CONFORMITY ASSESSMENT BODY
EIDAS
TRUST SERVICE PROVIDERS
ISO 27001
LA ISO 27001
LI ISO 27001
RM ISO 27005

CONFORMITY ASSESSMENT REPORT

INTRODUCTION

British Telecom PLC

Trust Service Provider providing Managed PKI service

This conformity assessment[1] has been registered under LSTI N°1665_129 - V1.0

Saint Malo, 22 August 2019

Signature numérique de Jean-Marc Philippe PEZERET
Date : 2019.08.24 20:47:11 +02'00'

Jean-Marc PEZERET
Lead Auditor

CONFIDENTIAL

ACCRÉDITATION COFRAC N°5-0546
CERTIFICATION DE PRODUITS ET SERVICES PORTÉE DISPONIBLE SUR WWW.COFRAC.FR

[1] LSTI SAS has been accredited pursuant to the accreditation certificate of French Accreditation Body COFRAC with registration number 5-0546 in accordance with NF EN ISO/IEC 17065:2013 as a certification body for products, processes, and services in accordance with the Annex of the accreditation certificate and in accordance with the eIDAS EU Regulation and the ETSI European Norms (details on www.cofrac.fr).

CONTENT

Conformity Assessment Body

LSTI SAS
10 Avenue Anita Conti
35400 Saint-Malo
France

LSTI Worldwide Limited
Clifton House – Fitzwilliam street lower
Dublin 2
Ireland

Armelle Trotin Head of certification
armelle.trotin@lsti.eu
Phone: +33 608675144

Accreditor

COFRAC
52 Rue Jacques Hillairet
75012 Paris
FRANCE
Phone: +33 144688220

Attestation of accreditation downloadable https://tools.cofrac.fr/annexes/sect5/5-0546.pdf

Description of the trust services

1 Designation of the trust service provider and of the trust services

BRITISH TELECOM PLC
BT HQ : BT Centre, 81 Newgate Street - EC1A 7AJ London - United Kingdom
Registered under the number: 01800000
BT PLC site : Ty Cynal - Watkiss way - CARDIFF - ENGLAND
Email : lyndon.a.davies@bt.com
Repository site : http://www.trustwise.com/repository/CPS/cps.htm

2 Abbreviations

BRG	Baseline Requirements Guidelines
CA	Certification Authority
CAB	CA/Browser
CAB	Forum CA/Browser Forum
CARL	Certification Authority Revocation List
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DVC	Domain Validation Certificate
DVCP	Domain Validation Certificate Policy
EAL	Evaluation Assurance Level
EV	Extended Validation
EVC	Extended Validation Certificate
EVCG	Extended Validation Certificate Guidelines
EVCP	Extended Validation Certificate Policy
IVC	Individual Validation Certificate
IVCP	Individual Validation Certificate Policy
LCP	Lightweight Certificate Policy
NCP	Normalized Certificate Policy
NCP+	Extended Normalized Certificate Policy
OCSP	Online Certificate Status Protocol
OID	Object IDentifier
OVC	Organizational Validation Certificate
OVCP	Organizational Validation Certificate Policy
PDS PKI	Disclosure Statement
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PTC	Publicly-Trusted Certificate
RA	Registration Authority
SSL	Secure Socket Layer
TLS	Transport Layer Security
TLS/SSL	Transport Layer Security/Secure Socket Layer protocol

TSP	Trust Service Provider
UTC	Coordinated Universal Time
BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
GMT	Greenwich Mean Time
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSAPS	Time-Stamping Practice Statement
TSU	Time-Stamping Unit

3 Audit organization

eIDAS Full audit

This audit has been carried out from Monday 2019/06/17 to Friday 2019/06/21 by Mr Jean-Marc Pezeret – Lead Auditor, Mr. Maxence Kersten – Auditor. They have been accompanied on the TSP part by Mr. Lyndon Davies.

Audited Sites addresses and functions :

SITE	Address	Function
Ty Cynal	Watkiss way, Cardiff	CA
Stadium House	5 Park Street Cardiff, CF10 1NT	Main Data Center
DRC Belfast	Telephone House 45-75 May Street Belfast, BT1 4NB	Disaster Recovery Data Center

Total audit time in days: 7 days on-site and 10 days in total.

Explanation of the context of the audit :
This audit is a full eIDAS renewal audit after one year.
In order to be part of a STN network, Digicert requires BT to organize an ETSI audit on the scope of their activity (Certificate Service Provider).
The set of concerned STN CAs managed by BT are defined in paragraph 4.3 in the present report.

Evolution since the previous audit:
There was no change besides the closing of the deviations identified in the previous audit.

The following public documents of the TSP have been the subject-matter of the audit:

	Titre	CSP Scope	Version	Date
PDS	SERVICE POLICY DISCLOSURE STATEMENT BT Managed Public Key Infrastructure Security	Yes		
CP/CPS	DigiCert - Certificate Policy for Symantec Trust Network (STN)	Yes	2.9	11.09.2018

CP/CPS	BT Certification Practice Statement for DigiCert STN Certificates	Yes	3.8.11	25.02.2019
T&Cs	Not in the scope of this audit	Yes		

4 Fulfilment of the requirements

This assessment report reflects the fulfilment of the requirements laid down in the relevant standards:

ETSI EN 319 403-V2.2.2: *Electronic Signatures and infrastructures (ESI) - Trust Service Providers conformity assessment - Requirements for conformity assessment bodies assessing Trust Service Providers*

ETSI EN 319 401 V2.2.1*: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*

ETSI EN 319 411-1 V1.2.2: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*

And;

Certification scheme: **LSTI-Q065-V6.1**: Certification rules for Trust Service providers

And;

CABForum - Baseline Requirements, version 1.6.5

4.1 Specific requirements

Use of Trademark and Brand:
No abnormal uses of logos and trademarks were identified during the audit.

Management of Complaints and Appeals of the TSP:
Nothing to report

Information on any change of conformity that could affects the TSP certification:
Nothing to report

Information on remaining open non-conformities since the last audit:
There we no pending open deviations at the time of our audit.

4.2 Conclusion of the audit

Number of major deviations if any: 0
Number of minor deviations if any: 9

Deviation list

Information on elements to monitor during the next audit:
There is no specific point to monitor during the next audit.

Auditor's comments on the TSP level of compliance:
We recommend that the ETSI compliance can be delivered to BT PLC, if the correction plan is defined and provided.

4.3 Conformity assessment targets

The list of products used and its version accordingly (HSM and SSCD):
HSM Luna SA5 (cryptomodule firmware version 6.2.1)

Information on the TSP that uses a QSignCD and/or QCSealCD published in the European list eIDAS art. 31. *(Precise the publication date of the Trusted List and proof in annexe)*
N/A : Within the scope of the audit, no QSCD are delivered. The audit only concerns the management of CAs that deliver LCP certificates to natural persons.

Change in the QC Statements of Certificates (have they been notified to LSTI)
No change was made in QCStatements since last audit.

Conformity assessment target trust services and certificates:
The following table gives the list of all the CAs that were subject to analysis during the audit. Information is also given about the CA certificate that were not in production during the audit, but that were used for delivering end-user certificates that are still potentially valid.

CA		CA Name [Serial Number] and activation date	Validity	
		Certificate policy	ETSI policy	Service / EKU
VeriSign Class 2 Public Primary Certification Authority - G3			17.07.2036	Root
1	BT Class 2 CA - G3		16.12.2024	BT Root
	1	Anglo American CA [180A17ED270F7F1CFC6288853397AABE] until 22/08/18 Anglo American CA [1BF50814203FF52FF3C4B063BF9C8A18] from 22/08/18		CA
		2.16.840.1.113733.1.7.9.1		
		2.16.840.1.113733.1.7.23.2 (since 25/09/18)	LCP + STN	
	2	BT Secure Email CA G3 [79980E914604AD7EF8A3DC4BCEDABA36] until 23/05/18 BT Secure Email CA G3 [7C0D2D0E5327EC1ABA2C45B5D11B2C5C] since 23/05/18	16/12/2019 16/12/2024	CA

			2.16.840.1.113733.1.7.9.1 (wrong OID)		
			2.16.840.1.113733.1.7.23.2 (since 25/09/18)	LCP + STN	
	3	Government of Malta e-Mail Certificate Service CA G3 [4D1ECCA727D4E0E84BECDF476C7DB6BA] from 23/05/18 to 01/08/18 Government of Malta e-Mail Certificate Service CA G3 [30968A19DB9F9064FB2CEE65887FD29D] from 01/08/18 to 04/12/18 Government of Malta e-Mail Certificate Service CA G3 [688DF77165F18C7E66F7D481893FCC45] since 04/12/18			CA
			2.16.840.1.113733.1.7.9 (wrong OID)		
			2.16.840.1.113733.1.7.23.2 (since 25/09/18)	LCP + STN	
	4	HM Revenue and Customs G3 [5FCFBFDDA103D8E9468B62536894E131] HM Revenue and Customs G3 [2F543A29A824B9D64F29725584358FD7] since 25/05/18			CA
			2.16.840.1.113733.1.7.9 (wrong OID)		
			2.16.840.1.113733.1.7.23.2 (since 23/09/2018)	LCP + STN	
	5	Malta Transport Authority - Licensing and Testing Directorate G3 [6310C07319134336C168AAAB066B1681] until 23/05/18 Malta Transport Authority - Licensing and Testing Directorate G3 [6C247DC979E1A6408930DF495716E3C2] since 23/05/18			CA
			2.16.840.1.113733.1.7.9 (wrong OID)		
			2.16.840.1.113733.1.7.23.2 (since 25/09/18)	LCP + STN	
	6	TrustWise G3 [6FE46D83BA8D5C16985BE8D53F94D813] revoked on 21/02/2019 TrustWise G3 [4C:D1:CC:A7:D3:E2:F8:87:96:4E:BE:B9:3A:9C:58:16] since 23/03/2018			CA
			2.16.840.1.113733.1.7.9 (wrong OID)		
			2.16.840.1.113733.1.7.23.2 (since 25/09/18)	LCP + STN	
2	BT Class 2 CA - G2			13.06.2023	CA
	3 bis	Government of Malta e-Mail Certificate Service CA G3 [41CE9369BC3D3D24D3A774B6EF308BD8] until 23/05/18		13.08.2020	CA
			2.16.840.1.113733.1.7.9 (wrong OID) - no production at the time of the audit		

Conformity Assessment Report modifications records

Version	Issuing Date	Changes
Version 0.1	5 June 2019	Initial Report
Version 1	22 August 2019	Validated

Auditors findings are written in purple.

5 Risk Assessment

REQ-5-01: The TSP shall carry out a risk assessment to identify, analyze and evaluate trust service risks taking into account business and technical issues.

Compliant. Risk analysis has been shown during audit.

REQ-5-02: The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

Compliant. The risk treatment is consistent with the risk analysis.

REQ-5-03: The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).

The risk analysis includes the security requirements and operational procedures required to implement the risk treatment measures.

REQ-5-04: The risk assessment shall be regularly reviewed and revised.

The last review of the risk assessment took place at the Security Forum in February 2019.

REQ-5-05: The TSP's management shall approve the risk assessment and accept the residual risk identified.

Changes made to the risk analysis are approved by management via Sharepoint Workflow or email. Its includes risk assessment and residual risk acceptance.

6 Policies and practices

Introduction: BT-PLC is performing on the scope of a Certification Service Operator (CSO), delivering Managed PKI services towards TSPs. TSPs are customers to BT-PLC.
The scope of the present audit is limited to this SCO scope.
BT is delivering the services within the scope of this audit under the STN policy (Symantec Trust Network) policy. Digicert has now acquired Symantec, but the STN policy (version 2.9, 11 September 2018) still applies.

6.1 Trust Service Practice Statement

REQ-6.1-01: The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.

Compliant:
BT has an internal ISMS (Information Security Management System), referred as :
BT-PLC has published its own Certification Practice Statement, referring to the STN policy with OID:
2.16.840.1.113733.1.7.23.2

BT's CPS document can be downloaded from the repository site, managed by them :

https://www.trustwise.com/repository/CPS/cps.htm

NOTA : This CPS can serve as a basis to BT's customer, who may derive their own CP/CPS, provided it remains in line with the *mother* policy.

REQ-6.1-02: The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.

Compliant: Security Forum is in charge of approving the ISMS, the risk analysis and mitigation are also approved by this Security Forum.
CP/CPS is approved by the product line manager of Managed PKI services, also called PMA (Policy Management Authority) as stated in the CP/CPS in § 1.5

In particular:

REQ-6.1-03: The TSP shall have a statement of the practices and procedures used to address all the requirements identified for the applicable TSP's policy.

Compliant: This is materialized by the CP/CPS document [BT Certification Practice Statement for DigiCert STN Certificates]

REQ-6.1-04: The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.

Compliant: See è§ 1.3 of the CPS

REQ-6.1-05: The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the service policy.

Compliant: CP/CPS is available to relying parties from the BT-PLC repository site
https://www.trustwise.com/repository/CPS/cps.htm

REQ-6.1-06: The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.

Compliant: The Managed PKI service Product Line team manages the PKI service.

REQ-6.1-07: The TSP's management shall implement the practices.

See deviation n° 02 : CPS does not reflect practice regarding certificate renewal
See deviation n° 06 : CPS mentions a contact point that seems not to be operational

REQ-6.1-08: The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement.

Compliant: Cf. § 1.5.6 in CP/CPS

REQ-6.1-09: The TSP shall notify notice of changes it intends to make in its practice statement.

Compliant: the CP/CPS states in § 1.5.6 "*Amended versions or updates shall be linked to the Practices Updates and Notices section of the BT Repository*"

REQ-6.1-10: The TSP shall, following approval as in **REQ-6.1-06** above, make the revised TSP's practice statement immediately available as required under **REQ-6.1-05** above.

Compliant: See **REQ-6.1-09**

REQ-6.1-11: The TSP shall state in its practices the provisions made for termination of service (see clause 7.12).

