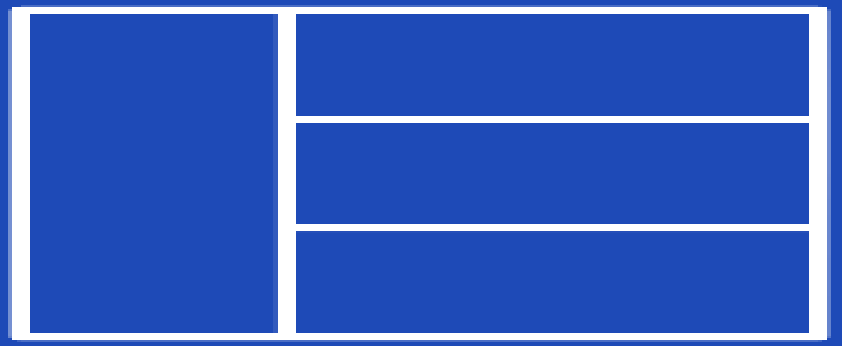
DIGITALTRUST

DIGITALTRUST IGTF CA Classic Accreditation

Level 12, Aldar HQ, Abu Dhabi,
United Arab Emirates

01



DigitalTrust & IGTF

DIGITALTRUST & IGTF

- Ankabut in the UAE
  - The Ankabut Project is the UAE Advance Network for Research and Education
  - Founded in August 2006 by Khalifa University, Institute of Applied Technology, United Arab Emirates University, Zayed University and Higher Colleges of Technology
  - Currently has 26 Universities as participating members
  - Ankabut to provide members access to National Grid Initiatives and also EGI participation
- DigitalTrust (previously DarkMatter Trust Services) primarily sought IGTF Accreditation so it would be in a position to provide Ankabut services needed to participate in target initiatives
  - Potentially not required for national grid initiatives but why not kill two birds with one stone?
  - Today Ankabut internally is primarily using a lower level of authentication than certificates
- DigitalTrust is open to providing certificate services to other national grid communities
  - Today, Public Trust grid certs are only issued within UAE
  - IGTF or Private Trust grid certs can be issued globally if desired by contract of appropriate RA
  - Public Trust grid certs can be facilitated for any global location

DIGITALTRUST & IGTF

- DigitalTrust is currently IGTF accredited for 3 Classic CAs
  - Public Trust Originally audited QV CP/CPS operated with DT RAs, now audited under DT CP/CPS & RAs
    - DarkMatter Assured CA (Grid Client)
    - DarkMatter Secure CA (Grid Host)
  - IGTF Trust Only (Private Trust) audited under DT CP/CPS & RAs
    - DarkMatter Private Root CA G4 (Private Root)
    - DarkMatter IGTF CA (Grid Host and Grid Client)

- Introducing New IGTF Options for DigitalTrust
  - Two New Global public trust CAs to be introduced soon…
  - New IGTF Trust Only hierarchy being submitted for accreditation now

New DIGITALTRUST IGTF Public Trust Anchors

- DigitalTrust is seeking to add to its' currently IGTF accredited Public Trust Classic CAs
  - Public Trust via QV subCAs now operated and audited under DT CP/CPS & RAs have limited ubiquity due to Google & Microsoft decisions to distrust. Subs are still trusted in Mozilla and Apple. NOTE: Mozilla has notified of intended distrust action also, but on hold currently due to DigitalTrust's appeal.
    - The two existing DarkMatter subCAs (1 for Grid Client, 1 for Grid Host) will be superseded with two DigitalTrust subCAs (1 for Grid Client, 1 for Grid Host) that will be publicly trusted via cross-sign and operated by trust partner.
    - DigitalTrust will operate as a Grid RA for the purpose of Grid cert issuance, and is currently undergoing new WebTrust for RAs Audit as part of current audit expected to be completed this month.
    - Expect the new public trust subCAs to be available in Q3 2019 (next month)
    - The CA operations will be WebTrust audited to BRs & CA
    - We are seeking to prime the pump now for review of these subs as soon as they are available.

