PUBLIC SERVICE DESCRIPTION
BT Managed Public Key Infrastructure Security

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

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

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

- CA Key Generation and Management
- Certificate Status Management and Validation

BT uses its own RA to validate requests for the service[1], confirming that the applicant company is registered and that the Managed PKI Security Administrator has the organisational authority required to operate the RA and enter into the Managed PKI Security contract on the applicant company's behalf.

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

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

BT provides the Managed PKI Security customer with certificate status data, either in the form of a Certificate Revocation List or through the use of the Online Certificate Status Protocol (OCSP), to validate certificates within their application(s). (Note: OCSP is not available to Managed PKI Security FastTrack customers). BT also provides status information to relying parties.

[1] How a customer initiates use of, and continues to use the Service is described on the BT Managed PKI Security website: http://www.globalservices.bt.com/uk/en/products/managed-pki-security

For further information, please see the Service Policy Disclosure Statement. This can be found by clicking on the Service Policy Disclosure Statement link in the How Can Help section at:

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