Compliant: The practices are defined in § 5.8 for CA termination .
Full termination plan is in the hand of BT-PLC's customers, as their TSP responsibility.

6.2 Terms and Conditions

GENERAL NOTICE : BT PLC is not a TSP, but a Managed PKI Service Operator , or Certification Service Operation (CSO). With this respects, it does not sell service to end users and subscribers, but support the service sold by TSPs. No T&Cs concerning subjects or subscribers are in the scope of responsibility of BT.

REQ-6.2-01: TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.

Out of BT's responsibility

REQ-6.2-02: The terms and conditions shall at least specify for each trust service policy supported by the TSP the following:

N/A - see **REQ-6.2-01**
We consider only CPS as input to BT's customer's T&Cs

a) the trust service policy being applied;

Yes - LCP policy and Symantec Trusted Network policy is applied by BT

b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;

N/A

c) the subscriber's obligations, if any;

N/A

d) information for parties relying on the trust service;

N/A

e) the period of time during which TSP's event logs are retained;

BT commits to 10 years retention time and six month after certificate expiration

f) the applicable legal system;

This point is not addressed by the BT CPS, but in the contractual agreement between BT and its customers.

g) procedures for complaints and dispute settlement;

N/A

h) whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;

Page 3 of CPS, footnote, mentions annual tSCHEME compliance audit.
Nothing is said about eIDAS compliance nor ETSI.

i) the TSP's contact information; and

Yes : contact information is present in the CPS, but it is not effective at the time of the audit.
[Deviation 06] : A contact point is set in the CPS and the PDS at email "cps.mpki@bt.com : The Certificate Policy Manager"

A test mail was sent on the 18th.
No answer no reaction received at the end of the audit week

j) any undertaking regarding availability.

No specific information

REQ-6.2-03: Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

Out of BT's responsibility

REQ-6.2-04: Terms and conditions shall be made available through a durable means of communication.

Out of BT's responsibility

REQ-6.2-05: Terms and conditions shall be available in a readily understandable language.

Out of BT's responsibility

REQ-6.2-06: Terms and conditions may be transmitted electronically.

Out of BT's responsibility

6.3 Information security policy

REQ-6.3-01: The TSP shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.

The document "Information Security Management System (ISMS)" acts as the information security policy, which is the main document of the BT ISMS. This document has been approved by management during the last security forum on the 12th of febuary 2019.

REQ-6.3-02: Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

This document is not published to third parties of BT Trustwise, but it is communicated to the BT representative of PKI customers. It is communicated on request.

In particular:

REQ-6.3-03: A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.

The document “Managed Trust Services ISMS_27001_2013 spreadsheet” references all applicable security policies.

REQ-6.3-04: The TSP shall publish and communicate the information security policy to all employees who are impacted by it.

Compliant. The ISMS policy and all policies are published in the BT’s internal SharePoint.
BT also has a specific portal that includes all security policies.

REQ-6.3-05: The TSP shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP's

functionality is undertaken by outsourcers.

BT retains overall responsibility and has no subcontractors for their TSP activities.

REQ-6.3-06: TSP shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the TSP.

No outsourcers in the TSP scope.

REQ-6.3-07: The TSP's information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

Compliant. These documents are reviewed at least once a year or when a significant change occurs.

REQ-6.3-08: Any changes that will impact on the level of security provided shall be approved by the management body referred to in **REQ-6.1-07**.

Compliant. These changes are approved by email.

REQ-6.3-09: The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.

Compliant. Depending on systems, internal software are used to control changes.

REQ-6.3-10: The maximum interval between two checks shall be documented in the trust service practice statement.

Compliant. See “BT Certification Practice Statement for DigiCert STN Certificate” section §8.1.

7 TSP management and operation

7.1 Internal organization

7.1.1 Organization reliability

REQ-7.1.1-01: The TSP organization shall be reliable.

Compliant. BT is a large international group with a high reputation in the field of technology.

In particular:

REQ-7.1.1-02: Trust service practices under which the TSP operates shall be non-discriminatory.

No discriminatory practices were found in BT's processes and services.

REQ-7.1.1-03: The TSP should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP's terms and conditions.

Compliant: BT provides services to all TSP companies wishing to outsource the technical management of PKI.

REQ-7.1.1-04: The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.

Compliant. BT Technology is a division within British Telecom and has sufficient financial resources to cover their PKI activities.

REQ-7.1.1-05: The TSP shall have the financial stability and resources required to operate in conformity with this policy.

See REQ-7.1.1-01.

REQ-7.1.1-06: The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

See REQ-6.2-02.

REQ-7.1.1-07: The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

Compliant: There is a contract signed between BT and each of its TSP customers.

7.1.1 Segregation of duties

REQ-7.1.2-01: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets.

Compliant. A strict segregation of duties' policy is applied in order to avoid unauthorized modification of BT's assets.

7.2 Human resources

REQ-7.2-01: The TSP shall ensure that employees and contractors support the trustworthiness of the TSP's operations.

Compliant: All skills and human resources are available in the "BT Security Software Services" document, especially for PKI requirements and related operations.

In particular:

REQ-7.2-02: The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.

Compliant. BT employment of qualified staff for their position.

REQ-7.2-03: TSP's personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.

BT Training platform is called "Learning Home": common BT e-learning.
Specific learning courses are also available in this platform.

REQ-7.2-04: This should include regular (at least every 12 months) updates on

new threats and current security practices.

New online courses are regularly sent to employees.

REQ-7.2-05: Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures.

Compliant: Appropriate disciplinary measures are fully applied in the “Job Description” (last sentence at the end of the document).

REQ-7.2-06: Security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.

Compliant, the document “roles and responsibilities” describes the roles.

REQ-7.2-07: Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified.

Compliant, see REQ-7.2-06. Employees with a critical role in BT’s operations are clearly identified.

REQ-7.2-08: Trusted roles shall be named by the management.

Compliant. The document is validated by the management.

REQ-7.2-09: Trusted roles shall be accepted by the management and the person to fulfil the role.

Trusted roles are clearly identified and named by management.

REQ-7.2-10: TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

See REQ-7.2-07.

REQ-7.2-11: Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.

It is not relevant to differentiate between “general” functions and TSP’s specific functions.

REQ-7.2-12: Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.

Compliant. All procedures are available to all employees and are used.

REQ-7.2-13: Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

Compliant. BT PKI’s managers have experience within BT.

REQ-7.2-14: All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.

Compliant. During the audit, no conflict of interest has been detected.

REQ-7.2-15: Trusted roles shall include roles that involve the following responsibilities:

a) Security Officers: Overall responsibility for administering the implementation of the security practices.

The Security Manager stands for the Security Officer role.

b) System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.

ASG (Application Support Group) is the name for the System Administrators team.

c) System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.

Included in the ASG team.

d) System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.

Included in the ASG team.

REQ-7.2-16: TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security requiring the principle of "least privilege" when accessing or when configuring access privileges.

Compliant, see REQ-7.2-08.

REQ-7.2-17: Personnel shall not have access to the trusted functions until the necessary checks are completed.

Compliant. Personnel do not have access to the application / systems until checks are completed.

7.3 Asset management

7.1.2 General requirements

REQ-7.3.1-01: The TSP shall ensure an appropriate level of protection of its assets including information assets.

Salsa Trustwise web application is used to have an application view (with responsible, support, ...), and Suportal web application is used to have a server view.

In particular:

REQ-7.3.1-02: The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment.

All IT systems are managed in Suportal web application.

7.1.3 Media handling

REQ-7.3.2-01: All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required.

Compliant: BT handle media securely; database assets are in a saferoom. The procedure “Doc Ref: LP21” details the process for the secure destruction of hard disk drives or other storage devices such as Hardware Security Modules (HSMs).

7.4 Access control

REQ-7.4-01: The TSP's system access shall be limited to authorized individuals.

[DC Belfast] Compliant. The document “Physical access register” gathers all physical access to the saferoom. BT application “BASOL” is used to manage authorizations.
[Stadium House] Same as for the Belfast DC, the access to the PKI server room is limited to authorized individuals.

In particular:

REQ-7.4-02: Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.

[Stadium House] Multiple firewalls are in place in order to protect backend servers from unauthorized access.

REQ-7.4-03: Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.

[Stadium House] Compliant. Firewall are configured to limit access to only authorized protocols and access.

REQ-7.4-04: The TSP shall administer user access of operators, administrators and system auditors.

Compliant. All systems and applications access are managed through VINTELA application, which is an in-house developed software.

REQ-7.4-05: The administration shall include user account management and timely modification or removal of access.

Itrust application (also in-house software) keeps all VINTELA traces of modification and removal of access with timestamp.

REQ-7.4-06: Access to information and application system functions shall be restricted in accordance with the access control policy.

Compliant. VINTELA manages all access to the application system, and all access to information is restricted via the SharePoint application.

REQ-7.4-07: The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.

Compliant. The separation of duties is described in the document "roles and responsibilities" .

REQ-7.4-08: TSP's personnel shall be identified and authenticated before using critical applications related to the service.

Compliant. All employees accessing applications or PKI systems are identified and authenticated by strong authentication (i.e. two-factor authentication).

REQ-7.4-09: TSP's personnel shall be accountable for their activities.

Compliant. All TSP personnel using TSP systems are authenticated to be accountable.

REQ-7.4-10: Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

See report ETSI EN 319 411-1 OVR-6.8.4-02.

7.5 Cryptographic controls

REQ-7.5-01: Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

7.6 Physical and environmental security

REQ-7.6-01: The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security.

[DC Belfast] Compliant: physical access to BT PKI operations system are protected.
[Stadium House] Compliant. Access to desk where administrators and operators' computers are is restricted.

In particular:

REQ-7.6-02: Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals.

[DC Belfast] Compliant, access to the safe / secure rooms is restricted to authorized employees.
[Stadium House] Compliant, see REQ-7.6-01.

REQ-7.6-03: Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.

[DC Belfast] Compliant, physical controls are implemented to avoid compromise of assets.
[Stadium House] Only employees can access to the critical assets, and all visitors are accompanied.

REQ-7.6-04: Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

[DC Belfast] Compliant, physical controls are implemented.
[Stadium House] Compliant, see REQ-7.6-03.

REQ-7.6-05: Components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

[DC Belfast] All assets included in TSP's operations scope are located in a saferoom.
[Stadium House] Apart from the administrator and operator computers, there are no critical components for the security of operations.

7.7 Operation security

REQ-7.7-01: The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

[Stadium House] Compliant. Generally, BT has a performant IT team and a secured IT environment.

In particular:

REQ-7.7-02: An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.

[Stadium House] Compliant. Security analysis is a common practice in PKI activities at BT.

REQ-7.7-03: Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.

[Stadium House] Compliant: BT has a written procedure “LP28 Change Management Policy” as well as a “LP22 Patching Policy”.
BT Security Team monitors vendors security patches and builds quarterly bundles to be deployed, including OS fixes and dependencies fixes. Those bundles are first tested by the security team, then they are made available to the whole BT system, installed and tested on a development and test PKI environment before being deployed on live system.
Every change and deployment are planned, scheduled and recorded in “HP service manager” and an Excel file.

REQ-7.7-04: The procedures shall include documentation of the changes.

[Stadium House] Compliant. See REQ-7.7-03.

REQ-7.7-05: The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.

[Stadium House] Compliant: BT uses different security systems such as IDS and firewalls. Antivirus software is used on workstations and is up-to-date.

REQ-7.7-06: Media used within the TSP's systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.

[Stadium House] Every USB keys is bit locked before being used on a computer.

REQ-7.7-07: Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

[Stadium House] Compliant: BT has a written procedure “LP21 Secure Media Destruction Process” for media destruction.

REQ-7.7-08: Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

[Stadium House] Compliant: Procedures for trusted and administrative roles are written in “LP05 Team

Management" document.

REQ-7.7-09: The TSP shall specify and apply procedures for ensuring that:

a) security patches are applied within a reasonable time after they come available;

[Stadium House] Compliant: BT's "LP22 Patching Policy" states security patches are deployed as soon as possible. Security patches are applied at least every quarter on the PKI infrastructure; every change is logged in the HP Services Change application. Workstation patches are applied as soon as possible.

b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and

[Stadium House] As of today, security patches are always applied and installed.

c) the reasons for not applying any security patches are documented.

[Stadium House] see b).

7.8 Network security

REQ-7.8-01: The TSP shall protect its network and systems from attack.

[Stadium House] Compliant. BT's network team is responsible to the network security, and to its monitoring in order to avoid attacks.

In particular:

REQ-7.8-02: The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.

[Stadium House] Compliant. PKI environment is segmented into networks area: frontend, backend, and signing servers / HSM are in separated environment (physical and / or logical).

REQ-7.8-03: The TSP shall apply the same security controls to all systems co-located in the same zone.

[Stadium House] Compliant. Security controls are applied on all servers inside the critical area (backend, with signing servers and HSM).

REQ-7.8-04: The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.

[Stadium House] Compliant. Firewall rules are compliant with the good practices and restrict protocols and accesses to those necessary.

REQ-7.8-05: The TSP shall explicitly forbid or deactivate not needed connections and services.

[Stadium House] Compliant. Firewall rules explicitly forbid not needed connections.

REQ-7.8-06: The TSP shall review the established rule set on a regular basis.

[Stadium House] Firewall rules are reviewed every 6 months. Export of firewall configurations are checked against internal rules management system (Moscow) and spreadsheets maintained by security manager. The process is described in the document "LP30 - Firewall Rules Check Process".

REQ-7.8-07: The TSP shall keep all systems that are critical to the TSP's operation

in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.9]).

[DC Belfast, DC Cardiff] Compliant. In both DC, PKI activities (servers and HSM) are in high security zone, with restricted access).

REQ-7.8-08: The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.

[Stadium House] BT network is well segmented; TSP servers as signing servers and HSM are separated from other systems.

REQ-7.8-09: The TSP shall not use systems used for administration of the security policy implementation for other purposes.