New DIGITALTRUST IGTF Trust Anchors

- DigitalTrust is seeking to add to its' currently private trust IGTF accredited Classic CAs
  - IGTF Trust Only (Private Trust) audited under DT CP/CPS & RAs currently has the following HLCA & Classic CA
    - DarkMatter Private Root CA G4 (Private Root)
    - DarkMatter IGTF CA (Grid Host and Grid Client)
  - DigitalTrust wishes to introduce and accredit the following New HLCA & Classic CA also operated under the DT CP/CPS & RAs
    - **DigitalTrust Private Root CA G4** (Private Root) [HLCA]
    - **DigitalTrust IGTF CA** (Grid Host and Grid Client) [Classic CA]
    - Same infrastructure, same policies, same procedures, same trusted personnel, just a new hierarchy
    - In part to transition completely to the DigitalTrust namespace, eventually the DarkMatter hierarchy will be retired

New DIGITALTRUST HLCA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            05:b0:ca:a5:f9:ef:4c:08:72:e4:e0:9d:32:6a:de:3e
    Signature Algorithm: sha384WithRSAEncryption
        Issuer: C=AE, O=DigitalTrust L.L.C., CN=DigitalTrust Private Root CA G4
        Validity
            Not Before: Aug  1 11:01:27 2019 GMT
            Not After : Aug  1 11:01:27 2039 GMT
        Subject: C=AE, O=DigitalTrust L.L.C., CN=DigitalTrust Private Root CA G4
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                5D:CE:AF:4F:F3:9C:5C:CC:B7:C3:3C:5E:46:A8:A6:7C:B9:6A:C6:AD
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

New DIGITALTRUST Classic CA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            14:62:69:dd:fe:56:11:46:3e:60:54:d4:3d:0e:52:30
    Signature Algorithm: sha384WithRSAEncryption
        Issuer: C=AE, O=DigitalTrust L.L.C., CN=DigitalTrust Private Root CA G4
        Validity
            Not Before: Aug  1 11:15:21 2019 GMT
            Not After : Aug  1 11:15:21 2029 GMT
        Subject: C=AE, O=DigitalTrust L.L.C., CN=DigitalTrust IGTF CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)

        X509v3 extensions:
            Authority Information Access:
                CA Issuers - URI:http://cacerts.digitaltrust.ae/DigitalTrustPrivateRootCAG4.crt
                OCSP - URI:http://ocsp.digitaltrust.ae

            X509v3 Subject Key Identifier:
                C7:27:81:18:2D:83:52:27:F5:6F:4A:49:76:46:FA:9D:4D:3B:71:71
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Authority Key Identifier:
                keyid:5D:CE:AF:4F:F3:9C:5C:CC:B7:C3:3C:5E:46:A8:A6:7C:B9:6A:C6:AD

            X509v3 Certificate Policies:
                Policy: 2.16.784.2.2.41.2.0.2.1
                  CPS: https://ca.digitaltrust.ae/CPS
                Policy: 2.16.784.2.2.41.2.2.3.1
                Policy: 2.16.784.2.2.41.2.2.3.2
                Policy: 2.16.784.2.2.41.2.2.3.3

X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl1.digitaltrust.ae/DigitalTrustPrivateRootCAG4.crl

                Full Name:

URI:http://crl2.digitaltrust.ae/DigitalTrustPrivateRootCAG4.crl

            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection,
1.3.6.1.4.1.311.10.3.12, OCSP Signing, TLS Web Server
Authentication
```

New DIGITALTRUST Classic CA Namespace

```
############################################################################
#NAMESPACES-VERSION: 1.0
#
# @(#)7f23888f.namespaces
# CA alias    : DigitalTrustIGTFCA
#    subord_of: DigitalTrustPrivateRootCAG4
#    subjectDN: /C=AE/O=DigitalTrust L.L.C./CN=DigitalTrust IGTF CA
#    hash     : 7f23888f

TO Issuer "/C=AE/O=DigitalTrust L.L.C./CN=DigitalTrust IGTF CA" \
  PERMIT Subject "/C=AE/O=DigitalTrustGrid/.*"

TO Issuer "/C=AE/O=DigitalTrust L.L.C./CN=DigitalTrust IGTF CA" \
  PERMIT Subject "/DC=com/DC=DigitalTrustGrid/.*"

