Assertion of Management as to
its Disclosure of its Business Practices and its Controls Over
its Certification Authority Operations
during the period from March 1, 2009 through June 30, 2009

08/12/09

FernUniversität in Hagen, Zentrum für Medien und IT operates as a certification authority (CA) known as Scientific Trust. Scientific Trust, as a root CA, provides the following certification authority services:

- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate status information processing (using an online repository)

Management of Scientific Trust is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure [http://ca.fernuni-hagen.de/certserver/policy.php], service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective internal controls can provide only reasonable assurance with respect to Scientific Trust’s CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in Scientific Trust’s management’s opinion, in providing its CA services at Hagen, Scientific Trust, during the period from March 1, 2009 through June 30, 2009:

- 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 Scientific Trust); 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 restricted to authorized individuals and protected from uses not specified in the CA’s business practices disclosure;
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 based on the AICPA/CICA WebTrust for Certification Authorities criteria [http://www.icca.ca/services-et-produits/occasions-daffaires-pour-les-ca/services-trust-webtrust-systrust/item13385.pdf], including the following:

**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 Key Destruction
- CA Key Archival
- CA Cryptographic Hardware Life Cycle Management

**Certificate Life Cycle Management Controls**
- Subscriber Registration
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Status Information Processing

**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 Journaling

Ralph Knoche

Head of CA and Identity Management department