit processes were observed.
3.3	Assurance of technical infrastructure	BT Managed PKI ISMS certified to ISO/IEC 27001: 2013 (LRQ0961984) Reviewed at Monthly management meetings. Penetration testing has been undertaken, by an independent BT team. Symantec also assured the system meets their requirements.
3.4	Suitability of personnel used	Personnel security and trustworthiness are addressed in the Trust Service Security Policy Document. Personnel meeting these requirements are deemed to be Trusted Persons. Roles and responsibilities include experience and qualification requirements for Trusted Persons and are included in Job

		Descriptions. Policies and procedures governing separation of duties and privileges and conflicts of interest are defined through the CPS.
3.5.1	Externally provided Trust Services and Trust Service Components	Externally provided trust components are provided as part of the BT group. BT have been advised clarify is needed on how these elements all come together under the ISMS.
3.5.2	Suppliers of technology, equipment and general support services	Contractual relationships exist with Symantec.
3.6	Service related policies and procedures	S3A Issue 19 provides an accurate description of BT Managed PKI service. Verified that the services referenced in the S3A/PSD are operational Services in accordance with the tScheme definition.
3.6.1	Information for users	Information for users is published at: http://www.globalservices.bt.com/uk/en/products/managed-pki-security and includes • Public Service Description • Certification Practice Statement • Privacy Statement • Service Policy Disclosure Statement
3.6.2	Information for assessors	An Assessor Service Description is available and was used during the assessment (Annex of the S3A)

tSd 0111	**Base**	
Schedule 1	Enterprise Criteria	Schedule 1 criteria complied with according to tScheme requirements.
Schedule 2	Service Policy disclosure Statement	Service Policy Disclosure Statement Issue 1.9 dated 27th March 2017 was assessed and meets requirements.

tSd 0042 Registration Services

3	Criteria	Registration for this scope include customer administrators (no PKI credentials). Customers are provided the tools to provide the registration authority to issue end-user certificates.
3.1.1	Information for users	All information required for users under tScheme made available to users, primarily through the BT Certification Practice Statement. Available publicly online at http://www.globalservices.bt.com/uk/en/products/managed-pki-security
3.2	Proxies	Proxies are not used by BT. Customers may use proxies.
3.3	Data Protection	BT's data protection policies and procedures are followed. Assessment for GDPR has been made.
3.4	Registrant agreement	Requirements documented within the BT Certification Practice Statement and reflected within the customer contracts.
3.5	Relying TSP agreement	No relying TSP is used.
3.6	Delivery of credentials	Delivery mechanism specified within the BT Certification Practice Statement. Credentials are only delivered using secure channels.
3.7	Internal procedures	Local procedures assessed and observed up to date and applicable to all tScheme activities
3.8	Records	Records were demonstrated to be maintained within the Symantec product, archived and managed in accordance with Service Policy.

tSd 0042 Registration Services

		A minor noncompliance with archival was identified, and a corrective action plan agreed.

tSd 0102 **Certification Authority**

3	Criteria	
3.1	Public Service Description	Public service description is available and published. Checked as part of the review of the Base Approval Profile.
3.2	Assessors Service Definition	The ASD specifies how the service's constituent parts are delivered. References to Qualified Certificate has been removed from the ASD in line with the agreed scope change.
3.3	Service/Certificate Policy	Documents up to date and available.
3.4	Service/Certification Practice Statement	BT Certification Practice Statement and SPDS are available on the public website. BT Certification Practice Statement maintenance is addressed in Section 8 of the BT Certification Practice Statement. Minor non-compliances between the CPS and local procedures were identified – corrective action plans have been agreed. The issues do no place service users at risk.
3.5.1	Authority and responsibility	Detailed in Local Procedures for Management and Governance.
3.5.2	Subscriber certificate renewal, rekey and update	Renewal, rey-key and update circumstances defined in the CPS. Local procedures used to implement functions assessed during this audit.
3.5.3	CA Key Management	CA Key management reference in CPS and addressed in local procedures.
3.5.4	Certificate issue	Certificate Management with respect to issuance managed with local procedures assessed.