TO Issuer "/C=AE/O=DigitalTrust L.L.C./CN=DigitalTrust IGTF CA" \
  PERMIT Subject "/DC=org/DC=DigitalTrustGrid/.*"
```

New DIGITALTRUST Grid Repository

https://digitaltrustgrid.ae/Grid/index.html

DIGITALTRUST

DigitalTrust PKI Services Grid Repository

DigitalTrust is an accredited IGTF Certification Authority via EUGridPMA.
DigitalTrust operates the DarkMatter Grid CAs, and is now seeking further accreditation of new DigitalTrust Grid CAs.

In June 2016, DarkMatter/DigitalTrust launched it's PKI Services when it created a number of Trust Anchors (root and sub CAs) for the provisioning of certificates.
DigitalTrust has two different hierarchies for the issuance of IGTF accredited grid certificates - one hierarchy that operates only within the IGTF (there are two chains, one for DarkMatter IGTF CA - already accredited, and an additional one accreditation is currently being sought for - DigitalTrust IGTF CA), and another hierarchy that chains to publicly trusted Root CAs (this hierarchy is already accredited since January 2017).

DigitalTrust is currently seeking the accreditation of the Private Trust IGTF ONLY hierarchy for the DigitalTrust IGTF CA.

DigitalTrust/DarkMatter Grid Public Trust CAs

Host Hierarchy

- **QuoVadis Root CA 2 G3** Off-line publicly trusted Root that signs subordinate CAs. This Root is intended to be Trusted for Host Certificates as part of the IGTF Classic distribution.
  CA Certificate: QuoVadis Root CA 2 G3.cer | QuoVadis Root CA 2 G3.der | 1f58a078.0
  Signing Policy: QuoVadisRootCA2G3.signing_policy | 1f58a078.signing_policy
  Namespace: QuoVadisRootCA2G3.namespaces | 1f58a078.namespaces
  Certificate Revocation List: DER format (QuoVadisRootCA2G3.crl)
  CA.info Link: QuoVadisRootCA2G3.info | 1f58a078.info
  CA.crl_url Link: QuoVadisRootCA2G3.crl_url
  CA Text Link: QuoVadisRootCA2G3.txt

- **DarkMatter Secure CA** On-line Subordinate CA to provide long-term user, host and service certificates. This sub-CA is Accredited as part of the IGTF Classic distribution.
  CA Certificate: DarkMatterSecureCA.cer | DarkMatterSecureCA.der | a69c3a14.0
  Signing Policy: DarkMatterSecureCA.signing_policy | a69c3a14.signing_policy
  Namespace: DarkMatterSecureCA.namespaces | a69c3a14.namespaces
  Certificate Revocation List: DER format (DarkMatterSecureCA.crl)
  CA.info Link: DarkMatterSecureCA.info | a69c3a14.info
  CA.crl_url Link: DarkMatterSecureCA.crl_url
  CA Text Link: DarkMatterSecureCA.txt

Client Hierarchy

- **QuoVadis Root CA 3 G3** Off-line publicly trusted Root that signs subordinate CAs. This Root is intended to be Trusted for Client Certificates as part of the IGTF Classic distribution.
  CA Certificate: QuoVadis Root CA 3 G3.cer | QuoVadis Root CA 3 G3.der | e442e424.0
  Signing Policy: QuoVadisRootCA3G3.signing_policy | e442e424.signing_policy
  Namespace: QuoVadisRootCA3G3.namespaces | e442e424.namespaces
  Certificate Revocation List: DER format (QuoVadisRootCA3G3.crl)
  CA.info Link: QuoVadisRootCA3G3.info | e442e424.info
  CA.crl_url Link: QuoVadisRootCA3G3.crl_url
  CA Text Link: QuoVadisRootCA3G3.txt

New DIGITALTRUST Grid Repository

https://digitaltrustgrid.ae/Grid/index.html

DigitalTrust Grid Private Trust CAs

IGTF Only Trust Hierarchy - Host, robot and client

- **DigitalTrust Private Root CA G4** Off-line private trusted Root that signs subordinate CAs. This Root is intended to be Trusted for Host, Robot and Client Certificates as part of the IGTF Classic distribution.
