- DCC need a committed service provider who knows and is investing in the market;
    - We have substantial knowledge of, and significant investment in, the future direction of PKI technology – BT are working to evolve tScheme and Symantec have a significant range of investment in PKI technology and IPR globally;
- We are committed to the UK Public sector and PKI market – We have a long term presence in both markets.
    - We offer a very competitive commercial model;

4 Running a managed PKI service is the sole focus of the BT operational unit. Both BT/Symantec operations and technical personnel adhere to the highest IT/InfoSec standards and Best Practices. BT data centres are externally audited every year to ensure the services meet certifications and accredited policy statements.

Part G The Recovery Process

The scenarios which must be planned for as part of the overall DCC service design are as follows:

1 Device key compromise, whereby a smart meter device key store has been compromised, corrupted or rendered unusable. This may occur for an individual device, or a batch of devices – for example a production run of metering equipment with a known flaw.

2 Organisational key compromise, whereby an organizational key has been compromised, lost, corrupted or rendered unusable. This scenario may vary in severity, depending on the role assigned by the certificate(s) corresponding to the private key.

3 Certificate Authority key compromise, whereby a Certificate Authority key has been compromised, lost, corrupted or rendered unusable. This is a very unlikely scenario, given the closed and highly controlled environment in which the CA key material is managed. Example scenarios include, in increasing order of severity, compromise of the Issuing CA, Root CA, Apex Trust Anchor CA, or Contingency Key.

Role of the SMKI

A primary role of the SMKI is to manage and secure all Certificate Authority key material. BT and Symantec have a long and unbroken history of securing highly sensitive private key material for government and e-commerce, including various National ID systems around the world, and the VeriSign Root Certificate Authorities which underpin global e-commerce.

In the case of organizational key compromise, certificates are revoked and reissued according to the CP/CPS, supported by the RA Agent and Authorised Subscriber portals within the SMKI.

In the case of device key compromise, the key regeneration and certificate replacement is a function of the subscriber or the device management systems. The SMKI supports this process through re-enrolment of the device certificates, which may trigger the 2nd duplicate device check and subsequent RA agent review, as per the SMKI workflows in the solution overview section.

In the case of CA key compromise, any compromised issuing CAs will be revoked if applicable, and any certificates issued under those CAs will be revoked (if organizational certificates) and reissued under a new issuing CA. Device certificates will be provisioned using the existing device management systems. Organisational certificates may be re-enrolled via the authorized subscriber portal.

In the case of Root CA key compromise, a new Root CA certificate is generated within the SMKI via a Root CA key ceremony. The distribution of the new Root CA key is a function of the DCC Trust Anchor Management System (TAMS), using the signing certificate issued by the SMKI.

In the case of compromise of the Apex Trusted Root (assumed to be the OCA root), the TAMS will need to load the apex contingency private key together with the decryption key to allow TAMP end points to unwrap the public key embedded within the OCA root certificate. Protection of the contingency key may form part of the SMKI key management function, with the key stored on an offline HSM for which multiple PIN Entry Device (PED) tokens are required for key export. Once the key is exported, a new key and OCA root is generated.

Key protection for the contingency recovery key

It is recommended that the contingency recovery key is generated and stored on a dedicated portable hardware security module, such as Safenet Luna CA4 or G5 module, as a non-exportable private key. This will give the same (or greater) level of key protection as the issuing and root CA keys. During a recovery situation, the Trust Anchor Management System would communicate with the HSM using a standard PKCS11 interface to access the private key in order to perform the required TAMP operations. The end to end process for generating and deploying the recovery key would be as follows.

Key Ceremony:

The Key Manager initialises the HSM, and defines the share policy: for example, 5 hardware keys to be registered, of which 3 are required to start up the HSM.

The key manager then connects the PIN entry device (PED) to the HSM, and starts the initialisation and key generation process. During this process, the PED will prompt for each shareholder in turn to insert their hardware key into the PED USB

slot. Once all hardware keys have been registered, the contingency recovery key pair is generated within the HSM. The public key is exported, and the private key remains within the HSM. There is no way to export the private key from the HSM.

The HSM is then shut down, and placed in the safe in the key ceremony room. The shareholders retain possession of their hardware share keys.

Recovery:

If the worst case scenario happens, and the contingency recovery key is required, the HSM is retrieved from the safe, and transported to the trust anchor management system, where it is connected to the host ready for use. The requisite number of shareholders are assembled, along with their hardware keys. The PED is connected to the HSM, and the TAMP system started. The PED will prompt each shareholder to insert their hardware key in turn, until the requisite number of keys has been entered (for example 3 of the 5 registered keys). Once the required number of keys have been inserted, the HSM will start up, and the contingency key will be available to the TAMP system software.