[Stadium House] Compliant. BT servers have dedicated purposes.

REQ-7.8-10: The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems).

[Stadium House] BT uses three different platforms for TSP's services: testing, pre-production and production platforms. The testing platform is on a dedicated network; both pre-production and production platforms are in the same network.

REQ-7.8-11: The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

[Stadium House] Compliant. Communication between Belfast DC backend and Cardiff DC backend is done through an IPSEC VPN site-to-site.

REQ-7.8-12: If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.

[Stadium House] Compliant. All PKI services are redundant in the principal DC (Cardiff). There is no redundancy in the backup DC (Belfast).

REQ-7.8-13: The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

[Stadium House] Regular scans are performed on BT servers by the BT security teams. If a critical vulnerability is detected, a request for emergency fix is transmitted to the Trustwise services team.

REQ-7.8-14: The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.

[Stadium House] Compliant: last third-party penetration test has been performed on October 2018.

REQ-7.8-15: The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

[Stadium House] Compliant, see REQ-7.8-14.

7.9 Incident management

ClarifyCRM software is used to manage incidents (production and security incidents). Clarify sends mail notification, and a phone call notification in the event of a priority incident.

REQ-7.9-01: System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored.

Compliant. All IT systems and service requests are monitored through Nagios application. The Nagios logs are monitored, and an incident ticket is opened in case of error.

In particular:

REQ-7.9-02: Monitoring activities should take account of the sensitivity of any information collected or analyzed.

A dedicated application sends an alarm to trusted roles especially via email.

REQ-7.9-03: Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.

IDS equipment are deployed in the front network area in order to detect such violation.

REQ-7.9-04: The TSP shall monitor the following events:

a) start-up and shutdown of the logging functions; and

All system logs are sent to the SPLUNK server.

b) availability and utilization of needed services with the TSP's network.

Compliant. Nagios monitor specifics Webservices and others needed services.

REQ-7.9-05: The TSP shall act in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.

Compliant. The procedure LP01 “Incident Management” describes a process that respond to this requirement.

REQ-7.9-06: The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

Compliant: BT PKI team manages a monthly detailed report “Managed PKI Operations Report_year_month” that fully specifies all the categorized incidents.

REQ-7.9-07: The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

Compliant. The incident management procedure indicates that the BT customers shall be notified in a such case.

REQ-7.9-08: Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

According to the STN policy, BT will notify the natural person of any breach of security.

REQ-7.9-09: The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.

Audit logs are not reviewed and the consistency of the logs is not checked.

REQ-7.9-10: The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.

Compliant. Any vulnerability is detected by BT security team through an internal tool.

REQ-7.9-11: For any vulnerability, given the potential impact, the TSP shall [CHOICE]:

Compliant. The tool used by BT gives the potential impact and the link to the CVE.

- create and implement a plan to mitigate the vulnerability; or

Vulnerability are reviewed during the monthly operation reports.

- document the factual basis for the TSP's determination that the vulnerability does not require remediation.

The vulnerability remediation is logged in the ticketing application.

REQ-7.9-12: Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

Compliant. The procedures exist and are used.

7.10 Collection of evidence

REQ-7.10-01: The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

Compliant. SPLUNK is managed by BT teams and keep all systems logs. Applications logs are in a database.

In particular:

REQ-7.10-02: The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.

Compliant for SPLUNK.

REQ-7.10-03: Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.

[Deviation 08] see ETSI EN 319 411-1 OVR-6.8.4-02.

REQ-7.10-04: Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

Compliant. PKI Symantec operations logs are available and includes all PKI operations.

REQ-7.10-05: The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.

All systems events are sent to the BT SPLUNK appliance.

REQ-7.10-06: The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.

PKI servers are synchronized to NTP servers every 17 minutes.

REQ-7.10-07: Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.3).

N/A. BT is not responsible to provide legal evidence.

REQ-7.10-08: The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

Logs are held in the Oracle database server.

7.11 Business continuity management

REQ-7.11-01: The TSP shall define and maintain a continuity plan to enact in case of a disaster.

Compliant. The document "LP02 Business Continuity" explains how BT will continue TSP operations in case of a disaster on its primary DC (Cardiff).

REQ-7.11-02: In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

BT has the sufficient infrastructure in place to restore all critical operations (i.e. certificate status information, certificate revocation and certificate issuance) in 2 hours.

7.12 TSP termination and termination plans

NOTA: This section is not in the scope of the audit.
The termination plans are under the responsibility of each BT's customers, as their TSP role.
BT has the technical capability to support termination plan requirements within the scope of a Managed PKI service provider…

7.13 Compliance

REQ-7.13-01: The TSP shall ensure that it operates in a legal and trustworthy manner.

Compliant. BT operates all its activities in a legal and trustworthy manner.

In particular:

REQ-7.13-02: The TSP shall provide evidence on how it meets the applicable legal requirements.

BT Technology reports to the BT Global Services, which is responsible in particular for the legality of BT's activities.

REQ-7.13-03: Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.

Services provided by BT are not for end users uses; this is the TSP (i.e. BT's customers) responsibility.

REQ-7.13-04: Applicable standards on accessibility such as ETSI EN 301 549 [i.10] should be taken into account.

See REQ-7.13-03.

REQ-7.13-05: Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

See §7.7.

End of the Conformity Assessment Report – ETSI EN 319 401

ETSI EN 319 411-1 V1.2.2 (2018-04)

Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

Auditors findings are written in purple.

5 General provisions on Certification Practice Statement and Certificate Policies

5.1 General requirements

OVR-5.1-01 [NCP+, EVCP]: all requirements specified for [NCP] shall apply.

N/A : Only LCP certificates in the scope

OVR-5.1-02 [DVCP, IVCP, OVCP]: all requirements specified for [LCP] shall apply.

N/A : Only LCP certificates in the scope

5.2 Certification Practice Statement requirements

OVR-5.2-01: The general requirements specified in ETSI EN 319 401, clause 6.1 shall apply.

Refer to report EN 319 401 section 6.1 - Compliant

OVR-5.2-02: The TSP's CPS should be structured in accordance with IETF RFC 3647 [i.3].

Compliant: The CP/CPS is aligned with the recommended structure..

OVR-5.2-03: The TSP's CPS shall include the complete CA hierarchy, including root and subordinate CA's.

Compliant: Cf. §1.1 in CPS

OVR-5.2-04: The TSP's CPS shall include the signature algorithms and parameters employed.

Compliant: Section 6.1 in CPS

OVR-5.2-05: The TSP shall publicly disclose its CPS through an online means that is available on a 24x7 basis.

The publication of CP/CPS towards end users is not in the scope of the CSO.
Still the BT PLC CP is published on a 24/7 resilient web page : 2 servers running in parallel in Cardiff (load balanced) and an synchronized instance in Belfast that could take over the CRL publication in case of disaster.

OVR-5.2-06 [PTC]: The requirement preceding clause 2.1 in clause 2 of the BRG [5] shall apply.

N/A

OVR-5.2-07 [PTC]: Clause 2.2 of BRG shall apply.

N/A

OVR-5.2-08 [EVCP]: Clause 8.3 of EVCG shall apply.

N/A

OVR-5.2-09 [EVCP]: Clause 8.2.1 of EVCG shall apply.

N/A

OVR-5.2-10: The TSP's CPS shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP.

Section 7 of the CPS gives details about certificate and CRL profiles ; It refers to signature in line with RFC but does not give details about practice for the concerned CAs - From the CPS, we don't know who is signing what, with what algorithm and what parameters.

5.3 Certificate Policy name and identification

OVR-5.3-01: If any changes are made to a CP as described in clause 4.2.5 which affects the applicability then the policy identifier should be changed.

BT is propagating the STN policy, with the STN OID.
The OID change is on the shoulders of Digicert.

5.4 PKI participants

5.4.1 Certification Authority

OVR-5.4.1-01: The TSP may make use of other parties to provide parts of the certification service.

BT-PLC relies on Digicert (Symantec) for the generation of customer's CAs

OVR-5.4.1-02: A TSP may include a hierarchy of CAs.

Yes - BT includes the STN hierarchy.

OVR-5.4.1-03 [CONDITIONAL]: Where a TSP includes a hierarchy of subordinate CAs up to a root CA, the TSP shall be responsible for ensuring the subordinate-CAs comply with the applicable policy requirements.

Compliant: BT propagates to the generated CAs, and the end user certificates, the STN policy.
The current audit checks the compliance of BT PLC practice with the "mother" STN policy document [DigiCert - Certificate Policy for Symantec Trust Network (STN) v2.9]
.

5.4.2 Subscriber and subject

5.4.3 Others

OVR-5.4.3-01: Other participants, not covered by the present document, may be identified by the TSP.

No other participants.

5.5 Certificate usage

6 Trust Service Providers practice

6.1 Publication and repository responsibilities

General Note BT-PLC, in its CSO role (Certification Service Operation), is supporting its customers for their publication obligations, but has no direct obligation such as TSP.
BT-PLC publishes on a resilient repository page all the CRLs related to the CAs it manages.
BT-PLC, as a client of STN network, also publishes the STN policy, and its own Certification Practice Statement on the following public URL : https://www.trustwise.com

DIS-6.1-01: The TSP shall make certificates available to subscribers, subjects and relying parties.

BT-PLC SA makes certificates available to subscribers

DIS-6.1-02: Upon generation, the complete and accurate certificate shall be available to the subscriber or subject for whom the certificate is being issued.

Compliant: Dissemination of the certificate is performed through sending a download link to the subject from where he can pick his public certificate in PKCS#7 format.

DIS-6.1-03: Certificates shall be available for retrieval in only those cases for which the subject's consent has been obtained. If the subject is a device or system, the consent of the natural or legal person responsible for the operating of the device or system needs to be obtained, instead of the subject.

Not under BT's responsibility.

DIS-6.1-04: The TSP shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 6.9.4).

Not under BT's responsibility.

DIS-6.1-05: The applicable terms and conditions shall be readily identifiable for a given certificate.

Not under BT's responsibility.

DIS-6.1-06 [LCP]: The information identified in **DIS-6.1-03** and **DIS-6.1-04** above shall be available as specified in the TSP's CPS.

N/A

DIS-6.1-07 [NCP]: The information identified in **DIS-6.1-03** and **DIS-6.1-04** above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.

N/A

DIS-6.1-08: The information identified in **DIS-6.1-04** above should be publicly and internationally available.

N/A

DIS-6.1-09 [CONDITIONAL]: If the TSP is issuing publicly-trusted certificates, the information identified in **DIS-6.1-04** above shall be publicly and internationally available.

N/A

6.2 Identification and authentication

6.2.1 Naming

6.2.2 Initial identity validation

REG-6.2.2-01: The TSP shall verify the identity of the subscriber and subject, and shall check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

Registration Authority tasks are not under the responsibility of BT.

6.2.3 Identification and authentication for Re-key requests

REG-6.2.3-01: Requests for certificates issued to a subject who has previously been registered with the same TSP shall be complete, accurate and authorized. This includes re-key following revocation or prior to expiration, or update due to change to the subject's attributes.

Compliant: See § 4.7.3 in BT' CPS describing the re-key process. The process is involving both the RA (the registration authority on BT's customer side and BT itself).

In particular:

- **REG-6.2.3-02:** The TSP shall check the existence and validity of the certificate to be rekeyed and that the information used to verify the identity and attributes of the subject are still valid.

See REG-6.2.3-01

- **REG-6.2.3-03** [EVCP]: Clauses 11.14.2 and 11.14.3 of EVCG [4] shall apply.

N/A

- **REG-6.2.3-04** [EVCP]: Clause 9.4 of EVCG [4], specifying the maximum validity period, shall apply.

N/A

- **REG-6.2.3-05** [OVCP], [IVCP] and [DVCP]: Clause 3.3.1 of BRG [5] shall apply.

N/A

- **REG-6.2.3-06** [OVCP], [IVCP] and [DVCP]: Validation information obtained by the TSP may be reused if compatible with clause 4.2.1 of BRG [5].

N/A

- **REG-6.2.3-07** [OVCP], [IVCP] and [DVCP]: Clause 6.3.2 of BRG [5], specifying the maximum validity period, shall apply.

N/A

- **REG-6.2.3-08:** If any of the TSP's terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with requirements **REG-6.3.4-02**, **REG-6.3.4-03, OVR-6.3.4-04** to **OVR-6.3.4-06, REG-6.3.4-07** and **REG-6.3.4-08**.

Out of scope

- **REG-6.2.3-09:** Requirements of clause 6.2.2 shall apply.

Refer to 6.2.2

6.2.4 Identification and authentication for revocation requests

REV-6.2.4-01: The TSP shall document as part of its CPS (see clause 5.2) the procedures for revocation of end user and CA certificates including:

Compliant: Section 4.9 in the BT CPS describes the revocation process and covers points a) to g) mentioned below

a) Who can submit requests for revocation or reports of events which may indicate the need to revoke a certificate.

Compliant: Described in CP §4.9.2

b) How they can be submitted.

Compliant: Described in CP §4.9.3

c) Any requirements for subsequent confirmation of requests for revocation or reports of events which may indicate the need to revoke a certificate.

Subsequent confirmation will depend on each TSP's process. Not in the scope of BT

d) Whether and for what reasons certificates can be suspended or revoked.

Compliant: Described in CP §4.9.1

e) The mechanism used for distributing revocation status information.

Compliant: See § 4.9.10 in the CP/CPS

f) The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties.

[Deviation 05] : The CPS states in § 4.9.5 "*BT takes commercially reasonable steps to process revocation requests without delay*" which cannot be considered as a specification of a maximum delay.

g) The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties.

See deviation n°5 above - No explicit commitment with maximum delay is mentioned

REV-6.2.4-02 [PTC]: Clause 4.9 of the BRG [5] shall apply.

N/A

REV-6.2.4-03: The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties shall be at most 24 hours.

This is not documented in the CPS - See deviation n° 5.

REV-6.2.4-04: The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties shall be at most 60 minutes.