  CA Certificate: DigitalTrust Private Root CA G4.cer | DigitalTrust Private Root CA G4.crt | d58bb4bc.0
  Signing Policy: DigitalTrustPrivateRootCAG4.signing_policy | d58bb4bc.signing_policy
  Namespace: DigitalTrustPrivateRootCAG4.namespaces | d58bb4bc.namespaces
  Certificate Revocation List: DER format (DigitalTrustPrivateRootCAG4.crl)
  CA.info Link: DigitalTrustPrivateRootCAG4.info | d58bb4bc.info
  CA.crl_url Link: DigitalTrustPrivateRootCAG4.crl_url
  CA Text Link: DigitalTrustPrivateRootCAG4.txt

- **DigitalTrust IGTF CA** On-line Subordinate CA to provide long-term user, host and service certificates. This sub-CA is Accredited as part of the IGTF Classic distribution.
  CA Certificate: DigitalTrustIGTFCA.cer | DigitalTrustIGTFCA.crt | 7f23888f.0
  Signing Policy: DigitalTrustIGTFCA.signing_policy | 7f23888f.signing_policy
  Namespace: DigitalTrustIGTFCA.namespaces | 7f23888f.namespaces
  Certificate Revocation List: DER format (DigitalTrustIGTFCA.crl)
  CA.info Link: DigitalTrustIGTFCA.info | 7f23888f.info
  CA.crl_url Link: DigitalTrustIGTFCA.crl_url
  CA Text Link: DigitalTrustIGTFCA.txt

DarkMatter/DigitalTrust Grid Certificate Policies, Practices, and Profiles

- **CP**: click-here
- **CPS**: CPS V1.11 pdf

We are here, 24/7, to help you with any Grid certificate support questions you might have.

Support Toll Free: 800-3275-2378 (UAE)

Support Direct: +971-2-417-1483

Email: pki-support@DigitalTrust.ae

Grid Certificate Support around the Clock!

Our support pages have been designed with both the network administrator and novice in mind. Our **Grid Certificate Support** pages provide step-by-step details for each of the most common web server applications used today. If yours is not listed, contact a support technician for further help.

DigitalTrust Contact Address:

DigitalTrust LLC
Level 12, AlDar HQ
P.O. Box 113979
Abu Dhabi, United Arab Emirates
T: +971-2-417-1483
W: https://www.digitaltrust.ae/

DarkMatter IGTF CAs

1 DT Public Trust

- IGTF HOST Classic CA provider created 2016, accredited January 2017: **DarkMatter Secure CA**
  - QV CP/CPS + DT RA
  - DT CP/CPS & RAs
- IGTF CLIENT Classic CA provider created 2016, accredited January 2017: **DarkMatter Assured CA**
  - QV CP/CPS + DT RA
  - DT CP/CPS & RAs
- 2 New CAs coming soon

2 DT IGTF Private

- IGTF CLIENT and HOST Classic CA provider created 2017, accredited 2018:
- **DarkMatter IGTF CA**
  - DT CP/CPS & RAs
- Seeking Accreditation of:
  - **DigitalTrust IGTF CA** issued by the **DigitalTrust Private Root CA G4**
  - Same CP/CPS & RAs
  - Namespace adjustment

3 DT Audits

- **DigitalTrust LLC** has now assumed all operations and contracts of the previous DarkMatter Trust Services
- Existing DT IGTF accredited CAs successfully completed self-audit review at last IGTF meeting
- Current WebTrust audits are being completed under **DigitalTrust LLC** and will include the new WebTrust RA certification

4 DigitalTrust IGTF

- **DigitalTrust LLC** is now the IGTF Member
- Same personnel, same infrastructure, same locations, same policies and processes, different legal entity
- 3rd annual WebTrust Audit almost completed now with **DigitalTrust** as the asserting entity
- Namespace adjustment request pending with the new private trust hierarchy

Questions?

Scott Rea
Head of **DigitalTrust**
Level 12, Aldar HQ
PO Box 113979
Abu Dhabi, UAE

https://digitaltrust.ae