DIGITALTRUST

DIGITALTRUST IGTF CAs Updates

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

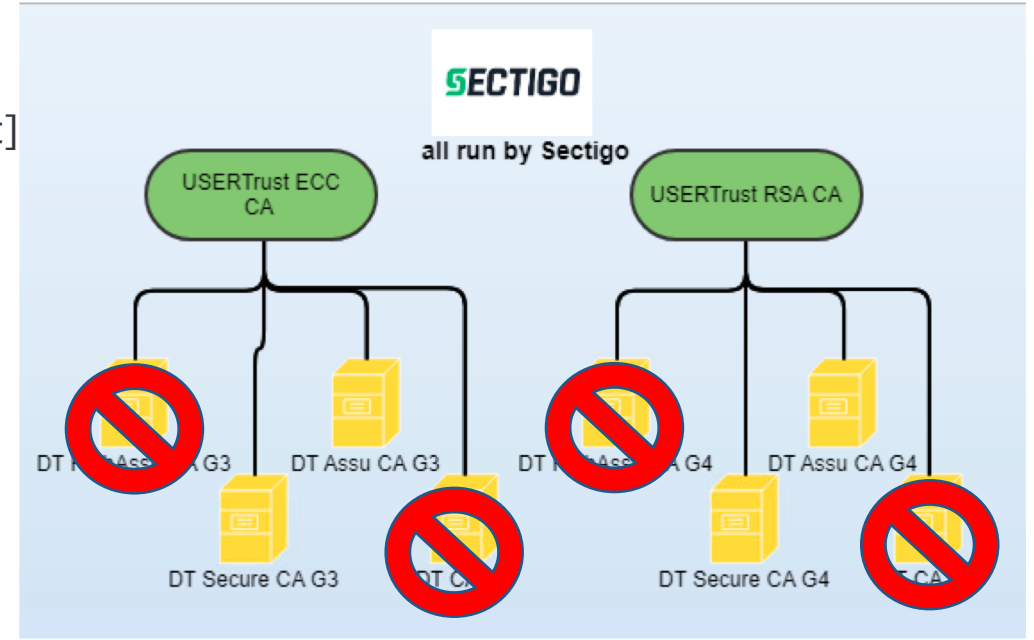
DIGITALTRUST & IGTF

- DigitalTrust acquired by Digital14 on Jan 1st, 2020
  - DigitalTrust Private Grid hierarchy updated in Karlsruhe 2019
  - Request to add new commercial hierarchy for DigitalTrust when subCAs are ready also presented in Karlsruhe 2019
    - This presentation is finalizing and formalizing the Public Trust hierarchy
    - Retirement of QuoVadis chain
    - Adding of Sectigo chain

- DigitalTrust is open to providing certificate services to 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 IGTF Classic accredited Public Trust CAs to be updated in the distribution
  - QV legacy chain is now removed, subCAs are revoked, key destruction audits available
  - New Sectigo Public Trust chains to be added to the distribution:
    - HLCA's x2 [ECC and RSA based hierarchies]
      - USERTrust ECC Certification Authority
      - USERTrust RSA Certification Authority
    - Classic CAs x 4 [2x ECC and 2x RSA based, Host+Client split]
      - ECC:
        - DigitalTrust Secure CA G3 [Run by the Issuer]
        - DigitalTrust Assured CA G3 [Run by the Issuer]
      - RSA
        - DigitalTrust Secure CA G4 [Run by the Issuer]
        - DigitalTrust Assured CA G4 [Run by the Issuer]



New DIGITALTRUST HLCA – Leveraging Sectigo ECC Anchor

Certificate:
- Data:
  - Version: 3 (0x2)
  - Serial Number: 5c:8b:99:c5:5a:94:c5:d2:71:56:de:cd:89:80:cc:26
- Signature Algorithm: ecdsa-with-SHA384
  - Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority
  - Validity
    - Not Before: Feb 1 00:00:00 2010 GMT
    - Not After : Jan 18 23:59:59 2038 GMT
  - Subject: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority
  - Subject Public Key Info:
    - Public Key Algorithm: id-ecPublicKey Public-Key: (384 bit); ASN1 OID: secp384r1; NIST CURVE: P-384
  - X509v3 extensions:
    - X509v3 Subject Key Identifier: 3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A
    - X509v3 Key Usage: critical Certificate Sign, CRL Sign
    - X509v3 Basic Constraints: critical CA:TRUE

New DIGITALTRUST HLCA – Leveraging Sectigo RSA Anchor

Certificate:
- Data:
  - Version: 3 (0x2)
  - Serial Number: 01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d
- Signature Algorithm: sha384WithRSAEncryption
  - Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
  - Validity
    - Not Before: Feb 1 00:00:00 2010 GMT
    - Not After : Jan 18 23:59:59 2038 GMT
  - Subject: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
  - Subject Public Key Info:
    - Public Key Algorithm: rsaEncryption Public-Key: (4096 bit) Modulus; Exponent: 65537 (0x10001)
  - X509v3 extensions:
    - X509v3 Subject Key Identifier: 53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
    - X509v3 Key Usage: critical Certificate Sign, CRL Sign
    - X509v3 Basic Constraints: critical CA:TRUE