Options:

One option is to clone the HSM during the initial key ceremony, using the secure cloning mechanism provided by the HSM firmware. In this case, one HSM could be transported to the TAMP system facility (but not activated), and the clone HSM kept in the key ceremony room safe as backup. In this case, the HSM would not need to be transported to the TAMP facility for recovery - although the shareholders would still need to be present to start the HSM.

Part H RA Management and RA Agents

1 We have included within our Solution Overview (part C) a number of process workflows that show how individual certificate requests will be handled and the role that the DCC RA plays in these processes.

2 BT/Symantec will work with DCC during the design phase of the SMKI implementation to develop the specific tools and define and document the processes and procedures that authorised subscribers and DCC RA personnel will need to follow to submit and approve CSRs prior to their transmission to either the Device or Organisation Certificate Authorities to support these workflows.

3 BT/Symantec will, once the processes are documented and the tools developed, produce a set of training materials and carry out a number of ‘train the trainer’ sessions for DCC at BT or DCC offices so that these trainers can train authorised subscribers and RA agents before the start of User Integration Testing. These training materials will be maintained throughout the lifetime of the contract and updated to reflect any changes to the tools, processes and procedures that are

required once the service is operational, so that they can be used to train new personnel or provide any refresher training that is needed over the lifetime of the project.

4 In addition, BT/Symantec will work with DCC to define and document a robust process for identifying and validating individual subscribers and RA agents that is commensurate with Device and Organisation Certificate Policies (CPs), associate Certificate Practice Statements (CPSs) and HMG Level 3 as defined in GPG43, during the design phase. These processes will draw upon our unparalleled experience of delivering PKI projects for financial, government and other institutions globally as well as other projects for UK government.

Part I Certificate Issuance Performance Metrics

1 BT will produce weekly and monthly management reports for DCC as stated in the requirements, which detail performance of the SMKI against the metrics for both the issuance of certificates for Device and Organisation Certificate Authorities as well as all the other service level metrics. The content, structure and frequency of these reports will be agreed with DCC during the design phase, but will include as a minimum information on the number of certificates requested, issued and where appropriate revoked by each organisation together with details of the time taken to respond to each certificate issuance or revocation request following approval. The report would also contain information, again split by organisation, of the number of batches submitted, the size of these batches and when these were submitted, approved and the certificates returned.

2 In addition, the RA portals for both the Device and Organisation Certificate Authorities will enable the RA Manager and individual RA Agents to view the certificate requests by organisation and view the number of certificates that have been issued, those certificate requests that have been rejected and any certificate requests that are pending waiting approval by the RA. It will also allow the RA Manager and RA Agents to view when individual certificates and batch requests were submitted, approved and actioned.

3 Every event in the certificate lifecycle is fully audited within the PKI backend system, including certificate request, approval, issuance and revocation. The time stamped audit trail includes full certificate details along with information of the actors involved. The audit trail is stored within the Symantec PKI Platform database indefinitely, and available for reporting via the administration interface or directly from the database for custom reports.

Part J tScheme Compliance

1 BT has been an active member of tScheme since its inception in 2004.

2 BT has the practical experience of taking three major services through the tScheme approval process namely:

- the BT Assure PKI service,
- the BT Managed Secure Messaging service, and;
- [redacted], which BT manages on behalf of the [redacted], through the tScheme approval process.

3 BT's PKI service operations are already ISO/IEC27001:2005 accredited and we propose to extend the scope of this ISMS to include the OCA and DCA service operations and extend this accreditation, which will be transitioned to ISO/IEC27001:2013 in the coming 12 months, to include those elements SMKI service that we would deliver to DCC to enable tScheme approval to be achieved.

4 tScheme will not approve services before they are operational. We would therefore plan to obtain Scheme Registered Applicant status for 1 September 2014. Registered Applicant status sets out the scope of the service approval and an agreed timeline for completing the tScheme assessment, and would ensure that full tScheme approval can be obtained within the first quarter of live operation.

5 To support DCC in delivering tScheme accreditation, BT will produce the Specification of Service Subject to Assessment (S3A), engage the tScheme-recognised assessor and manage the accreditation process. However, as the tScheme accreditation will cover the full scope of the SMKI and not just those elements provided by BT/Symantec accreditation, DCC input will be required to complete the S3A and to confirm how the requirements of the tScheme Base Approval Profile, which primarily relates to the overall governance of the service, are best evidenced. DCC will also need to ensure that the PMA and its Registration Authority service operation are in scope of its own BTISO/IEC27001:2005(2013) accreditation and provide support for the annual audits of these elements of the SMKI service by the tScheme-recognised assessor appointed by BT.

