KPMG

The Directors
Trustis Limited
Boars Hill
Oxford
OX1 52Q
England

17 March 2004

Dear Sirs

Independent Auditor's Opinion on Management's Assertion Regarding the Root and Subordinate Key Generation Processes performed on the *23rd December 2003* and the 14th January 2004 for Trustis Ltd.

We have examined Trustis Ltd (Trustis) management assertions at Attachments B and C, that in generating and protecting The Trustis FPS Root Certificate Authority (CA) and Subordinate Certificate Authority (CA) keys performed on the 23rd of December 2003, and the 14th of January 2004 Trustis:

- Has conducted Root CA and Subordinate CA Key Generation, and Signing to the standards required by the Trustis FPS Root CA Certificate Policy.
- Documented its key generation and protection procedures in the relevant Certificate Policies (CP) and the Certification Practice Statement (CPS) for Trustis Ltd. As part of our review we looked at:
  - Trustis Certification Practice Statement, Version 1.0
  - Trustis FPS Root Certificate Policy, Version 1.03
  - Trustis FPS Certificate Policy, Version 1.03
- Included appropriate detailed procedures and controls in its Root CA and Subordinate CA Key Generation Scripts for Trustis FPS. As part of our review, the following procedures were reviewed:
  - CD-TIP-001-CA Build Instructions v6.1 Root CA
  - CD-TIP-001-CA Build Instructions v6.1 SubCA
  - T-TSC-FPS-AUDIT- Key Signing Matrix (Root and Simply Sign) v1.1

- T-TSC-FPS-Audit-Certificate Profiles (Root and SimplySign) v1.2
- CD-TIP-001-CA Build Instructions v6.2 FPSVCA
- T-TSC-FPS-AUDIT- Key Signing Matrix (Healthcare Sub CA) v1.0
- T-TSC-FPS-Audit-Certificate Profiles (Root and SimplySign) v1.2
- T-TSC-FPS-Audit-Certificate Profiles (Healthcare Sub CA) v1.0)
- T-adm-TSC-trustis-fps-root-PDS (Public Disclosure Statement) v1.03
- T-adm-tsc-Trustis FPS Simply Sign disclosure statement v1.0
- T-adm-tsc- Trustis FPS Healthcare disclosure v0.1

- Maintained effective controls to provide reasonable assurance that Trustis FPS Root CA and Subordinate CA keys were generated and protected in conformity with the procedures described in the Trustis FPS Root and Subordinate CA CPs and Trustis CPS and with the Key Generation Scripts; and
- Performed, during the key generation process, all the procedures required by the Key Generation Scripts;

based on the CA key generation criteria specified as part of Principle 2.1, Key Lifecycle Management Controls, of WebTrust for Certification Authorities, version 1.0 (Web Trust CA). Our assessment of the Key Lifecycle Management Controls is documented in Attachment C of Appendix 2.

Trustis Management is responsible for its assertions. Our responsibility is to express an opinion on management's assertions based on our examination.

Our examination included:

(1) Obtaining an understanding of Trustis' documented plan of procedures to be performed for the generation of the Root CA and Subordinate CA key pairs for the Trustis FPS CA Service (the "Key Generation Scripts");

(2) Examining the Key Generation Scripts;

(3) Assessing, during the key generation process, the effectiveness of controls over the integrity and confidentiality of all private keys (including back-up copies) and access keys (e.g., physical keys, tokens and passwords) used in the establishment of the Trustis CA service;

(4) Observing the performance of those procedures documented in the Key Generation Scripts.

We believe that our examination provides a reasonable basis for our opinion.

In our opinion, the managements assertions referred to above are fairly stated, in all material respects, based on the CA Key Generation Criteria, as set out in Web Trust CA.

KPMG

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of:

(1) Changes made to the system or controls;

(2) Changes in processing requirements;

(3) Changes required because of the passage of time; or

(4) A deterioration in the degree of compliance with the policies or procedures.

This report is intended solely for the information and use of the management of Trustis Ltd and Trustis FPS regarding the procedures performed by Trustis Ltd on the 23rd of December 2003 and the 14th of January 2004, to generate the Root CA and Subordinate CA keys for the Trustis FPS CA Service, and is not intended to be and should not be used by anyone other than these specified parties, without prior written approval by KPMG.

Malcolm Marshall
Partner
KPMG LLP

B Management's Assertion on Root CA Key generation for Trustis FPS

Management Assertion
CA Root Key Generation and Associated Procedures
Trustis Ltd FPS - PKI for Certificate Services.

Trustis Ltd FPS operates a number of certification authorities as part of PKI infrastructure support for customers. To support the infrastructure Trustis has created an Off Line root certificate authority that will be used to sign a number of subordinate operational CA's which will issue certificates to subscribers.

Trustis Ltd. generated the root key for this CA in the presence of auditors on 23 December 2003.

O= Trustis Limited
OU= Trustis FPS Root CA
Fingerprint = 3BC0 380B 33C3 F6A6 0C86 1522 93D9 DFF5 4B81 C004 (SHA-1)

Trustis Ltd is responsible for establishing and maintaining the procedures for Root Key generation, applying effective controls over the generation process and maintaining the integrity and confidentiality of all private keys and access keys (including physical keys, electronic tokens and passwords, or other shared secret information), used in the establishment of the Root Key, and for controls and procedures relevant to the generation and protection of the Root Key.