[Deviation 07] : The status of the certificate is modified in the PKI database as soon as the revocation has been processed (almost immediately). But the CRL will only reflect this new status on the publication date that could (worst case) be 12 hours later.

REV-6.2.4-05 [CONDITIONAL]: If the revocation request requires revocation at a future date (e.g. subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the confirmation time in **REV-6.2.4-04** according to the TSP's policies.

N/A

REV-6.2.4-06: A TSP may give faster process times then the time required in **REV-6.2.4-03** and **REV-6.2.4-04** for certain revocation reasons.

There is no formalized feature about this requirement.

REV-6.2.4-07: The time used for the provision of revocation services shall be synchronized with UTC at least once every 24 hours.

Compliant: NTP synchronization is performed every 1024 seconds.

REV-6.2.4-08: Requests for revocation and reports of events relating to revocation shall be processed on receipt.

Compliant**:** The revocation is processed as soon as it has been validated by the requester , through authentication by his secret passphrase.

REV-6.2.4-09: Requests for revocation and reports of events relating to revocation shall be authenticated, checked to be from an authorized source.

Compliant: Request for revocation can be performed by end users directly from the front-end application portal provided by DIGICERT (revoke button). They are authenticated thanks to their passphrase that they set up during registration.

6.3 Certificate Life-Cycle operational requirements

6.3.1 Certificate application

REG-6.3.1-01 [CONDITIONAL]: If the subject's key pair is not generated by the CA, the certificate request process shall check that the subject has possession or control of the private key associated with the public key presented for certification.

For all the CAs in the scope of the audit, the key-pair is generated by the subject, from his browser. The request for certificate is send as a PKCS#7 file, signed with the secret key of the subject, thus proving the possession of the key.

REG-6.3.1-02 [EVCP]: For a dual control procedure in the validation process EVCG [4], clause 14.1.3, shall apply.

N/A

6.3.2 Certificate application processing

REG-6.3.2-01: Application for certificates shall be from a trusted registration service.

Application for certificate is performed by the subject on the end-user interface, but validation of the request is done by the RA through an authenticated admin account. The application is then handled and processed by the system operated by BT.

In particular:

- **REG-6.3.2-02** [CONDITIONAL]: When external registration service providers are used registration data shall be exchanged securely and only with recognized registration service providers, whose identity is authenticated.

RA organization is not in the scope of BT's responsibility.
BT defines for his customer admin accounts to allow validation of certificate requests, based on all the criteria that the customer has defined.
Certificate based authentication, from a private BT managed CA (BT cluster enterprise CA)

6.3.3 Certificate issuance

See clause 6.6.1 for certificate profiles.

GEN-6.3.3-01: The CA shall issue certificates securely to maintain their authenticity.

Compliant: Certificates are issued and signed by the CA. A link for retrieval of the certificate is sent to the end-user, who has generated his key-pair.

In particular:

- **GEN-6.3.3-02:** The CA shall take measures against forgery of certificates.

Compliant: The generation of certificate is performed in the high security BT data center, where the online HSM stands and the application servers are. Signature by the CA on the HSM prevents from forgery.

- **GEN-6.3.3-03** [CONDITONAL]: In cases where the CA generates the subjects' key pair, the CA shall guarantee confidentiality during the process of generating such data.

N/A: The subject generates the key-pair

- **GEN-6.3.3-04:** The procedure of issuing the certificate shall be securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject-generated public key.

Compliant: The process is automatized from request, PCKS#7 file generation, validation by the RA, and generation of the certificate. The certificate is downloadable for the customer through a temporary link that he receives on his email address.
For secure email CA, the approbation for issuing the certificate is automatic : certificate request is over-signed by a certificate issued by a BT CA. A Symantec application is deployed in the customer IT systems on a Windows Server: it checks the users rights to get a certificate in the Active Directory.

- **GEN-6.3.3-05:** The TSP should not issue certificates whose lifetime exceeds that of the CA's signing certificate.

Compliant: The STN software suite will not allow certificates beyond the lifetime of the CA.

- **GEN-6.3.3-06** [CONDITIONAL]: If the TSP does issue certificates whose lifetime exceeds the lifetime of the CA's signing certificate, the TSP shall ensure that the

certificate status (see clause 6.3.10) can still be verified by relying parties after expiry of the CA certificate.

N/A.

When the CA generated the subject's key pair:

- **GEN-6.3.3-07** [CONDITIONAL]: If the CA generated the subject's key pair, the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA;

N/A

- **SDP-6.3.3-08** [LCP] and [NCP] [CONDITIONAL]: If the CA generated the subject's key pair, the private key shall be securely passed to the registered subject; or to the TSP managing the subject's private key; and

N/A

- **SDP 6.3.3-09** [NCP+][CONDITIONAL]: If the CA generated the subject's key pair, the secure cryptographic device containing the subject's private key shall be securely delivered to the registered subject or, in the case of the TSP managing the key on behalf of the subject, the TSP shall ensure that the subject has sole control (or if the subject is a legal person "control") over its signing key.

N/A

GEN-6.3.3-10: Re-assignment of distinguish name [CHOICE]:

- [All policies except DVCP]: Over the life time of the CA a subject distinguished name which has been used in a certificate shall never be re-assigned to another subject.

Not in the scope of the CSO: The naming responsibility and unicity of it is on the TSP's Registration Authority responsibility. BT PLC just builds the certificate with the required DB. The system prevents to have wo certificates with the same DN under the same CA at the same time (except overlap allowed in case of re-key). From the certificate samples we had, we can see that the risk to have homonyms over time is not null

- [DVCP] Over the life time of the CA a subject distinguished name which has been used in a certificate shall never be re-assigned to another subject unless the subscriber has provided evidence of rightful ownership of the name.

N/A

GEN-6.3.3-11 [CONDITIONAL]: If a certificate is issued to a natural person identified in association with the legal person, then the subject attributes identifying the organization in the certificate should represent the legal person or sub- entity of that legal person and the subject identifier in the certificate shall be the natural person.

RA responsibility, not in the scope of BT
Samples certificate we had are compliant with this requirement.

GEN-6.3.3-12: The CP identifier shall be [CHOICE]:

- [NCP]:
  - as specified in clause 5.3 item a); and/or
  - an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

N/A

- [NCP+]:
  - as specified in clause 5.3 item b); and/or
  - an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

N/A.

- [LCP]:
  - as specified in clause 5.3 item c); and/or
  - an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

BT uses the STN policy OID for class 2 certificates:

- [EVCP]:
  - as specified in clause 5.3, item d);
  - as specified in EVCG [4], clause 9.3.2; and/or
  - an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

N/A

- [DVCP]:
  - as specified in clause 5.3, item e);
  - as specified in BRG [5], clause 1.2 or 7.1.6.1; and/or
  - an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

N/A

- [OVCP]:
  - as specified in clause 5.3 item f);
  - as specified in BRG [5], clause 1.2 or 7.1.6.1; and/or
  - an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

N/A

- [IVCP]:
  - as specified in clause 5.3 item g);
  - as specified in BRG [5], clause 1.2 or 7.1.6.1; and/or

- an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

N/A

6.3.4 Certificate acceptance

OVR-6.3.4-01: The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate. See clause 6.9.4.

T&Cs towards subject and subscribers is not under BT's responsibility.

In particular:

- **REG-6.3.4-02:** Before entering into a contractual relationship with a subscriber, the TSP shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 6.9.4.

T&Cs towards subject and subscribers is not under BT's responsibility.
Still, a template T&Cs is proposed by BT within the registration interface.

- **REG-6.3.4-03** [CONDITIONAL]: If the subject is a person (i.e. not a device), and not the same as the subscriber, the subject shall be informed of his/her obligations.

T&Cs towards subject and subscribers is not under BT's responsibility.

Communication of the terms and conditions:

- **OVR-6.3.4-04:** The TSP shall communicate the terms and conditions through a durable (i.e. with integrity over time) means of communication, and in a human readable form before the agreement.

T&Cs towards subject and subscribers is not under BT's responsibility.

- **OVR-6.3.4-05:** The terms and conditions may be transmitted electronically.

T&Cs towards subject and subscribers is not under BT's responsibility.
The T&Cs are communicated to the

- **OVR-6.3.4-06:** The terms and conditions may use the model PKI disclosure statement given in annex A.

T&Cs towards subject and subscribers is not under BT's responsibility.

- **REG-6.3.4-07:** The TSP shall record the agreement with the subscriber and if the subscriber and subject are two separate entities and the subject is a natural or legal person, with the subject.

T&Cs towards subject and subscribers is not under BT's responsibility.
BT records the various steps of certificate application.
The enrollment step includes the visualization of the generic T&Cs. See figure 1 below.

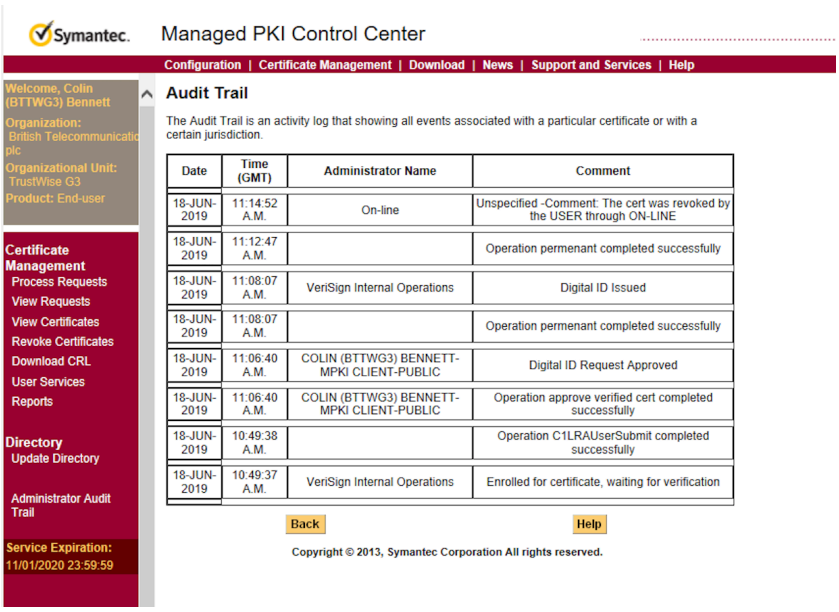


Fig. 1 - Log view of enrolment

- **REG-6.3.4-08:** The agreement in requirement **REG-6.3.4-07** shall involve explicit acceptance of the terms and conditions by a wilful act which can be later supported by evidence.

The acceptance is recorded as part of the overall registration records.

Where the subscriber and subject are two separate entities and the subject is a natural or legal person:

- **REG-6.3.4-09** [CONDITIONAL]: If the subscriber and subject are two separate entities and the subject is a natural or legal person, the agreement shall be in 2 parts.

T&Cs towards subject and subscribers is not under BT's responsibility.
[Deviation 09] The by default T&Cs provided by BT does not split in 2 parts. Moreover, it was not clear during the audit weather the T&Cs is systematically re-adapted by the TSP or not.
T&Cs should be a contract between the subjects/subscriber and the Certificate Authority (the legal entity delivering the certificates) and BT.

- **REG-6.3.4-10** [CONDITIONAL]: If the subscriber and subject are two separate entities and the subject is a natural or legal person, the first part of the agreement shall be ratified by the subscriber and shall include:

  a) agreement to the subscriber's obligations (see clause 6.9.4);

  b) if the TSP's practices require use of a secure cryptographic device, agreement by the subscriber to use a secure cryptographic device;

  c) consent to the keeping of a record by the TSP of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clauses 6.4.5 and 6.4.6), the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services;

d) whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate;

e) confirmation that the information to be held in the certificate is correct;

f) obligations applicable to subjects (see clause 6.9.4).

Registration: not in the scope of the CSO

- **REG-6.3.4-11** [CONDITIONAL]: Where the subscriber and subject are two separate entities and the subject is a natural or legal person, the second part of the agreement shall be ratified by the subject and shall include:

a) the agreement by the subject on the obligations applicable to subjects (see clause 6.9.4);

b) if the TSP's practices require use of a secure cryptographic device, agreement by the subject to use a secure cryptographic device;

c) consent to the keeping of a record by the TSP of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation (see clauses 6.4.5 and 6.4.6), the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the TSP terminating its services.

Registration: not in the scope of the CSO

Where the subject and subscriber are the same entity or the subject is a device:

- **REG-6.3.4-12** [CONDITIONAL]: If the subject and subscriber are the same entity or the subject is a device, the agreement shall be in one or two parts.

Registration: not in the scope of the CSO

- **REG-6.3.4-13** [CONDITIONAL]: If the subject and subscriber are the same entity or the subject is a device, the agreement shall include the part 1 (see **REG-6.3.4-10)** and part 2 (see **REG-6.3.4-11)** items listed above.

Registration: not in the scope of the CSO

- **REG-6.3.4-14** [PTC]: Clause 9.6.3 of BRG [5] shall apply to the first part of the agreement (see **REG-6.3.4-10**).

N/A.

- **REG-6.3.4-15** [EVCP]: Clause 11.8 of EVCG [4] shall apply to the first part of the agreement (see **REG-6.3.4-10**).

N/A.

- **REG-6.3.4-16:** The agreement may be in electronic form.

A proposed standard agreement is in electronic form within the RA interface. BT's customers can customize this form for their context.

- **REG-6.3.4-17:** The records identified above shall be retained for the period of

time as indicated to the subscriber (as part of the terms and conditions).

Registration: not in the scope of the CSO
BT, as a CSO, keeps technical records about the generation of the certificates

6.3.5 Key pair and certificate usage

OVR-6.3.5-01: The subscriber's obligations (see clause 6.3.4) shall include:

BT PLC is not dealing with subscribers and subjects - This obligation is not in the scope of the CSO

OVR-6.3.5-02 [CONDITIONAL]: If the subject and subscriber are separate entities and the subject is a natural or legal person, the subject's obligations shall comply with **OVR-6.3.5-01 for** points b), c), e), f), h), i) and j).