Our knowledge and experience in this area will reduce the overall cost, effort, risk and time associated with the delivery of tScheme accreditation for DCC.

Part K Testing

1 General

Within the auspices of the overall Project Plan, the BT Project Manager and Test Manager will be responsible for the Testing work packages. The Testing Manager will generate initial draft Test Strategy & Test Data Strategy for consultation with the DCC and other stakeholders during the Design Phase. This initial draft will be based on the real experiences of developing similar plans

across a range of other Government and Commercial clients implementations. There is a standard system test plan for the base PKI platform, which is supplemented with test cases for any additional components and workflows specific to a particular implementation. This test plan is drafted during the pre-implementation phase, and would be presented to, and agreed with DCC prior to this stage.

2 The Test Manager with the BT PKI service experts will work with DCC and stakeholders to define, document and agree the final testing strategy, associated risks, dependencies and timing within the overall Project Plan. The deliverables at the end of this activity will be the Test Strategy, the Test Data Strategy and detailed Test Plan with its interdependencies. These deliverables will enable the DCC to more accurately understand the various scope, objectives, deliverables, risks and efforts involved in the PIT, SIT and UIT stages.

3 Key activities will include:

- Agreeing communication protocols
- Defining SMKI platform's non-functional tests & acceptance criteria
  - System documentation, system performance and security model validation
- Defining the functional & interface tests along with acceptance criteria
  - Systems tests, data level tests, user interface tests

4 The SMKI platform will undergo a process of software implementation and configuration, followed by activation with CA keys for integration testing. This system activation is referred to as bootstrapping, from which point all CA activity is controlled and audited as per CP/CPS requirements. System testing of the platform consists of two major phases: pre-bootstrap component testing, and post-bootstrap end to end testing. Once pre and post bootstrap tests are completed, witnessed and signed off by DCC stakeholders, the SMKI moves into the user integration testing phase. Symantec and BT act in a supporting role during this phase, providing input into test activities where necessary and addressing any issues that arise.

5 Testing – Assurance

BT/Symantec will design a test plan which covers all requirements documented within the DCC SOR, together with any requirements arising from subsequent clarifications and discussions between BT and DCC. Each test case will reference one or more specific requirements. The test plan is presented to DCC for approval and adjusted as necessary before signoff.

The test plan includes the process for signing off each test case, including the DCC authorised witnesses, witness schedule and activities to be witnessed. Test results are entered for each test case, together with any relevant output data.

In order to streamline the test witnessing process, the test plan will be executed twice. The plan will first be executed by BT internally during the pre-bootstrap build phase. Once all tests are complete, the system is reinitialised and all test data removed, and the test plan is then executed a second time, with full witnessing by DCC stakeholders. Only when all tests are complete and witnessed will the system be signed over for user integration testing.

6 Pre-Integration testing

The SMKI platform will undergo a process of software implementation and configuration, followed by activation with live issuing CA keys. The activation of live CA keys is referred to as bootstrapping, from which point all CA activity is controlled and audited as per CP/CPS requirements.

System testing of the platform consists of two major phases: pre-bootstrap component testing, and post-bootstrap end to end testing. There is a standard CLP system test plan for the base platform, which is supplemented with test cases for any additional components and workflows specific to a particular implementation. This test plan is drafted during the pre-implementation phase, and agreed to by DCC prior to the professional services engagement.

The System test plan is executed twice. The first execution (pre bootstrap testing) occurs during initial setup to ensure that all components are operating correctly as they are installed and configured with test CA keys. Any issues arising during this phase which cannot be fixed immediately are raised with support and allocated a case number.

Once the software is operating correctly and all tests completed successfully, the system is reinitialized and cleaned of any test data before being activated with user integration live CA keys. The test plan is then executed a second time (post bootstrap testing), with each test case being witnessed by DCC.

Once all post bootstrap tests have been completed successfully, and to the satisfaction of DCC, the system as a whole is signed off as fully operational, and may be opened for Integration Testing.

7 Integration testing

BT and Symantec will work with DCC to build a service user facing test plan. This plan may be based on the workflow test cases included in the system test plan, and will include end to end testing of subscriber services, including registration, portal access, individual certificate request, batch certificate request and certificate pickup.

8 **Testing – Environments**

BT/Symantec will provide three physically separate PKI platforms to support the SMKI implementation.

The first is the development/reference PKI platform that BT/Symantec will use for its own internal system/pre-integration testing. This platform will be retained for the duration of the contract and will be used to test new release and enhancements to the service, should these be required, before these are deployed onto the either the DCC test or production environments.