tSd 0102	Certification Authority	
3.6	Records	Records are maintained in accordance with BT’s data retention policy and in line with Symantec’s product recommendations.

tSd 0103 Signing key Pair Management

3	Criteria	
3.1.1.1	Signing Key Pair generation and provision - Information for users	Addressed in the BT Certification Practice Statement sections 6 and 7. Key Pair Provision is managed by BT customers.
3.1.1.2	Signing Key Pair generation and provision - Information for assessors	The required information is provided in the S3A
3.1.2	Signing Key Pair generation and provision - Specific QC criteria	Service not provided.
3.2.1.1	Signing capability provision - Information for users	Service not provided.
3.3.1.1	Signing capability revocation - Information for users	Service not provided.
3.4	Recording	Records are maintained in accordance with the Certificate Practice Statement.

tSd 0104	**Certificate Generation**	
3	Criteria	
3.1.1	Information for users	Certificate Practice Statement provides this information for users, publicly available.
3.1.2	Information for assessors	Certificate Practice Statement and Assessor Service Description referenced documents provide information for assessors.
3.2	Creation of certificates	Documented within the BT Certification Practice Statement and local Key Ceremony Procedures.
3.3	Records	Records are maintained in accordance with the Certificate Practice Statement. Records of key ceremonies are available in electronic and paper forms.

tSd 0105 Certificate Dissemination

3	Criteria	
3.1.1	Information for users	As documented in the BT Certification Practice Statement.
3.1.2	Information for assessors	As documented in the BT Certification Practice Statement and Assessor Service Description referenced documents.
3.2	Certificate dissemination mechanism(s)	Certificates are made available as per the CPS. Public certificate are available at: https://www.trustwise.com/services/client/searchSubscriberBT.html
3.3	Records	Records are maintained in accordance with the Certificate Practice Statement.

tSd 0106 Certificate Status Management

3	Criteria	
3.1.1	Information for users	Detail of methods available are in the Certificate Practice Statement. CRLs are available via HTTP at Onsitecrl.trustwise.com. OCSP is an optional service the customer can request.
3.1.2	Information for assessors	Detail of methods available in the Certificate Practice Statement. Assessor Service Description and referenced documents provide details.
3.2	Internal procedures	The service provides CRLs and optionally OCSP. These are automatically updated, with service monitoring to detect errors.
3.3	Records	Records are maintained in accordance with the Certificate Practice Statement.

tSd 0107 Certificate Status Validation

3	Criteria	**Surveillance May 2016**
3.1.1	Information for users	Detail of methods available are in the Certificate Practice Statement. CRLs are available via HTTP at Onsitecrl.trustwise.com. OCSP is an optional service the customer can request.
3.1.2	Information for assessors	Assessor Service Description provide document details that in turn provide detailed and sufficient information.
3.2	Relying Party Agreement	Documented in the BT Trust Services Relying Party Charter,
3.3	Internal procedures	Local procedures manage Certificate Status Validation, these are documented and consistent with requirements. CRL were sampled and found to be accurate.
3.4	Records	Records are maintained in accordance with the Certificate Practice Statement.

4 Assessor comments

This tScheme re-certification assessment has successfully demonstrated BT Managed PKI Security is being managed, in accordance with the published certification policy and practice statement, reflecting the service documented in the Public Service Description.

NOTE: Qualified Certificate have been taken out of scope.

Several minor non-compliances were noted, and corrective action plans agreed. These do not place the service users or relying parties at significant risk and do not prevent the re-certification recommendation.

- 136282_SBCCRW01. Missed schedule for an Internal Audit.
- 136282_SBCCRW02. The method of Vulnerability Assessment documented in the CPS is inaccurate.
- 136282_SBCCRW03. Some electronic records are not archived as per the CPS.
- 136282_SBCCRW04. Weekly inspection of audit logs is not performed (other risk mitigation factors are in place).
- 136282_SBCCRW05. Internal audit required by a local procedure not undertaken.
- 136282_SBCCRW06. Upon service termination written process devices from operational practice.