Out of scope of BT's responsibility

OVR-6.3.5-03: The notice to relying parties (see clause 6.9.4) shall recommend the relying party to:

Out of scope of BT's responsibility

6.3.6 Certificate renewal

[Deviation 02] BT CPS states in its CPS that Certificate renewal is the issuance of a new certificate to the Subscriber without changing the public key or any other information in the certificate.
From the application interface, a "Renew" button indeed is active. It seems that this button re-builds a certificate an requires a new key-pair.
Clarification of the real implemented practice is needed.

6.3.7 Certificate Re-key

Certificate rekeys is allowed by the policy, but not proposed …

6.3.8 Certificate modification

Certificate rekeys is allowed by the policy, but not really proposed … It has to be handled like the first registration.

6.3.9 Certificate revocation and suspension

REV-6.3.9-01: The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests (see also **REV-6.2.4-03**).

Revocation of certificates are performed within 24h.
A new CRL is published every 12hours as a minimum.

REV-6.3.9-02: The TSP shall revoke any non-expired certificate:

The TSP can revoke user certificates for the mentioned reasons.

a) that is no longer compliant with the CP under which it has been issued; or

b) that the TSP is aware of changes which impact the validity of the certificate; or

c) for which the used cryptography is no longer ensuring the binding between the subject and the public key.

REV-6.3.9-03: The subject, and where applicable the subscriber, of a revoked or suspended certificate, where possible, shall be informed of the change of status of the certificate.

[Deviation 03] With a test certificate generated on BT Trustwise, revocation was performed by the TSP but no notification was received by the subject.

REV-6.3.9-04: Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

Re-instation is not supported. Once a certificate is revoked even rekey is no longer possible.

Where Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used:

- **CSS-6.3.9-05** [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, these shall be published at least every 24 hours;

Compliant: BT publishes the CA CRL every 12 hours as a minimum.

- **CSS-6.3.9-06** [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, every CRL shall state a time for next scheduled CRL issue, unless it is the last CRL issued for those certificates in the scope of the CRL, in which case the nextUpdate field in the CRL defined in IETF RFC 5280 [7], should be set to "99991231235959Z";

Compliant: CRLs include a *nextUpdate* field.

- **CSS-6.3.9-07** [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, a new CRL may be published before the stated time of the next CRL issue.

The TSP publishes CRLs at regular intervals only.

CSS-6.3.9-08 [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, the CRL shall be signed by the CA or an entity designated by the TSP.

The CRLs are signed by the issuing CA.

CSS-6.3.9-09 [PTC]: The TSP shall operate and maintain its certificate status information.

N/A.

CSS-6.3.9-10 [PTC]: Clause 4.10.2 of BRG [5] shall apply.

N/A.

CSS-6.3.9-11 [EVCP]: TSP shall comply with EVCG [4], clause 13.

N/A.

Where CARL is used:

- **CSS-6.3.9-12** [CONDITIONAL]: If CARL is used, a new CARL shall be generated at least once a year with a nextUpdate of at most 1 year after the issuing date;

The CARL validation period is 1 year… Publication is performed by DIGICERT.

- **CSS-6.3.9-13** [CONDITIONAL]: If CARL is used, a new CARL shall be generated once a CA certificate has been revoked.

This process is managed by DIGICERT and is out of BT's responsibility

CSS-6.3.9-14: In the case of any cross-certificates issued by the CA to other TSPs, the CARL should be issued at least every 31 days.

N/A currently.

6.3.10 Certificate status services

CSS-6.3.10-01: The TSP shall provide services for checking the status of the certificates.

Compliant: The TSP provides CRL publication services.

In particular:

- **CSS-6.3.10-02:** Revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.

CRL web page is running on a server that is redundant in BT PLC datacenter, with another occurrence running in Belfast datacenter.

- **CSS-6.3.10-03:** The integrity and authenticity of the status information shall be protected.

The CRLs are signed by CA's secret key, therefore protected in integrity and authenticity.

- **CSS-6.3.10-04:** Revocation status information shall include information on the status of certificates at least until the certificate expires.

Status information delivered by CRL contains the required data. Currently BT has not activated the "pruning" option, meaning that expired certificates are kept on the revocation lists.

Revocation status information methods:

- **CSS-6.3.10-05:** OCSP or CRL shall be supported.

CRL are supported.

- **CSS-6.3.10-06:** OCSP should be supported.

OCSP is not supported for the CAs within the scope of this audit.

- **CSS-6.3.10-07** [PTC]: OCSP shall be supported.

N/A.

When a TSP supports multiple methods (CRL and OCSP) to provide revocation status:

- **CSS-6.3.10-08** [CONDITIONAL]: If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status, any updates to revocation status shall be available for all methods;

N/A

- **CSS-6.3.10-09** [CONDITIONAL]: If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status, the information provided by all services shall be consistent over time taking into account different delays in updating the status information for all the methods.

N/A

- **CSS-6.3.10-10:** The revocation status information shall be publicly and internationally available.

Compliant: the revocation status is publicly available from the repository
http://onsitecrl.trustwise.com
NOTA : The certificates contain a CRLDP extension pointing to the exact concerned CRL file. The access to the parent directory is not possible.

6.3.11 End of subscription

No policy requirement

6.3.12 Key escrow and recovery

The TSP does not support neither key escrow nor key recovery.

6.4 Facility, management, and operational controls

6.4.1 General

OVR-6.4.1-01: The requirements identified in ETSI EN 319 401 [8], clauses 5, 6.3 and 7.3, shall apply.

Compliant. See ETSI EN 319 401 report.

6.4.2 Physical security controls

OVR-6.4.2-01: The requirements identified in ETSI EN 319 401 [8], clause 7.6, shall apply.

Compliant, see ETSI 401 report for more information.

In addition the following particular requirements apply:

OVR-6.4.2-02: The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

[DC Belfast] Compliant, the saferoom reserved for TSP operations is physically protected to unauthorized access.

[DC Cardiff] Compliant. Authorizations to the administrator and operator room is restricted (iris and badge).

OVR-6.4.2-03: Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area.

[DC Belfast] Compliant, any unauthorized person is accompanied.
[DC Cardiff] Compliant. Same as in the Belfast DC.

OVR-6.4.2-04: Every entry and exit shall be logged.

[DC Belfast] Compliant, a visitor book is in the room and every access through the badge system is logged (the traces were seen during the audit).
[DC Cardiff] Same as in Belfast DC, but it seems very difficult to access to these logs.

OVR-6.4.2-05: Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services.

[DC Belfast] Compliant, TSP services are in a specific room.

OVR-6.4.2-06: Any parts of the premises shared with other organizations shall be outside the perimeter of the certificate generation and revocation management services.

[DC Belfast] Compliant, see **OVR-6.4.2-05.**
[DC Cardiff] Compliant, no premises shared with other organizations.

OVR-6.4.2-07: Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

[DC Belfast, Cynal street] Compliant, there is access by global badge, with specific control (fingerprint, iris or PIN code access) for sensitive areas.

OVR-6.4.2-08: The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

[DC Belfast] During the visit, both physical and environmental security were checked. Fire protection is made by Inergen gas, there is two power providers (two arrivals), and multiple telecommunications entry points.

OVR-6.4.2-09: Controls shall be implemented to protect against equipment, information, media and software relating to the TSP's services being taken off-site without authorization.

[DC Belfast] Dual access control is provided in order to avoid this kind of problem.

OVR-6.4.2-10: Other functions relating to TSP's operations may be supported within the same secured area provided that the access is limited to authorized personnel.

[DC Belfast] Backup databases are is the saferoom.

OVR-6.4.2-11: Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates.

[DC Belfast] Root CA private keys are not held by BT.

6.4.3 Procedural controls

OVR-6.4.3-01: The requirements **REQ-7.4-04** to **REQ-7.4-09** in ETSI EN 319 401 [8], shall apply.

Compliant. See ETSI EN 319 401 report.

In addition, the following particular requirements apply:

GEN-6.4.3-02: Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

N/A. Certification issuance by the root CA is not under BT control. Indeed, this process is delegate to DigiCert as it manages and controls the BT Root CA private key.

GEN-6.4.3-03 [PTC]: BRG [5], clause 4.3 shall apply.

N/A.

6.4.4 Personnel controls

OVR-6.4.4-01: The requirements identified in ETSI EN 319 401 [8], clause 7.2 shall apply.

Compliant. See ETSI EN 319 401 report.

OVR-6.4.4-02: In addition to the trusted roles identified in ETSI EN 319 401 [8], (7.2-15), the trusted roles of the registration and revocation officers responsibilities as defined in CEN TS 419 261 [i.9] should be supported.

N/A. BT PKI Managed Services delegates revocation and registration to their customers.

OVR-6.4.4-03 [PTC]: The role of validation specialist shall be included as specified in BRG [5].

N/A.

6.4.5 Audit logging procedures

OVR-6.4.5-01: The requirements identified in ETSI EN 319 401 [8], clause 7.10, shall apply.

Compliant, see ETSI EN 319 401 report.

In addition the following particular requirements apply:

OVR-6.4.5-02: All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

All PKI systems logs are sent to BT Splunk which is managed by a BT support team.

REG-6.4.5-03: All events related to registration including requests for certificate re-key or renewal shall be logged.

N/A. Registration is out of the scope.

REG-6.4.5-04: All registration information including the following shall be recorded:

N/A. Registration is out of the scope.

a) type of document(s) presented by the applicant to support registration;

b) record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;

c) storage location of copies of applications and identification documents, including the subscriber agreement (see requirement **REG-6.3.4-07**);

d) any specific choices in the subscriber agreement (e.g. consent to publication of certificate, see requirement **REG-6.3.4-07**);

e) identity of entity accepting the application;

f) method used to validate identification documents, if any; and

g) name of receiving TSP and/or submitting Registration Authority, if applicable.

REG-6.4.5-05: The TSP shall maintain the privacy of subject information.

Compliant. The protection of customer information is ensured by securing the Trustwise services infrastructure.

GEN-6.4.5-06: The TSP shall log all events relating to the life-cycle of CA keys.

Compliant. PKI events logs are stored in the database.

GEN-6.4.5-07: The TSP shall log all events relating to the life-cycle of certificates.

See GEN-6.4.5-06.

GEN-6.4.5-08: The TSP shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.

BT manages only CA keys, see GEN-6.4.5-06.

REV-6.4.5-09: The TSP shall log all requests and reports relating to revocation, as well as the resulting action.

Compliant, see GEN-6.4.5-06.

6.4.6 Records archival

OVR-6.4.6-01: The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:

a) log of all events relating to the life cycle of keys managed by the CA, including any subject keypairs generated by the CA (see requirement **GEN-6.4.5-08**);

Compliant. All logs regarding CA keys (only keys managed by BT) are in the database ; logs are not deleted.

b) documentation as identified in clause 6.3.4.

N/A. Registration is out of the scope.

6.4.7 Key changeover

No policy requirement.

6.4.8 Compromise and disaster recovery

OVR-6.4.8-01: The requirements identified in ETSI EN 319 401 [8], clauses 7.9 and 7.11, shall apply.

In addition the following particular requirements apply:

TSP systems data backup and recovery:

- **OVR-6.4.8-02:** TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.

Compliant. All systems and data required to resume CA operations are duplicated in the Belfast DC (with processes disabled). BT makes sure to resume operations within 2 hours in the Belfast DC.

- **OVR-6.4.8-03:** In line with ISO/IEC 27002 [i.7], clause 12.3: Back-up copies of essential information and software should be taken regularly.

Databases are synchronized every 15 minutes.

- **OVR-6.4.8-04:** Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

See OVR-6.4.8-03.

- **OVR-6.4.8-05:** Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

Compliant, the DR plan is tested annually. Last test was on the 8th December 2018.

- **OVR-6.4.8-06:** Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.

Compliant. People involved in the full DR plan test are in the trusted role list.

- **OVR-6.4.8-07** [CONDITIONAL]: If risk analysis identifies information requiring dual controlfor management, for example keys, then dual control should be applied to recovery.

CA key compromise:

- **OVR-6.4.8-08:** The TSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a CA's private key as a disaster.

Compliant. Loss or compromise of CA’s private keys are addressed in the business continuity plan.

- **OVR-6.4.8-09:** The processes planned as per requirement **OVR-6.4.8-08** shall be in place.

Compliant.

- **OVR-6.4.8-10:** Following a disaster, the TSP shall, where practical, take steps to avoid repetition of a disaster.

N/A. This is out of primary responsibility of BT.

In the case of compromise as a minimum:

- **OVR-6.4.8-11:** The TSP shall inform the following of the compromise: all

subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSPs;

- **OVR-6.4.8-12:** The TSP shall make the information in **OVR-6.4.8-11** available to other relying parties;
- **OVR-6.4.8-13:** The TSP shall indicate that certificates and revocation status information issued using this CA key may no longer be valid; and
- **OVR-6.4.8-14:** The TSP shall revoke any CA certificate that has been issued for the compromised TSP when a TSP is informed of the compromise of another CA.

Algorithm compromise:

- **OVR-6.4.8-15:** Should any of the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP shall inform all subscribers and relying parties with whom the TSP has agreement or other form of established relations. In addition, the TSP shall make this information available to other relying parties.

This is not provided for in TSP procedures.

- **OVR-6.4.8-16:** Should any of the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP shall schedule a revocation of any affected certificate.

This is not provided for in TSP procedures.

6.4.9 Certification Authority or Registration Authority termination

In the CPS, BT specifies that it is the customer's responsibility to have a termination plan.
This part is outside the scope of this audit because we only consider the operator functions of the certification authority, not the responsibilities of the TSP.

OVR-6.4.9-01: The requirements identified in ETSI EN 319 401 [8], clause 7.12, shall apply.

N/A.