The second is the DCC test environment, which will be provisioned for start of Pre-Integration Testing and which will be used to support DCC System Integration and User Integration testing. This platform will again by retained for the duration of the contract and will, following the completion of system and user integration testing, provide the enduring test environment that is required for business as usual (BAU) testing and to facilitate new entrant service user testing.

The third is the DCC production environment, which will be provisioned for the start User Integration testing on 1 April 2015 and will be replicated in a second secure site to ensure business continuity.

The DCC test environment will be located in the same secure site as one of the two production platforms and will be supported by the same operational team, but will be exist on physically separate hardware and share no common components. The test and production systems will make use of a shared data centre back-up solution

9 Testing – Defect Management

All incidents and defects reported to the BT Service Desk will be ticketed and the priority level agreed with DCC and regular updates provided in line with the agreed service levels until the incident is resolved or the defect corrected.

Where this requires a new release of any software component or a configuration change, BT will first deploy this onto its development/reference environment and execute a test plan that is commensurate with the complexity and scale of change, and its likely impact in event of failure.

BT/Symantec will share the results of this testing and, if appropriate, the roll-back plans for backing out the change in the event of problem, and obtain DCC agreement before rolling out the change onto the DCC test environment. This will enable DCC to perform any additional testing that might be required to ensure that the change has no adverse impact on the wider DCC eco-system.

BT/Symantec will advise DCC on the scope of testing that is needed for any change or new release and will recommend which subset of tests from the originally agreed user facing test plan should be performed before the change is rolled out onto the production environment.

Once DCC has completed and signed-off on these tests, BT will implement the change on the DCC production environment in a manner that minimises the impact on the overall SMKI service and at a time agreed with DCC.

Any changes to software components will be merged back in to the version managed product code repository. The details of the ticket will be recorded against the software component changed in the repository.

All changes will be supported by an appropriate documentation pack, which will include release notes detailing fixed tickets, completed test plans and, where appropriate, updates to any process and support documentation, User Guides and training materials.

Part L Service Management

1 BT operates an existing large scale operational service and believes that the complexity of the SMKI programme demands absolute adherence, by all service components providers, to a common Service Management protocol.

2 The ITIL framework is an ideal basis upon which to design and implement an integrated service model. BT underpins all new service provision with the ITIL best practice. Success in terms of SMKI delivery schedule and in-life operations will be determined by a coherent and binding strategy by all DCC providers across the entire service life-cycle.

3 The BT Service Manager would be responsible for working with the DCC Service Manager's during live operations to deliver the service metrics outlined in B8/SoR Appendix C for the DCC and its stakeholders.

4 Service Management - risks and mitigation

The key risks to effective Service Management for the SMKI programme need to be addressed at Service Strategy stage. It would arise from a fragmented approach to service provision by SMIP service providers with the 'big picture' out of focus or misaligned to the desired SMIP business outcomes. The consequences of such an approach include;

- Service providers adopting a 'silo' mentality towards service delivery.
- Functional IT delivery askew with Service delivery
- Communication channels are evoked in reaction to problems only.
- Service analytics are incoherent, incomplete and as a result incredulous.

To mitigate this risk the DSP, the CSP and SMKI suppliers must collaborate with Smart DCC in design and development of the service. It is imperative that this commence at the start of the PIT Phase.

BT would recommend that DCC appoint Service Champions from each of the providers who would consult and cooperate as a forum. At the Service Strategy stage of the service life-cycle the forum would liaise with service user representatives to agree and define the service. This definition would be the basis of the Service Level Agreement (SLA) between Smart DCC and the suppliers. The forum would also determine and obtain business/financial approval for service provision.

Following Service definition, the Service Champion forum would develop and publish clear and unambiguous Service stratagem to their respective Service Design teams. These teams will develop the Operational Level Agreements (OLA) that underpin and 'cost in' with the SLA.

Ineffectual or non-existent management during Service Transition phase is the primary cause of system and consequential business failure. The Service Champion forum would provide the core of the Change Approval Board (CAB) and ensure scope, risk and business benefits for all changes were aligned.

The Service Champion forum would retain its role in maintaining service awareness throughout the Service Operations. Quality information shared between service suppliers is the critical 'life-blood' of the SMIP service. A common service data portal is important but the establishment of business relationships should be given strategic priority as well. Regular operations forums are one means to this end.

As key drivers for Service Improvement initiatives, the Service Champion forum should determine the data that provides the best measure of service success and weakness. BT/Symantec recognises that this project is a complex large scale programme with high profile.