January 11, 2012

Dear PMA,

We are currently in the process of amending our CPS to more accurately describe our Client Certificate policies. We expect to release the new CPS later this year. Some of these revisions will clarify IGTF certificate policies and likely clarify some of the questions raised about DigiCert's application for accreditation, we'd thought you' give you advanced notice of the changes related to IGTF Certificates.

We plan on adding the following language to our CPS:

1. Section 1.2 Document Name And Identification – The following OIDs are assigned to identify certificates issued according to IGTF Classic profile with secured infrastructure:

Grid Client certificate with Public Trust	2.16.840.1.114412.4.31.1
Grid Client certificate with Grid-only Trust	2.16.840.1.114412.31.4.1.1
Grid Host certificate with Public Trust	2.16.840.1.114412.1.31.1
Grid Host certificate with Grid-only Trust	2.16.840.1.114412.31.1.1.1

2. Section 1.3.2 Registration Authorities - For IGTF certificates, a designated RA is responsible for vetting the identity of each certificate applicant.

3. Section 1.3.5 Other Participants - Other participants include Accreditation Authorities (such as the PMA and Federation for IGTF certificates and the applicable community sponsorship for EU certificates); Bridge CAs and CAs that cross-certify DigiCert CAs as trust anchors in other PKI communities; Card Management Systems and integrators (CMSs) that ensure proper operation and provisioning of PIV-I cards; and Time Source Entities, Time Stamp Token Requesters, and Time Stamp Verifiers involved in trusted timestamping. Accreditation Authorities are granted an unlimited right to re-distribute DigiCert's root certificates and related information in connection with the accreditation.

4. Section 2.1 Repositories - DigiCert publishes its root certificates, revocation data for issued digital certificates, CPs, CPSs, Relying Party Agreements, and standard Subscriber Agreements in DigiCert's repositories which are publicly available through the web at http://www.DigiCert-Grid.com/.

5. Section 3.1.5 Uniqueness of Name – Added:

IGTF Certificates	For device certificates, a unique name is included in the DN fields. For individuals, DigiCert may append a unique user ID to the name listed in the CN field. E.G. If there are 4 unique subjects all called Scott Rea, then the following may be an appropriate representation of how each may be uniquely identified in the Common Name element of the DN: 1. Scott Rea 2. Scott A. Rea 3. Scott Rea 25643 4. Scott Rea 98671

6. Section 3.2.3.1 Authentication for Role-based Client Certificates - IGTF and EU Qualified Certificates are not issued as role-based certificates.

7. Section 3.2.3.3 Authentication for Group Client Certificates - IGTF and EU Qualified Certificates are not issued as role-based certificates.

8. Section 3.3.1 Identification and Authentication for Routine Re-Key – For IGTF added the following method of re-authentication: Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated private key

9. Section 4.9.1 Circumstances for Revocation - Subscribers are required to request revocation as soon as possible (within one day after detection) if the Private Key corresponding to the Certificate is lost or compromised or if the data in the certificate is no longer valid.

10. Section 5.5.1 Types of Records Archived - Sufficient identity authentication data to satisfy the identification requirements of Section 3.2

11. Section 6.1.4 CA Public Key Delivery to Relying Parties - All accreditation authorities supporting DigiCert certificates and all application software providers are permitted to redistribute DigiCert's root anchors.

12. Section 6.2.1 Cryptographic Module Standards and Controls - IGTF Certificate Subscribers must protect their Private Keys in accordance with the applicable Guidelines on Private Key Protection, including the use of strong pass phrases to protect private keys.

13. Section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods - IGTF signing certificates have a lifetime that is at least twice the maximum lifetime of an end entity certificate.

14. Section 7.1.2 Certificate Extensions - IGTF certificates comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

15. Section 9.6.3 Subscriber Representations and Warranties - Subscribers are required to notify DigiCert and any applicable RA if any change occurs that could affect the status of the Certificate

16. Section 9.12.2 Notification Mechanism and Period - Major changes affecting accredited certificates are announced and approved by the accrediting agency prior to becoming effective.

All of these changes will become effective after adopted by the DigiCert Policy Authority and after the PMA's approval. Please let us know if you have any concerns with these changes.

Sincerely yours,

DIGICERT, INC.