In addition the following particular requirements apply:

OVR-6.4.9-02: Requirement **REQ-7.12-06** of ETSI EN 319 401 [8], shall apply to the following information for their respective period of time as indicated to the subscriber and relying party (see in particular **REG-6.3.4-17** and CSS-6.3.10-02**):**

a) registration information (see clauses 6.2.2, 6.3.1 and 6.3.4);

Not of the audit scope.

b) revocation status information (see clause 6.3.10);

Not of the audit scope.

c) event log archives (see clauses 6.4.5 and 6.4.6).

Not of the audit scope.

OVR-6.4.9-03: Requirement **REQ-7.12-10** of ETSI EN 319 401 [8], shall also include the handling of the revocation status for unexpired certificates that have been issued.

Not of the audit scope.

OVR-6.4.9-04: When another cross certified TSP stops all operations, including handling revocation (see 6.4.9-03), all cross certificates to that TSP shall be revoked.

N/A.

6.5 Technical security controls

6.5.1 Key pair generation and installation

OVR-6.5.1-01: The requirements identified in ETSI EN 319 401 [8], clause 7.5, shall apply.

See the related chapter(s) in section ETSI EN 319 401 of this report: Compliant

In addition, the following particular requirements apply:

GEN-6.5.1-02: The TSP shall generate CA keys, including keys used by revocation and registration services, securely and the private key shall be secret.

Compliant: No change since the last audit - A last key-ceremony was performed following the previous audit. Previously generated unused key-pairs were destroyed, and a few new key pairs on a KC HSM operation in strict FIPS mode were pre-generated for potential future CA re-key or CA creations.

- **GEN-6.5.1-03:** The CA key pair generation and the subsequent certification of the public key, shall be undertaken in a physically secured environment (see clause 6.4.2) by personnel in trusted roles (see clause 6.4.4).

Key Ceremonies (KC) were conducted in the secure server room (Cardiff DataCenter) with proper trusted role staff.

- **GEN-6.5.1-04:** The CA key pair used for signing certificates shall be created under, at least, dual control.

CA keys were generated by personnel in trusted roles under dual control.

- **GEN-6.5.1-05:** The number of personnel authorized to carry out CA key pair generation shall be kept to a minimum and be consistent with the TSP's practices.

The number of personnel in charge of the PKI secrets is consistent with this requirement, given the size of the PKI.

- **GEN-6.5.1-06:** CA key pair generation should be performed using an algorithm as specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

Compliant: Algorithm is SHA2withRSAencryption.

- **GEN-6.5.1-07:** The selected key length and algorithm for CA signing key should be one which is specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

No change since last audit: WARNING The key length of the current CAs within the scope of this audit are 2048 bits long. The current recommendation of SOG-IS and the TS 119 312 is that for signing purpose on a duration longer than 6 years the size of the key should be higher than 3000. BT managed CAs have a life of 5 years.

GEN-6.5.1-08: Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, the

CA shall generate a new certificate for signing subject key pairs, and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate.

Formally BT PLC as PKI operator is not responsible for the non-disruption of the production capability of his TSP customers. BT send a warning information to his customers before the certificate expires.

GEN-6.5.1-09: Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, the new CA certificate shall also be generated and distributed in accordance with the present document.

See GEN-6.5.1-08

GEN-6.5.1-10: The operations described in **GEN-6.5.1-08** and **GEN-6.5.1-09** should be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with the TSP (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a TSP which will cease its operations before its own certificate-signing certificate expiration date.

Not under BT' responsibility

GEN-6.5.1-11: The TSP shall have a documented procedure for conducting CA key pair generation for certificate signing keys for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users.

BT PLC is using indeed a common procedure for generating the CAs that are in the scope of this audit. The auditors had access to all the latest key ceremony scripts and reports used.
Root CA signing is not under BT responsibility, it is managed by DIGICERT
SubCA (Primary CAs in the meaning of STN policy) are not either under BT responsibility, they are managed by DIGICERT.
Production CAs are generated by BT, with the support of DIGICERT.
BT performs the key ceremony, builds a self-signed certificate and request a proper signature from DIGICERT, currently under the BT Class 2 CA - G3 Primary CA. BT then installs the signed certificate in the PKI management suite.

GEN-6.5.1-12: The procedure of **GEN-6.5.1-11** shall indicate, at least, the following:

The only change since the last audit was the closing of a deviation.
The last KC report has proved to be compliant with a) to d) requirements.

a) roles participating in the ceremony (internal and external from the organization);

The previous deviation on this point has been solved and checked after the audit.
The last KC has clearly mentioned participants.

b) functions to be performed by every role and in which phases;

OK on the last KC

c) responsibilities during and after the ceremony; and

OK on the last KC

d) requirements of evidence to be collected of the ceremony.

Compliant.

GEN-6.5.1-13: The TSP shall produce a report proving that the ceremony, as in **GEN-6.5.1-11** above, was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured.

Compliant: Last KC report performed on the 6th September 2018 has been checked.

GEN-6.5.1-14: This report shall be signed [CHOICE]:

- For root CA: by the trusted role responsible for the security of the TSP's key management ceremony

N/A

(e.g. security officer) and a trustworthy person independent of the TSP's management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.

- For subordinate CAs: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out.

Some KC report has been manually signed by the PKI manager (Karl) and a witness (Janet Cope).
[Deviation 04] Last KC ceremony reports were improved since last audit, and have on the first page the list of participants with roles. But the two latest KC reports seen on the field were not manually signed.

GEN-6.5.1-15 [PTC]: Clause 6.1.1.1 of the BRG [5] shall apply.

N/A.

DIS-6.5.1-16: CA signature verification (public) keys shall be available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.

CA keys, and all the trust chain up to the root, are delivered to the users through PKCS#7 files, when retrieving the certificate. The chain of trust guarantees the integrity.
Theses CA's certificates can also be retrieved from the following public URL :
https://www.trustwise.com/SearchDigitalID.html

When the CA generates the subject's keys:

- **SDP-6.5.1-17** [CONDITIONAL]: If the CA generates the subject's keys, CA-generated subject keys shall be generated using an algorithm recognized as being fit for the uses identified in the CP during the validity time of the certificate.

N/A : The TSP does not generated the subject's keys

- **SDP-6.5.1-18** [CONDITIONAL]: If the CA generates the subject's keys, CA-generated subject keys should be of a key length and for use with a public key algorithm as specified in ETSI TS 119 312 [i.10] for the purposes stated in the CP during the validity time of the certificate.

N/A : The TSP does not generated the subject's keys

- **SDP-6.5.1-19** [CONDITIONAL]: If the CA generates the subject's keys , CA-generated subject keys shall be generated and stored securely whilst held by the TSP.

N/A : The TSP does not generated the subject's keys

- **SDP-6.5.1-20** [CONDITIONAL]: If the CA generates the subject's keys, the subject's private key shall be delivered to the subject's device or to the TSP managing the subject's private key, in a manner such that the secrecy and integrity of the key is not compromised.

N/A : The TSP does not generated the subject's keys

- **SDP-6.5.1-21** [CONDITIONAL]: If the CA generates the subject's keys and if the TSP or any of its designated RAs become aware that a subject's private key has been

communicated to an unauthorized person or an organization not affiliated with the subject, then the TSP shall revoke all certificates that include the public key corresponding to the communicated private key.

N/A : The TSP does not generated the subject's keys

- **SDP-6.5.1-22** [CONDITIONAL]: If the CA generates the subject's keys, the CA shall delete all copies of a subject private key after delivery of the private key to the subject, except for conditions as described in clause 6.3.12.

N/A : The TSP does not generated the subject's keys

- **SDP-6.5.1-23** [NCP+] [CONDITIONAL]: If the CA generates the subject's keys, the TSP shall secure the issuance of a secure cryptographic device to the subject.

N/A : The TSP does not generated the subject's keys

In particular:

- **SDP-6.5.1-24** [CONDITIONAL]: If the CA generates the subject's keys, secure cryptographic device preparation shall be done securely.

N/A : The TSP does not generated the subject's keys

- **SDP-6.5.1-25** [CONDITIONAL]: If the CA generates the subject's keys, secure cryptographic device shall be securely stored and distributed.

N/A : The TSP does not generated the subject's keys

6.5.2 Private key protection and cryptographic module engineering controls

OVR-6.5.2-01: TSP's key pair generation, including keys used by revocation and registration services, shall be carried out within a secure cryptographic device which is a trustworthy system which:

a) is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national or internationally recognized evaluation criteria for IT security provided this is a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or

b) meets the requirements identified in ISO/IEC 19790 [3] or FIPS PUB 140-2 [12] level 3.

The HMS that is used by BT PLC to generate the key-pairs is a Luna SA5.
This Luna SA5 (cryptomodule firmware version 6.2.1 is FIPS certified with certificate NIST N° 2480 (see appendix II). During the last Key Ceremony, this HSM has been used in strict FIPS 140-2 level 3 mode.
NOTA: The key-pairs that were generated before the last key-ceremony (and before the previous audit) were not in line with the current requirement. But BT has taken the actions to close this deviation for any future operation.

OVR -6.5.2-02: The secure cryptographic device shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

[Deviation 01] If the HSM LunaSA5 used for key generation is now operated in FIPS mode, the online production HSMs used for signing end-user certificates on each CA is operated in non-FIPS mode.

OVR -6.5.2-03: The above secure cryptographic device should be assured as per **OVR-6.5.2-01**-a), above.

See deviation 01

GEN-6.5.2-04: The CA private signing key shall be held and used within a secure cryptographic device meeting the requirements of **OVR-6.5.2-01** and **OVR-6.5.2-02** above.

See deviation 01

GEN-6.5.2-05 [CONDITIONAL]: When outside the secure cryptographic device (see **GEN-6.5.2-04** above) the CA private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.

Compliant: the key pairs generated on the KC HSM are loaded on a FIPS compliant backup HSM and loaded on the production HSMs in Cardiff, and on the off-line HSM in Belfast (DRC).

GEN-6.5.2-06: The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 6.4.2).

Compliant: The copies of the key pairs are stored and backed-up in an HSM. They are also stored in a safe collocated within the Key Ceremony room. Access to the Key Ceremony room needs multiple access control.

GEN-6.5.2-07: The number of personnel authorized to carry out the CA private signing key back up, storage and recovery shall be kept to a minimum and be consistent with the CA's practices.

Compliant: See **GEN-6.5.2-06**
Last KC report shows involvement of 3 persons.

GEN-6.5.2-08: Copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

Compliant: See point c) above about backup HSM

GEN-6.5.2-09 [CONDITIONAL]: Where the CA private signing keys and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.

Compliant: No change since last audit

OVR -6.5.2-10: The secure cryptographic device shall not be tampered with during shipment.

Compliant: No change since last audit

OVR -6.5.2-11: The secure cryptographic device shall not be tampered with while stored.

Compliant: No change since last audit

OVR -6.5.2-12: The secure cryptographic device shall be functioning correctly.

Compliant: During the audit, the two HSMs in production were functioning.

GEN-6.5.2-13: The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

Compliant: There is a specific procedure about decommissioning sensitive media. For HMs, this includes the reset to zero and key erasing.

6.5.3 Other aspects of key pair management

OVR-6.5.3-01: The TSP shall use appropriately the CA private signing keys.

Compliant, see below:

In particular:

- **OVR-6.5.3-02:** The TSP shall not use the CA private signing keys beyond the end of their life cycle.

Compliant: This is currently enforced by the SYMANTEC management suite

- **GEN-6.5.3-03:** CA signing key(s) used for generating certificates as defined in clause 6.3.3, and/or issuing revocation status information, shall not be used for any other purpose.

The keyUsage for any CA is set at Certificate Sign, CRL Sign. Thus, any other usage of the CA Key is not authorized and currently not used.

- **GEN-6.5.3-04:** The certificate signing keys shall only be used within physically secure premises.

CA HSMs are stored in the secure rooms of Datacenters Cardiff.

- **GEN-6.5.3-05:** The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice as in requirement **GEN-6.5.1-07**.

Compliant, see §6.5.1 above (CA's key length of 2048 bits, use of RSA with SHA256).

- **GEN-6.5.3-06:** All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

No change since last audit - Report for key destruction ceremony were checked.
One for deletion of keys in HSM CA3 was performed on 17 January 2013 (just after the CA3 to CA4 migration)
One for deletion of keys in HSM CA4 was performed on 18 October 2017 (just after the CA4 to SA5 migration that occurred on 8/10/2017)Keys are destroyed when they are no longer needed, or when certificates to which they correspond expire or are revoked. This is written on the Termination plan (point 3); note that this information should appear in the CPS (***Area of improvement***).

- **GEN-6.5.3-07** [CONDITIONAL]: If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in Recommendation ITU-T X.509 [6] and aligned with **GEN-6.5.3-05**.

Self-signed certificates are only used temporarily before them to be signed by DIGICERT.

6.5.4 Activation data

GEN-6.5.4-01: The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two trusted employees.

Compliant: At least three items out of 10 and belonging to separate personal are need to install or recover CA's key pairs.

If the TSP issues a secure cryptographic device:

- **SDP-6.5.4-02** [CONDITIONAL]: If the TSP issues a secure cryptographic device, secure cryptographic device (e.g. smartcard) deactivation and reactivation shall be done securely.

N/A : no cryptographic device is delivered

- **SDP-6.5.4-03** [CONDITIONAL]: If the TSP issues a secure cryptographic device, and where the personalized secure cryptographic device (e.g. smartcard) has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and

distributed separately from the secure cryptographic device.

N/A : no cryptographic device is delivered

6.5.5 Computer security controls

OVR-6.5.5-01: The requirements **REQ-7.4-01, REQ-7.4-02**, **REQ-7.4-03** and **REQ-7.4-10** in ETSI EN 319 401 [8] shall apply.

In addition the following particular requirements apply:

GEN-6.5.5-02: Local network components (e.g. routers) shall be kept in a physically and logically secure environment.

[DC Belfast, DC Cardiff] Compliant. All assets, except the arrival of the network (Optical fiber arrival) are in a secure room.