Trustis assesses the procedures and controls used for generation and protection of the root key. All operations are to standards compliant with BS7799 (ISO 17799) and tScheme[1]. All operations and their compliance with the declared standards are subject to independent audit and approval.

In respect of the above, Trustis Ltd Management asserts that the procedures and controls generation and protection of the root key detailed in this letter the following actions have been taken:-

- Trustis has documented the Trustis Root CA Key Generation and protection procedures in the relevant sections of the Trustis FPS Root CA Certificate Policy (T-adm-TSC-trustis-FPS-root-certificate-policy-v1.03, T-adm-TSC-trustis-fps-root-PDS-v1.03) and Trustis Certification Practice Statement, (T-ADM-Certification Practice Statement V1_0 - Trustis)
- Trustis has included appropriate detailed procedures and controls in the document: Key Generation Script for Trustis FPS (CD-TIP-001-CA Build Instructions v6.1 ROOT, CD-

[1] The UK scheme for Trust Service Assurance www.tscheme.org.uk

TIP-001-CA Build Instructions v6.1 SUBCA, T-TSC-FPS-AUDIT- Key Signing Matrix (Root and Simply Sign) v1.1, T-TSC-FPS-Audit-Certificate Profiles (Root and SimplySign) v1.2).

- Trustis maintained effective controls to provide reasonable assurance that Trustis Ltd Root CA Keys were generated and protected in conformity with the procedures described in the relevant sections of the Trustis FPS Root CA Certificate Policy and Trustis Certification Practice Statement and with the Key Generation Script for the Trustis FPS Root CA; and
- Trustis has performed, during the Root CA key generation process, all of the procedures required by the Key Generation Script for the Trustis FPS Root CA.

Trustis Ltd's management further asserts that criteria used for the for root key generation is either in accordance with Web Trust for Certification Authorities (V1.0) or at a minimum represents an equivalent standard of control, assurance and best practice.

Signed .....

Title TECHNICAL DIRECTOR

For Trustis Ltd ALAN T LIDDLE

C Management's Assertion on Subordinate CA Key generation for Trustis FPS

Management Assertion
CA Key Generation, Signing and Associated Procedures
Trustis Ltd. FPS - PKI for Certificate Services.

Trustis Ltd FPS operates a number of certification authorities as part of PKI infrastructure support for customers. To support the infrastructure Trustis has created an Off Line root certificate authority that will be used to sign a number of subordinate operational CA's, which will issue certificates to subscribers.

Establishing operational CAs includes generation of CA keys and signing of the operational CA by the Trustis FPS Root CA.

Trustis Ltd is responsible for establishing and maintaining the procedures for CA Key generation, applying effective controls over the generation process and maintaining the integrity and confidentiality of all private keys and access keys (including physical keys, electronic tokens and passwords, or other shared secret information), used in the establishment of the CA-key, and for controls and procedures relevant to the generation and protection of the CA and its CA-key.

Trustis assess the procedures and controls used for generation and protection of operational CA keys. All operations are to standards compliant with BS7799 (ISO 17799) and tScheme[2]. All operations and their compliance with the declared standards are subject to independent audit and approval.

In respect of the above, Trustis Ltd Management asserts that the procedures and controls generation and protection of CA keys the following actions have been taken:-

- Trustis has conducted the CA Key Generation and signing to the standards required by the Trustis FPS Root CA Policy
- Trustis has documented the Trustis CA Key generation, protection and signing procedures in the relevant sections of the Trustis FPS Root CA Certificate Policy T-adm-TSC-trustis-FPS-root-certificate-policy-v1.03, T-adm-TSC-trustis-fps-root-PDS-v1.03), the specific Governing Certificate Policy for each operational CA and Trustis Certification Practice Statement, (t-adm-tsc-trustis-fps-certificate-policy-v1.03, t-adm-tsc- Trustis FPS Healthcare disclosure-v0.1, t-adm-tsc-Trustis FPS Simply Sign disclosure statement v1.0, T-ADM-Certification Practice Statement V1_0 – Trustis)
- Trustis has included appropriate detailed procedures and controls in the document: Key Generation and CA Signing Script for Trustis FPS operational CAs

[2] The UK scheme for Trust Service Assurance www.tscheme.org.uk

- Trustis maintained effective controls to provide reasonable assurance that Trustis FPS CA Keys were generated and protected in conformity with the procedures described in the relevant sections of the Trustis FPS Root CA Certificate Policy and Trustis Certification Practice Statement and with the Key Generation and CA Signing Script for Trustis FPS operational CAs and
- Trustis has performed, during the CA key generation and signing process, all of the procedures required by the Key Generation and CA Signing Script for Trustis FPS operational CAs.

Trustis Ltd. management further asserts that criteria used for the for CA key generation and signing is in accordance with Web Trust for Certification Authorities (V1.0) or at a minimum represents an equivalent standard of control, assurance and best practice.

Signed .....