New DIGITALTRUST Classic CA – Host/Service ECC

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0e:0b:fc:6f:8e:0b:ec:ac:61:60:e2:7b:91:ff:ff:c8
Signature Algorithm: ecdsa-with-SHA384
Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority
Validity
Not Before: Jan 8 00:00:00 2020 GMT
Not After : Jan 7 23:59:59 2030 GMT
Subject: **C=AE, O=Digital Trust L.L.C., CN=DigitalTrust Secure CA G3 [Run by the Issuer]**
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (384 bit); ASN1 OID: secp384r1; NIST CURVE: P-384
X509v3 extensions:
X509v3 Authority Key Identifier:
keyid:3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A
X509v3 Subject Key Identifier: 1F:BF:53:06:F1:4D:31:86:80:63:95:20:F0:45:C1:35:97:65:A8:46
X509v3 Key Usage: critical Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical CA:TRUE, pathlen:0
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.6449.1.2.2.77
Policy: 2.23.140.1.2.2
X509v3 CRL Distribution Points:
Full Name: URI:http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl
Authority Information Access:
CA Issuers - URI:http://crt.usertrust.com/USERTrustECCAddTrustCA.crt
OCSP - URI:http://ocsp.usertrust.com

New DIGITALTRUST Classic CA Namespace – Host/Service ECC

```
##############################################################################
#NAMESPACES-VERSION: 1.0
#
# @(#)d9343743.namespaces
# CA alias    : DigitalTrustSecureCAG3-runbytheissuer
#    subord_of: USERTrustECCCertificationAuthority
#    subjectDN: /C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G3  [Run by the Issuer]
#    hash     : d9343743

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G3  [Run by the Issuer]" \
  PERMIT Subject "/C=AE/O=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G3  [Run by the Issuer]" \
  PERMIT Subject "/DC=com/DC=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G3  [Run by the Issuer]" \
  PERMIT Subject "/DC=org/DC=DigitalTrustGrid/*"
```

New DIGITALTRUST Classic CA – Host/Service RSA

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 8e:fc:a7:34:7b:3a:ed:10:0b:c0:49:96:30:49:cc:f4
Signature Algorithm: sha384WithRSAEncryption
Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
Validity
Not Before: Jan 8 00:00:00 2020 GMT
Not After : Jan 7 23:59:59 2030 GMT
Subject: **C=AE, O=Digital Trust L.L.C., CN=DigitalTrust Secure CA G4 [Run by the Issuer]**
Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (4096 bit) Modulus;Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier: keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
X509v3 Subject Key Identifier: 1B:7E:7B:B5:E9:DE:A0:C5:94:45:51:89:8D:43:4E:F5:48:4E:B5:B9
X509v3 Key Usage: critical Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical CA:TRUE, pathlen:0
X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.6449.1.2.2.77
Policy: 2.23.140.1.2.2 X509v3
CRL Distribution Points:
Full Name: URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
Authority Information Access:
CA Issuers - URI:http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt
OCSP - URI:http://ocsp.usertrust.com

New DIGITALTRUST Classic CA Namespace – Host/Service RSA

```
##############################################################################
#NAMESPACES-VERSION: 1.0
#
# @(#)943fd5f3.namespaces
# CA alias    : DigitalTrustSecureCAG4-runbytheissuer
#    subord_of: USERTrustRSACertificationAuthority
#    subjectDN: /C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G4  [Run by the Issuer]
#    hash     : 943fd5f3

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G4  [Run by the Issuer]" \
  PERMIT Subject "/C=AE/O=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G4  [Run by the Issuer]" \
  PERMIT Subject "/DC=com/DC=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Secure CA G4  [Run by the Issuer]" \
  PERMIT Subject "/DC=org/DC=DigitalTrustGrid/*"
```

New DIGITALTRUST Classic CA – Client/Robot ECC

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 7d:2c:0c:f1:4c:97:d4:89:5d:c2:9b:ea:d0:6d:c1:cb
Signature Algorithm: ecdsa-with-SHA384
Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust ECC Certification Authority
Validity
Not Before: Jan 8 00:00:00 2020 GMT
Not After : Jan 7 23:59:59 2030 GMT
Subject: **C=AE, O=Digital Trust L.L.C., CN=DigitalTrust Assured CA G3 [Run by the Issuer]**
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey Public-Key: (384 bit) pub: ASN1 OID: secp384r1 NIST CURVE: P-384
X509v3 extensions:
X509v3 Authority Key Identifier: keyid:3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A
X509v3 Subject Key Identifier: 1A:20:25:6C:33:92:99:FD:15:EE:8B:00:DA:34:73:0F:33:27:A1:12
X509v3 Key Usage: critical Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical CA:TRUE, pathlen:0
X509v3 Extended Key Usage: TLS Web Client Authentication, E-mail Protection
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.6449.1.2.2.77
X509v3 CRL Distribution Points:
Full Name: URI:http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl
Authority Information Access:
CA Issuers - URI:http://crt.usertrust.com/USERTrustECCAddTrustCA.crt
OCSP - URI:http://ocsp.usertrust.com