GEN-6.5.5-03: Local network components (e.g. routers) configurations shall be periodically checked for compliance with the requirements specified by the TSP.

[DC Cardiff] Global BT Network team manages the Trustwise Services network.

GEN-6.5.5-04: The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

[DC Cardiff] Users of “managed PKI control center” have multi-factor authentication enforced.
All administrators are logged through two-factor authentication.

DIS-6.5.5-05: Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

[DC Cardiff] Adding or deleting a certificate requires to be connected to a critical system, located securely.

CSS-6.5.5-06: Revocation status application shall enforce access control on attempts to modify revocation status information.

[DC Cardiff] Control center operators need to login to perform a revocation.
End users can revoke their certificate directly on publicly accessible web page with their email and a passphrase (defined during the enrolment process).

OVR-6.5.5-07: Continuous monitoring and alarm facilities shall be provided to enable the TSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

[DC Cardiff] Nagios is used to monitor all PKI services servers. Citrix gateway that is used to access to all system resources is also monitored.

6.5.6 Life cycle security controls

OVR-6.5.6-01: The requirements identified in ETSI EN 319 401 [8], clause 7.7 shall apply for all service components.

Compliant. See ETSI EN 319 401 report.

In addition the following particular requirements apply:

OVR-6.5.6-02 [NCP]: Capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available.

N/A. Only LCP certificates.

OVR-6.5.6-03 [PTC]: Clause 5 of the BRG [5] shall apply.

N/A.

6.5.7 Network security controls

OVR-6.5.7-01: The requirements identified in ETSI EN 319 401 [8], clause 7.8 shall apply.

Compliant. See ETSI EN 319 401 report.

In addition the following particular requirements apply:

OVR-6.5.7-02: The TSP shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.

[DC Belfast] Compliant. The room for TSP activities is dedicated for the purpose. Both the HSM and the signing servers are inside a safe-rack (access restricted by a combination).
[DC Cardiff] Signing servers and HSMs are inside a safe-rack. Others CA systems are in a dedicated room in the 14th floor. The person who can access to the safe-rack can't access to the room.

OVR-6.5.7-03: The TSP shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

[DC Cardiff] Compliant. All systems or applications account are regularly reviewed. Regarding protocols and ports that are not used, see report ETSI EN 319 401 clause 7.8. An internal application called VINTELA is used to manage all logical account (application and systems credentials).

OVR-6.5.7-04: The TSP shall grant access to secure zones and high security zones to only trusted roles.

[DC Belfast] Compliant. Dual control in enforced, and only trusted role can access to the high security zones dedicated for TSP operations.
[DC Cardiff] Access to the PKI room are restricted to trusted roles.

OVR-6.5.7-05: The Root CA system shall be in a high security zone.

[DC Belfast, DC Cardiff] Root CA keys are not owned by BT.

6.6 Certificate, CRL, and OCSP profiles

6.6.1 Certificate profile

GEN-6.6.1-01: The certificates shall meet the requirements specified in Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

The delivered certificates concerned by the audit are LCP certificates with EKU = Web client authentication and email protection. They follow the RFC5260 recommendation.
Due to evolution of STN policy, the CA certificate profile implemented some change , propagating to changes in the end user certificate profiles :

5 recently produced certificates on each CA were analyzed during the audit.
Correction of the previous deviation (wrong OID) has been corrected.
No other flaw has been identified on the current profiles.

GEN-6.6.1-02: The certificate shall be issued according to the relevant certificate profile [CHOICE]:

- [LCP, NCP and NCP+] for issuance of certificates to natural persons (excluding for web site certificates): ETSI EN 319 412-2 [9].

Compliant: Certificates are delivered to natural persons.

- [LCP, NCP and NCP+] for issuance of certificates to legal persons (excluding for web site certificates): ETSI EN 319 412-3 [10].

N/A.

- [PTC] for issuance of certificates for web sites or devices: ETSI EN 319 412-4 [2].

N/A.

6.6.2 CRL profile

OVR-6.6.2-01: The CRL shall be as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

The CRL profiles properly comply with the IETF RFC 5280 requirements.
Sequence number for BTSecureEmailCA seem not to be consecutive.

6.6.3 OCSP profile

N/A: There is no OCSP service on the CAs concerned by the present audit.

OVR-6.6.3-01: The OCSP shall be as defined in IETF RFC 6960 [11].

OVR-6.6.3-02: If the OCSP responder receives a request for status of a certificate that has not been issued then the responder shall not respond with a "good" status as per clause 2.2 of IETF RFC 6960 [11].

OVR-6.6.3-03: The CA should monitor such requests concerning non-issued certificates on the responder as part of its security response procedures to check if this is an indication of an attack.

6.7 Compliance audit and other assessment

6.8 Other business and legal matters

6.8.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

6.8.2 Financial responsibility

OVR-6.8.2-01: The requirement **REQ-7.1.1-04** identified in ETSI EN 319 401 [8], shall apply.

Compliant. See ETSI EN 319 401 report.

6.8.3 Confidentiality of business information

No policy requirement

6.8.4 Privacy of personal information

OVR-6.8.4-01: The requirement **REQ-7.13-05** identified in ETSI EN 319 401 [8], shall apply.

Compliant. See ETSI EN 319 401 report.

In addition the following particular requirements apply:

OVR-6.8.4-02: The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed TSP's system components.

[Deviation 08] Registration data stored in the database are not protected against being revealed; no encryption method is applied to the database. This deviation was identified during the previous audit.
A migration of the database (that would include database encryption) should have been performed before March 2019.

OVR-6.8.4-03: Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clauses 6.4.5 and 6.4.6).

CA's private keys are securely retained (in SafeNet Backup HSM, in a safe inside of the Cardiff Stadium House DC).

6.8.5 Intellectual property rights

No policy requirement

6.8.6 Representations and warranties

OVR-6.8.6-01: The requirements **REQ-6.3-05** and **REQ-6.3-06** identified in ETSI EN 319 401 [8] shall apply.

In addition the following particular requirements apply:

- **OVR-6.8.6-02:** The TSP shall provide all its certification services consistent with its CPS.

Compliant. CA operations are compliant with the current CPS.

- **OVR-6.8.6-03** [PTC]: The TSP shall comply with BRG [5], clause 9.6.

N/A.

6.8.7 Disclaimers of warranties

See clause 6.8.6.

6.8.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.9.4.

6.8.9 Indemnities

No policy requirement

6.8.10 Term and termination

No policy requirement

6.8.11 Individual notices and communications with participants

No policy requirement

6.8.12 Amendments

No policy requirement

6.8.13 Dispute resolution procedures

OVR-6.8.13-01: The item h) of requirement **REQ-6.2-02** identified in ETSI EN 319 401 [8], and the requirement

N/A.

REQ-7.1.1-06 identified in ETSI EN 319 401 [8], shall apply.

Compliant, see ETSI EN 319 401 report.

6.8.14 Governing law

Not in the scope of the present document

6.8.15 Compliance with applicable law

OVR-6.8.15-01: The requirements **REQ-7.13-01 and REQ-7.13-02** identified in ETSI EN 319 401 [8], shall apply.

Compliant, see ETSI EN 319 401 report.

6.9 Other provisions

6.9.1 Organizational

OVR-6.9.1-01: The requirements identified in ETSI EN 319 401 [8], clause 7.1 shall apply.

Compliant, see ETSI EN 319 401.

In addition the following particular requirements apply:

OVR-6.9.1-02: The parts of the TSP concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies.

Compliant. Generation and revocation are operating by the BT clients (TSPs) and not BT itself.

In particular:

- **OVR-6.9.1-03:** The senior executive, senior staff and staff in trusted roles, of the

TSP concerned with certificate generation and revocation management shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

See OVR-6.9.1-02.

OVR-6.9.1-04: The parts of the TSP concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

See OVR-6.9.1-02.

6.9.2 Additional testing

OVR-6.9.2-01: The TSP shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

Compliant, tests certificates during audit were emitted in production by the BT's CA "Trustwise G3".

OVR-6.9.2-02: Any test certificates should clearly indicate that they are for testing purposes (e.g. by the subject name).

It was not the case during the audit, but certificates were revoked directly after the test.

OVR-6.9.2-03 [PTC]: BRG [5], clause 2.2 shall apply.

N/A.

OVR-6.9.2-04 [PTC]: For cross certificates, clause 3.2.6 of BRG [5] shall apply.

N/A.

6.9.3 Disabilities

OVR-6.9.3-01: The requirements **REQ-7.13-03** and **REQ-7.13-04** identified in ETSI EN 319 401 [8], shall apply.

Compliant. See ETSI EN 319 401 reports.

6.9.4 Terms and conditions

N/A. This requirement concerns primarily BT's customers - As a managed PKI service provider, BT has delivered to its customers a contract with terms and conditions as far as there are concerned.

OVR-6.9.4-01: The requirements identified in ETSI EN 319 401 [8], clause 6.2 shall apply.

In addition the following particular requirements apply:

OVR-6.9.4-02: The terms and conditions shall include at minimum the following elements:

a) the indication of what constitutes certificate acceptance, as specified in **OVR-6.3.4-01**;

b) the period of time for which the records are retained according to **OVR-6.3.4-17**;

c) the subscriber's obligations as specified in **OVR-6.3.5-01**;

d) where applicable, the subject's obligations as specified in **OVR-6.3.5-02**;

e) the notice to relying parties as specified in **OVR-6.3.5-03**;

f) the ways in which a specific policy adds to or further constrains the requirements of the CP as defined in the present document, see **OVR-7.2-01**.

OVR-6.9.4-03 [PTC]: The TSP may limit its responsibilities as indicated in clause 9.8 of BRG [5].

OVR-6.9.4-04 [EVCP]: The TSP may limit its responsibilities as indicated in clause 9.8 of BRG [5] within the restrictions indicated in EVCG [4], clause 18.

7 Framework for the definition of other certificate policies

7.1 Certificate policy management

OVR-7.1-01: The authority issuing a CP other than the ones defined in clause 5 shall demonstrate that the CP is effective.

BT-PLC is a Certification Service Operator that is included in the Symantec Trusted Network (STN) . BT applies therefore the STN policy. The ETSI EN319411-1 policy, as defined in clauses 5 and 6 of the present report applies on top of the STN policy.

In particular, when the TSP issues other CPs:

- **OVR-7.1-02:** The CP shall identify which of the certificate policies defined in the present document it adopts as the basis, plus any variances it chooses to apply.

Compliant: The current BT service offer, as specified by the STN policy, is based on the ETSI LCP policy.

- **OVR-7.1-03:** There shall be a body (e.g. a policy management authority) with final authority and responsibility for specifying and approving the CP.

Compliant: The body within BT-PLC is called " BT-PLC SA Certification Policy Approval Council"

- **OVR-7.1-04:** A risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the CP for the stated community and applicability.

Compliant: See EN 319 401 §

- **OVR-7.1-05:** CPs should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the CP.

Compliant: See § 9.10 in the CP

- **OVR-7.1-06:** A defined review process should exist to ensure that the CP is supported by the CA's CPS.

There are several internal audits performed by BT-PLC.
BT is also requirement ETSI audits like the one which is subject to the present report.
BT is also subject to audit related to the UK scheme (T-SCHEME)

- **OVR-7.1-07:** The TSP should make available the CPs supported by the TSP to its user community.

Compliant: CP are always made public on the repository site.

- **OVR-7.1-08:** Revisions to CPs supported by the TSP should be made available to subscribers and relying parties.

Compliant: CP are always made public on the repository site.

- **OVR-7.1-09:** The CP shall incorporate, or further constrain, all the requirements identified in clauses 5 and 6 where they are without a specific marking relating CP as specified in clause 5.3.

Compliant: BT's CP is derived from the STN policy. The STN Policy is also published on the repository site.

- **OVR-7.1-10:** The CP shall specify the Recommendation ITU-T X.509 [6] certificate profile requirements.

Compliant: See section 6.6 of the report.

- **OVR-7.1-11:** Certificate profiles as defined by ETSI EN 319 412 part 2 to 4 [2], [9] and [10] should be used where appropriate.

Compliant: See section 6.6 of the report.

- **OVR-7.1-12:** A unique object identifier shall be obtained for the CP of the form required in Recommendation ITU-T X.509 [6].

Compliant: CP OID

7.2 Additional requirements

OVR-7.2-01: Subscribers and relying parties shall be informed, as part of implementing the requirements defined in clause 6.9.4, of the ways in which the specific policy adds to or further constrains the requirements of the CP as defined in the present document.

The STN policy , as a root policy, is published on the repository site.