Title TECHNICAL DIRECTOR

For Trustis Ltd ALAN T LIDDLE

KPMG

The Directors
Trustis Limited
Boars Hill
Oxford
OX1 52Q
England

17 March 2004

Dear Sirs

Audit Report

We have examined Trustis Ltd ("Trustis") management assertions in Attachment B accompanying this report, regarding PKI and CA operations for Trustis. We have reviewed the PKI infrastructure for Certificate Services specifically focusing on the controls on Certificate Authority (CA) and PKI operations disclosure of business practices. This review was conducted against the following criteria from Web Trust for Certification Authorities V1.0 (Web Trust CA).

CA Business Practice Disclosures

Service Integrity

- Key Lifecycle Management Controls
  - CA Key Generation
  - CA Key Storage, Backup and Recovery
  - CA Cryptographic Hardware Lifecycle Management
  - CA Public Key Distribution
  - CA Key Usage

CA Environmental Controls

- Certification Practice Statement and Certificate Policy Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management

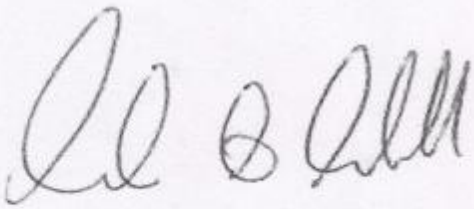
- Business Continuity Management
- Monitoring and Compliance
- Event Logging and Monitoring.

As a result of reviewing the adequacy of the documentation no instances of nonconformity were noted with the Trustis Limited management assertion that the relevant services are in accordance with the criteria defined in Web Trust CA or, at a minimum represents an equivalent level of control, assurance and best practice.

Attachment C sets out the three principles, related criteria and tests from Web Trust CA, together with results of the tests performed by KPMG.

Additional audit procedures are required to assess routine ongoing operational performance of Trustis against the declared management assertions from which an opinion on ongoing conformity with the procedures may be given.

This report is intended solely for the information and use of the Directors of Trustis Ltd regarding the procedures for the Trustis FPS CA Service, and is not intended to be and should not be used by anyone other than these specified parties, without prior written approval by KPMG.



Malcolm Marshall
Partner
KPMG LLP

B Trustis Ltd Management Assertion on PKI and CA Operations For Trustis FPS

Management Assertion
Trustis Ltd. FPS - PKI Infrastructure for Certificate Services.
Controls on CA and PKI Operations
Disclosure of Business Practices

Trustis Ltd. FPS operates a number of Certification Authorities (CAs) as part of PKI infrastructure support for customers. To support the infrastructure Trustis operates an Off Line Root CA and a number of Subordinate Operational CA's which issue certificates to subscribers.

The following services are provided.

- Subscriber Registration
- Certificate Issuance
- Certificate Life Cycle Management
- Subscriber Key Management (where applicable)[1]
- Certificate Renewal
- Certificate Rekey
- Certificate Distribution (where applicable)
- Certificate Suspension (where applicable)
- Certificate Revocation(where applicable)
- Certificate Status Promulgation

The management of Trustis Ltd is responsible for establishing and maintaining and, applying effective controls over the Trustis FPS PKI and Certificate Services, business practice disclosure (defined in the Governing Certificate Policy), service integrity (including key and certificate life cycle management controls) and CA environmental controls.

These controls contain mechanisms for management and monitoring and are subject to external audit. Where services (such as registration authority activities) are carried out by Third parties they are subjected to the controls and audit standards required by the Governing Certificate Policies. These controls contain monitoring mechanisms and actions are taken to correct deficiencies identified.

---

[1] Not all aspects of FPS certificate Services offer all these options

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provided only reasonable assurance with respect to Trustis' CA and PKI operations. The effective of controls may also vary over time.

Trustis management has assessed control over its FPS PKI certificate services. Based on the assessment it is the opinion of Trustis limited management in providing its FPS certification services that it has.

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  Subscriber information was properly authenticated (for the registration activities performed by Trustis-FPS CAs) and
  The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
  Subscriber and relying party information was controlled under the provisions of the UK Data Protection Act 1998
  The continuity of key and certificate life cycle management operations was maintained; and
  CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity
- Operated its relevant services in accordance with the Specification of Service Subject to Assessment (Trustis-CD-S3A-001 v1.4)
- Operated its relevant services and security management controls and processes in accordance with BS7799 (ISO 17799)

Trustis Ltd. management further asserts that it has operated the relevant services in accordance with criteria defined in Web Trust for Certification Authorities V1.0[2] or, at a minimum represents an equivalent standard of control, assurance and best practice.

Signed .....

Title TECHNICAL DIRECTOR

For Trustis Ltd ALAN T LIDDLE

[2] Relevant aspects of the Web Trust for Certification Authorities are provided as an Annex A to this letter.

Annex A to Trustis Ltd -Management's Assertion on PKI and CA Operations For Trustis FPS

CA Business Practices Disclosure
Service Integrity
Key Life Cycle Management Controls
- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls
- Certificate Issuance

CA Environmental Controls
- Certification Practice Statement and Certificate Policy Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Event Logging and Monitoring