New DIGITALTRUST Classic CA Namespace – Client/Robot ECC

```
##############################################################################
#NAMESPACES-VERSION: 1.0
#
# @(#)a883462e.namespaces
# CA alias    : DigitalTrustAssuredCAG3-runbytheissuer
#    subord_of: USERTrustECCCertificationAuthority
#    subjectDN: /C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G3  [Run by the Issuer]
#    hash     : a883462e

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G3  [Run by the Issuer]" \
  PERMIT Subject "/C=AE/O=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G3  [Run by the Issuer]" \
  PERMIT Subject "/DC=com/DC=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G3  [Run by the Issuer]" \
  PERMIT Subject "/DC=org/DC=DigitalTrustGrid/*"
```

New DIGITALTRUST Classic CA – Client/Robot RSA

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0f:bb:f3:c6:87:f6:a4:a9:95:e2:11:16:98:e7:9f:92
Signature Algorithm: sha384WithRSAEncryption
Issuer: C=US, ST=New Jersey, L=Jersey City, O=The USERTRUST Network, CN=USERTrust RSA Certification Authority
Validity
Not Before: Jan 8 00:00:00 2020 GMT
Not After : Jan 7 23:59:59 2030 GMT
Subject: **C=AE, O=Digital Trust L.L.C., CN=DigitalTrust Assured CA G4 [Run by the Issuer]**
Subject Public Key Info:
Public Key Algorithm: rsaEncryption Public-Key: (4096 bit) Modulus; Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Authority Key Identifier: keyid:53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB
X509v3 Subject Key Identifier: F6:8A:69:AE:70:D8:59:ED:3D:2D:39:44:9F:AB:B7:00:19:CB:8F:18
X509v3 Key Usage: critical Digital Signature, Certificate Sign, CRL Sign
X509v3 Basic Constraints: critical CA:TRUE, pathlen:0
X509v3 Extended Key Usage: TLS Web Client Authentication, E-mail Protection
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.6449.1.2.2.77
X509v3 CRL Distribution Points:
Full Name: URI:http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl
Authority Information Access:
CA Issuers - URI:http://crt.usertrust.com/USERTrustRSAAddTrustCA.crt
OCSP - URI:http://ocsp.usertrust.com

New DIGITALTRUST Classic CA Namespace – Client/Robot RSA

```
############################################################################
#NAMESPACES-VERSION: 1.0
#
# @(#)3e0d64db.namespaces
# CA alias    : DigitalTrustAssuredCAG4-runbytheissuer
#    subord_of: USERTrustRSACertificationAuthority
#    subjectDN: /C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G4  [Run by the Issuer]
#    hash    : 3e0d64db

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G4  [Run by the Issuer]" \
  PERMIT Subject "/C=AE/O=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G4  [Run by the Issuer]" \
  PERMIT Subject "/DC=com/DC=DigitalTrustGrid/*"

TO Issuer "/C=AE/O=Digital Trust L.L.C./CN=DigitalTrust Assured CA G4  [Run by the Issuer]" \
  PERMIT Subject "/DC=org/DC=DigitalTrustGrid/*"
```

DarkMatter IGTF CAs

1 DT Public Trust

- IGTF HOST Classic CA providers created 2020, accredited in Karlsruhe:
  DigitalTrust Secure CA G3
  DigitalTrust Secure CA G4
  - Sectigo CP/CPS + DT RA
- IGTF CLIENT Classic CA providers created 2020, accredited in Karlsruhe:
  DigitalTrust Assured CA G3
  DigitalTrust Assured CA G4
  - Sectigo CP/CPS + DT RA
- 2 QV CAs retired

2 DT IGTF Private

- IGTF Cl[illegible]d HOST Classi[illegible] prov[illegible]r created 2017 [illegible]dited [illegible]018:
  - ~~**Lega[illegible] Com[illegible] IGTF CA**~~
  - D[illegible]S & RAs
- Accreditation 2019:
  - **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 prior 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 under new ownership – Digital14 LLC from Jan 1, 2020
- Same personnel, same infrastructure, same locations, same policies and processes, different owner
- 4th annual WebTrust Audit almost completed now with **DigitalTrust** as the asserting entity

Questions?

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

Scott.Rea@DigitalTrust.ae

https://digitaltrust.ae