End of the Conformity Assessment Report - ETSI EN 319 411-1

APPENDIX I - CERTIFICATES SAMPLES (Produced after OID correction)

Certificat LCP / BT Secure Email CA

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            46:23:f7:d2:54:a1:c7:6e:47:4d:8c:49:48:e5:db:03
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, O=British Telecommunications plc, OU=Symantec Trust Network,
OU=Class 2 Managed PKI Individual Subscriber CA, CN=BT Secure Email CA G3
        Validity
            Not Before: May  1 00:00:00 2019 GMT
            Not After : Apr 30 23:59:59 2020 GMT
        Subject: O=British Telecommunications plc, OU=BT Secure Email CA,
OU=www.trustwise.com/rpa, CN=Chhabra,G,Gaurav,VQI R
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9e:78:05:65:f0:9b:de:41:a4:ea:92:94:58:ff:
                    34:b3:98:f5:b6:ac:e8:69:3e:1c:6a:8e:49:6e:31:
                    23:e4:6b:87:54:78:ae:19:e6:dc:bc:75:ce:97:90:
                    68:87:c5:ad:7b:ab:58:b9:2a:94:47:0a:2e:b6:99:
                    92:f2:47:46:fe:dc:b7:11:70:fd:41:4d:ab:e7:17:
                    fa:2c:6b:12:31:dc:42:16:9a:6d:43:3c:5b:37:9d:
                    7c:6c:0e:21:32:1a:f3:ad:85:75:4c:70:07:77:f6:
                    09:5c:5d:95:29:fc:42:5e:ee:fe:d3:5e:ab:ea:74:
                    d2:37:4e:6b:ab:7c:e8:3c:b9:7b:6b:27:68:3b:92:
                    95:4d:eb:13:1f:9c:e3:de:22:a9:55:92:fd:19:27:
                    c8:8a:ef:59:8c:5e:be:32:bb:8d:5a:51:b6:c0:43:
                    c8:2f:c9:10:f4:c0:8e:aa:ad:4b:e3:a2:bc:c4:16:
                    2f:46:7a:a3:71:f6:91:cd:30:a1:b0:ba:2c:df:4d:
                    0a:47:d5:06:3c:26:0d:dd:15:23:cd:98:82:9f:6b:
                    93:ab:f9:5b:b3:6a:c8:05:1a:90:03:54:fe:9b:d9:
                    7f:07:35:d8:06:f1:be:c9:ba:ce:5a:d3:ce:a1:25:
                    87:16:46:e3:0c:86:3b:41:a0:60:b0:07:1f:bf:ad:
                    ee:0d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 CRL Distribution Points:

                Full Name:

URI:http://onsitecrl.trustwise.com/BritishTelecommunicationsplcBTSecureEmailCA/LatestCRL
-G3.crl

            X509v3 Key Usage: critical
                Digital Signature
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.113733.1.7.23.2
                  CPS: https://www.trustwise.com/cps

            X509v3 Subject Alternative Name:
                email:gaurav.2.chhabra@bt.com
    Signature Algorithm: sha256WithRSAEncryption
         72:00:03:10:85:ea:f1:a8:2d:3a:27:3f:ad:8d:27:28:8f:c7:
         e5:43:9d:3a:6f:ab:0e:3a:ca:42:4e:5c:27:60:f8:7e:9a:15:
         50:1f:d1:3f:6d:e8:88:6c:e1:d2:aa:51:fa:94:f4:7c:0f:d7:
         d3:ae:6c:ab:b1:d8:b5:99:71:81:ef:6d:43:eb:9c:6b:ac:88:
```

```
          9a:b8:67:82:9b:0e:3f:cd:07:ea:1c:f8:6a:f6:05:c1:23:1c:
          51:61:89:c3:5a:2d:df:65:f3:45:ef:e5:36:d9:83:5c:1e:3d:
          63:e7:b2:60:98:08:d6:bb:e0:f7:96:43:ec:b7:9a:00:bb:9e:
          16:16:39:9d:73:f5:7a:d6:70:ff:80:34:2c:c0:e6:80:e8:96:
          d2:4e:0a:a0:24:ac:c7:fa:7d:2c:63:f1:11:a5:8c:44:b7:2e:
          47:7f:bc:66:3a:da:e5:b5:b6:dd:23:b5:bd:6c:34:69:d2:20:
          25:4f:c8:81:68:15:65:8a:e8:82:a4:59:65:fc:e4:eb:b7:8f:
          b0:24:0a:7e:a6:68:29:48:34:3b:cc:ba:e7:2e:26:eb:21:42:
          3e:9f:7c:46:8a:d3:d0:e9:9f:cd:16:1c:45:e5:c1:8a:83:5b:
          98:c6:36:2c:8a:9d:f4:7f:78:9e:8a:2a:71:e4:d9:c5:d3:7e:
          29:9c:5f:fd
```

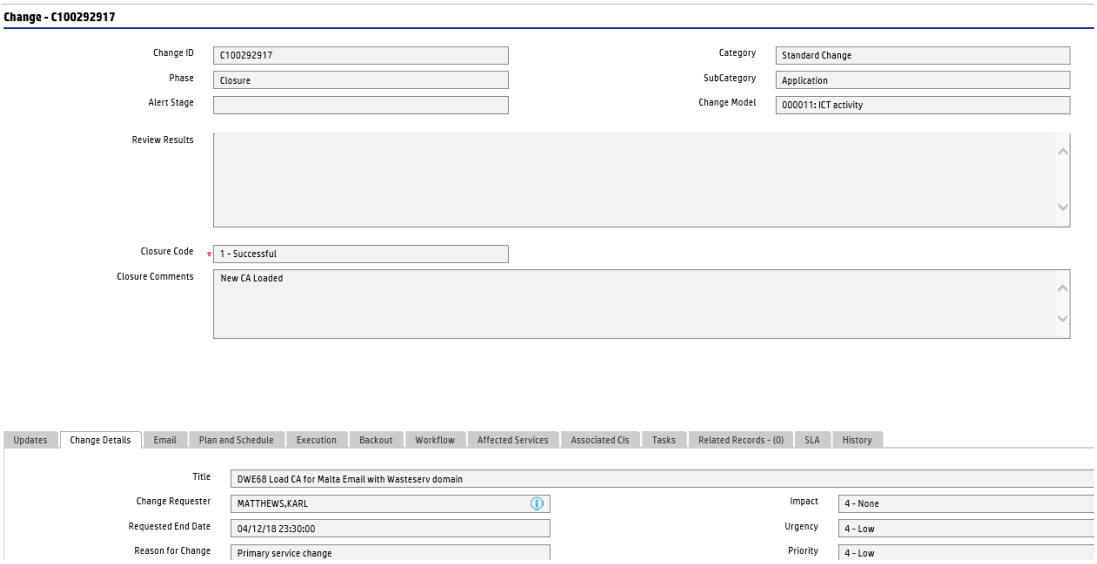
Certificat LCP / HM Revenue and Customs G3

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            46:4f:a4:5c:f3:33:1d:d9:54:8b:43:06:1d:cc:a9:cc
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GB, O=Valuation Office Agency, OU=Symantec Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=HM Revenue and Customs G3
        Validity
            Not Before: Oct 17 00:00:00 2018 GMT
            Not After : Oct 17 23:59:59 2019 GMT
        Subject: O=Valuation Office Agency, OU=HM Revenue & Customs G3,
OU=www.trustwise.com/rpa, OU=LA CODE - J0405, CN=Rob
Stark/emailAddress=rstark@aylesburyvaledc.gov.uk
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e2:63:d6:e0:2d:92:aa:84:9d:8a:98:03:93:68:
                    cc:50:0c:06:3e:47:aa:60:78:12:86:25:ec:1c:4f:
                    75:71:61:10:e5:fb:9e:60:9e:7c:ae:64:fe:cb:a0:
                    ba:66:d7:fc:44:e1:d6:9f:e1:3d:e8:87:9c:7d:ad:
                    f2:59:0c:2e:51:ea:89:8c:92:a5:56:24:a6:51:b3:
                    92:45:37:a6:74:dc:b4:cc:b7:3c:0e:6b:dd:27:bc:
                    0d:df:6d:ea:5d:b6:63:74:a4:09:a3:38:fb:e5:d4:
                    bd:05:84:7d:b7:1e:76:82:a1:c5:91:87:22:30:c4:
                    9e:7d:19:13:10:56:90:bc:c6:40:68:44:93:51:1e:
                    65:8c:90:3d:4e:91:2f:a5:00:bb:cc:cf:91:d0:51:
                    5a:e9:43:eb:ef:71:59:81:ca:57:55:74:fd:73:df:
                    25:dc:fc:a7:b3:48:55:5e:c3:8c:96:2b:17:67:88:
                    6a:8f:d2:97:42:57:d8:f8:af:4b:36:b2:5d:95:03:
                    02:d9:11:2c:68:be:cf:df:0d:67:f6:01:45:1c:7e:
                    c7:ac:42:f3:7c:27:62:b1:5f:a0:fe:f5:cd:78:2f:
                    3a:28:df:16:d8:14:e0:2b:f3:4a:4b:62:b1:64:5e:
                    b8:7e:61:88:6d:47:f2:34:5d:42:0b:7a:90:dd:a4:
                    0e:b3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Certificate Policies:
                Policy: 2.16.840.1.113733.1.7.23.2
                  CPS: https://www.trustwise.com/cps

            X509v3 Key Usage:
                Digital Signature, Key Encipherment
            Netscape Cert Type:
                SSL Client
            X509v3 CRL Distribution Points:

                Full Name:

URI:http://onsitecrl.trustwise.com/ValuationOfficeAgencyHMRevenueCustomsG3/LatestCRL.crl
```

```
        X509v3 Extended Key Usage:
            TLS Web Client Authentication, E-mail Protection
    Signature Algorithm: sha256WithRSAEncryption
         3a:5c:3a:44:77:1a:f9:d5:14:4b:3c:92:98:05:02:29:9e:e5:
         71:bb:97:8f:af:99:b0:57:1c:be:a0:8a:0f:b7:fa:c2:dc:5a:
         49:6d:42:88:83:d4:43:bf:64:3b:36:29:1a:b7:11:b6:82:77:
         4f:c3:d2:9e:63:1c:01:fc:7b:f0:e1:e2:b3:23:ab:4f:08:42:
         9f:c0:f1:fd:23:b7:77:a0:2c:51:5a:77:50:a3:6a:0b:9e:5b:
         f4:e9:b2:50:bb:d7:d2:04:a7:c7:ff:e3:da:6f:b6:1e:a8:25:
         b4:7b:a9:3b:01:69:b0:fc:5d:bf:e8:5b:7e:66:c1:02:5a:29:
         bb:01:b9:15:bd:a9:0f:c5:22:9f:7d:b7:0e:01:4c:91:44:a9:
         4f:54:35:e9:cf:52:69:ae:a6:11:55:d5:9b:16:3b:59:da:cb:
         df:a4:6a:2e:04:85:fa:e1:e0:db:2a:45:a8:ed:3a:ec:4b:24:
         33:e1:82:fc:cc:9f:29:a0:64:9d:7f:e0:6e:05:eb:35:46:0a:
         b1:81:83:5a:69:ef:50:ae:b9:c7:19:ed:f3:2f:6d:1f:a4:b2:
         6a:20:b1:3b:e8:ed:bd:25:28:2c:52:6f:22:36:e5:3d:cb:d6:
         72:92:f1:7f:ed:fc:8a:13:8d:80:c7:ec:50:bd:02:8a:40:19:
         7a:73:5a:f8
```

APPENDIX II - OTHER EVIDENCES

E1 - Gov Malta Change Record: tracing the last CA certificate change (Dec 2018) to incorporate constrained domains.



E2 - FIPS140-2 certificate for HSM - Luna SA 5

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm (http://localhost:1672http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm)

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
2479	12/01/2015	VMAX 6 Gb/s SAS I/O Module with Encryption from EMC	EMC Corporation	Hardware Version: 303-161-101B-05; Firmware Version: 2.13.39.00
2480	12/02/2015	Luna® PCI-e Cryptographic Module	SafeNet, Inc.	Hardware Version: VBD-05-0100, VBD-05-0101 and VBD-05-0103; Firmware Version: 6.2.1 and 6.2.5
2481	12/02/2015	Luna® PCI-e Cryptographic Module	SafeNet, Inc.	Hardware Version: VBD-05-0100, VBD-05-0101 and VBD-05-0103; Firmware Version: 6.2.1 and 6.2.5
2482	12/07/2015	DRAEGER WCM9113 802.11ABGN VG2	Draeger Medical Systems Inc.	Hardware Version: MS32018 Rev. 02; Firmware Version: VG2 with Bootloader version 1.7
2483	12/11/2015	CryptoComplyTM | Java	SafeLogic Inc.	Software Version: 2.2-fips
2484	12/14/2015	SUSE Linux Enterprise Server 12 - StrongSwan Cryptographic Module	SUSE, LLC	Software Version: 1.0
2485	12/14/2015	HiKey PKI Token	Chunghwa Telecom Co., Ltd.	Hardware Version: HiKey3.0-BK; Firmware Version: HiKey COS V3.0
2486	12/15/2015	Luna® Backup HSM Cryptographic Module	SafeNet Assured Technologies, LLC	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.7 and 6.10.9
2487	12/15/2015	Luna® G5 Cryptographic Module	SafeNet Assured Technologies, LLC.	Hardware Version: LTK-03, Version Code 0102; Firmware Version: 6.10.7 and 6.10.9
2488	12/15/2015	Luna® PCI-E Cryptographic Module and Luna® PCI-E Cryptographic Module for Luna® SA	SafeNet Assured Technologies, LLC.	Hardware Version: VBD-05, Version Code 0100, VBD-05, Version Code 0101, VBD-05, Version Code 0103; Firmware Version: 6.10.7 and 6.10.9
2489	12/15/2015	Luna® PCI-E Cryptographic Module and Luna® PCI-E Cryptographic Module for Luna® SA	SafeNet Assured Technologies, LLC.	Hardware Version: VBD-05, Version Code 0100, VBD-05, Version Code 0101, VBD-05, Version Code 0103; Firmware Version: 6.10.7 and 6.10.9
2490	12/15/2015	Cisco Catalyst 6506, 6506-E, 6509, 6509-E Switches with Wireless Services Module-2 (WiSM2)	Cisco Systems, Inc.	Hardware Version: (6506, 6506-E, 6509 and 6509-E) with WiSM2, CN56XX, WS-X6K-SLOT-CVR-E, WS-SVCWISM2FIPKIT= , [CVPN6500FIPS/KIT=, version D0] and one Supervisor Blade: (VS-S2T-10G, VS-S2T-10G-XL, VS-S720-10G-3C or VS-S720-10G-3CXL); Firmware Version: 8.0
2491	12/16/2015	FireEye CM Series: CM-4400, CM-7400, CM-9400	FireEye, Inc.	Hardware Version: CM-4400, CM-7400, CM-9400; Firmware Version: 7.6
2492	12/16/2015	FireEye EX Series: EX-3400, EX-5400, EX-8400, EX-8420	FireEye, Inc.	Hardware Version: EX-3400, EX-5400, EX-8400, EX-8420; Firmware Version: 7.6
2493	12/16/2015	FireEye FX Series: FX-5400, FX-8400	FireEye, Inc.	Hardware Version: FX-5400, FX-8400; Firmware Version: 7.6