



**Assertion of the Directors as to its Disclosure of its  
Business Practices and its Controls Over its Certification Authority Operations  
during the period from January 1, 2008 through to March 31, 2008**

11 August, 2008

DigiCert, Inc (DigiCert) operates as a Certification Authority (“CA”) known as DigiCert Security Services CA. DigiCert, as a Root CA, provides the following certification authority services:

- Subscriber registration
- Certificate renewal
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

The Directors of DigiCert are responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its **Certification Practice Statement** on its website, 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 controls can provide only reasonable assurance with respect to DigiCert’s Certification Authority operations. Furthermore because of changes in conditions, the effectiveness of controls may vary over time.

The Directors have assessed the controls over its CA operations. Based on that assessment, in the Directors of DigiCert, Inc.’s opinion, in providing its Certification Authority (CA) services at Lindon, Utah USA, DigiCert, Inc, during the period from January 1, 2008 through to March 1, 2008:

- 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 DigiCert, Inc); 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 authorised 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 authorised and performed to maintain CA systems integrity;

based on the AICPA/CICA WebTrust for Certification Authorities Criteria 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 Renewal  
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

Ken Bretschneider  
Chief Executive Officer





**KPMG LLP**  
1 The Embankment  
Neville Street  
Leeds LS1 4DW  
United Kingdom

Tel +44 (0) 113 231 3000  
Fax +44 (0) 113 231 3200  
DX 724440 Leeds

Ken Bretschneider  
President/CEO  
DigiCert Inc  
335 South 520 West  
Canopy Building II, Suite 200  
Lindon, UT 84042  
USA

Our ref **wm/jc/637**  
Contact **Warren Middleton**  
Tel + 44 113 231 3646

11 August 2008

Dear Sirs

### **Report in relation to the WebTrust for Certification Authorities Criteria**

In accordance with the terms of our engagement letter dated 2<sup>nd</sup> May 2008 and further to our license to do such work issued to us by the AICPA/CICA, we have examined the assertion by the Directors of DigiCert Inc (“the Company”) <http://www.digicert.com/ssl-cps-repository.htm> that in providing its Certification Authority (“CA”) services at Utah, during the period from 1<sup>st</sup> January 2008 through to 31<sup>st</sup> March 2008 the Company has:

- Disclosed its key and certificate life cycle management business and information privacy practices <http://www.digicert.com/ssl-cps-repository.htm> 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 the Company); 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 authorised 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 authorised and performed to maintain CA systems integrity.

based on the AICPA/CICA WebTrust for Certification Authorities Criteria  
[http://www.webtrust.org/certauth\\_fin.htm](http://www.webtrust.org/certauth_fin.htm).



The Directors of the Company have sole responsibility for their assertion. Our responsibility under the terms of our engagement letter is to form an opinion on management's assertion, on the basis of the work performed, and report our opinion.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and accordingly included (1) obtaining an understanding of the Company's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion for the period 1<sup>st</sup> January 2008 through to 31<sup>st</sup> March 2008, the Company's Directors' assertion, as set forth in the first paragraph, is fairly stated in all material respects, based on the AICPA/CICA WebTrust for Certification Authorities Criteria.

Because of inherent limitations in controls, errors 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, (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures, may alter the validity of such conclusions.

The WebTrust seal of assurance for Certification Authorities on the Company's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at the Company and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.



This report does not include any representation as to the quality of the Company's services beyond those covered by the WebTrust for Certification Authorities Criteria, nor the suitability of any of the Company's services for any customer's intended purpose.

Yours faithfully

KPMG LLP

**KPMG LLP**  
11 August 2008