

SERVICE POLICY DISCLOSURE STATEMENT
Managed PKI

STATEMENT TYPES	STATEMENT DESCRIPTIONS
TSP contact information:	<p>BT Trust Services Helpdesk PP2, Ty Cynnal Watkiss Way Cardiff, CF11 0SW Telephone: 0870 6087878 Email: support@trustwise.com</p>
Relying Party validation procedures and usage:	<p>Managed PKI Customer: CRLs are posted in customer-specific repositories, the URL of which is communicated to the Managed PKI customer.</p> <p>Managed PKI customers, may also contract for OCSP services, which allows them to check the status of certificates through the use of OCSP. The URL for the relevant OCSP responder is communicated to the Managed PKI Customer.</p> <p>Other Relying Parties (VeriSign Trust Network (VTN) certificates only): Certificate status information is available through web-based query functions accessible through the BT Repository at: https://www.trustwise.com/SearchDigitalID.html</p>
Reliance limits:	None Specified.
Obligations of Subscribers:	<p>The Managed PKI customer is responsible for specifying the obligations of Subscribers for the certificates that they issue. However , for VTN certificates, the end user (Certificate holder) warrants as a minimum that:</p> <ul style="list-style-type: none"> • Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created. • No unauthorised person has ever had access to the Subscriber's private key. • All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true. • All information supplied by the Subscriber and contained in the Certificate is true. • The Certificate is being used exclusively for authorised and legal purposes, consistent with the BT CPS. • The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise. <p>For more information see BT CPS (Issue 3.6) § 9.6.3 http://www.trustwise.com/repository/CPS/cps.htm</p>

<p>Checking obligations of relying parties</p>	<p>The Managed PKI customer is responsible for specifying the obligations of parties relying on the certificates that they issue. However, for VTN certificates, as the relying party is required:</p> <ul style="list-style-type: none"> • To independently assess & determine whether the Certificate is being used for an appropriate purpose. • Not to use the Certificate beyond the limitations set out in BT CPS (Issue 3.6) § 1.4.1 and for purposes prohibited in BT CPS (Issue 3.6) § 1.4.2. • To check the status of the Certificate on which they wish to rely as well as all the Certificates in the Certificate Chain. • To confirm assent to BT's Relying Third Party Charter. <p>For more information see BT CPS (Issue 3.6) § 9.6.4 http://www.trustwise.com/repository/CPS/cps.htm</p> <p>And BT's Relying Third Party Charters http://www.trustwise.com/rpa/index.html</p>
<p>Limited Warranty disclaimer/Limitation of liability:</p>	<p>Direct or indirect loss of profits, anticipated savings, indirect or consequential loss and destruction of data are excluded. Otherwise £750k for any one incident or related series of incidents or £1.5m in any 12 month period.</p> <p>For more detail see customer contract.</p>
<p>Privacy Policy:</p>	<p>Details of BT's Privacy & Security Policy can be found at: http://www.globalservices.bt.com/CampaignDetailAction.do?Record=Managed_PKI_Privacy_security_policy_campaign_all_en-gb</p>
<p>Refund Policy:</p>	<p>None specified – Managed PKI customer pays for service on service acceptance.</p>
<p>Applicable law and dispute resolution:</p>	<p>Applicable Law - Law of England & Wales</p> <p>Dispute Resolution procedure – subject to individual customer agreement</p>
<p>TSP & repository licences, trust marks and audit:</p>	<p>The BT Trust Services operation is accredited to ISO27001 and the Managed PKI service tScheme approved.</p>