DARKMATTER: A UAE BASED CYBER SECURITY COMPANY

IGTF UPDATE

SEP 2016

DARKMATTER

GUARDED BY GENIUS

CONTENTS

DARKMATTER PKI

DARKMATTER TRUST OBJECTIVES

PKI PROVISIONING CAPABILITIES

DARKMATTER SERVICES

STATUS UPDATE

PUBLIC KEY INFRASTRUCTURE

PROMOTING NATIONAL TRUST

UAE National Public Key Infrastructure provides interdisciplinary national trust establishment,
achieves full international interoperability, and enables the foundational services required for a digital economy

National Trust and Interoperability

National Trust Anchors

International Recognition

Private trust communities

Public Trust and IGTF

Private Trust anchors

Certificate Provisioning

Identity credentials

Web site security

Secure communications

Device security

Document Signing

Code Signing

Public Trust and IGTF ONLY

Trusted grid certificates

Professional Services

E-Services establishment

PKI integration

Policies: CP, CPS, RPS, SOPs

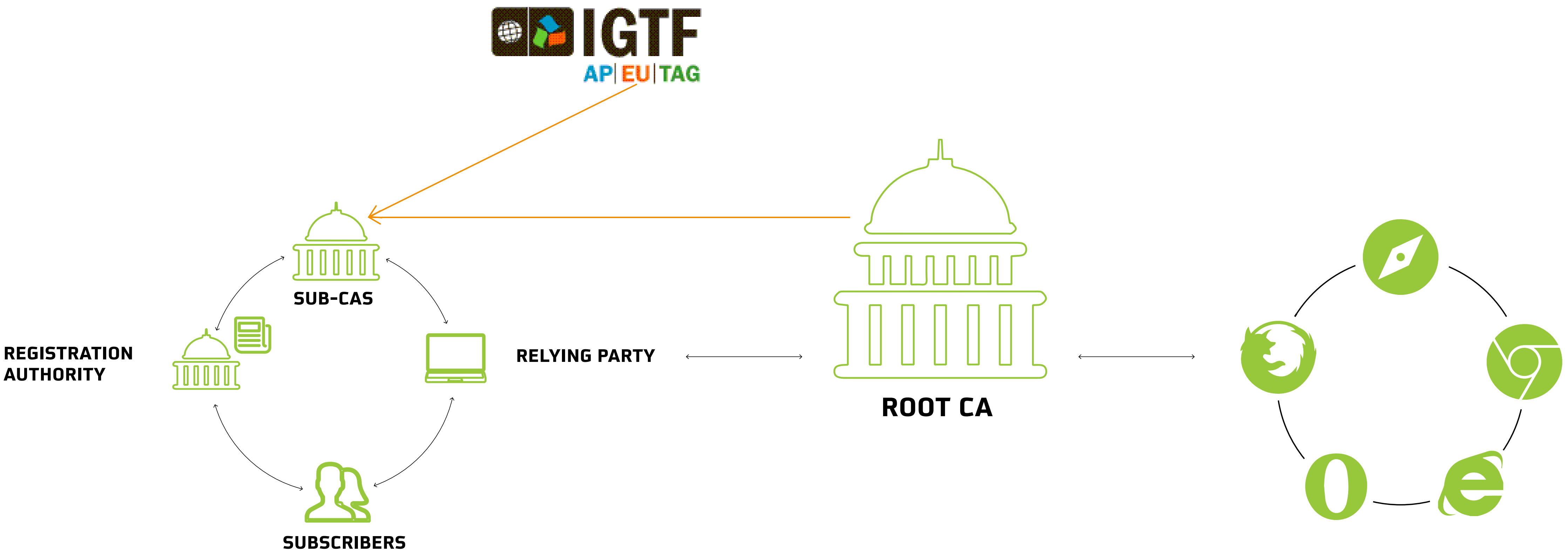
Cross-certification mapping

PK-enablement of Applications

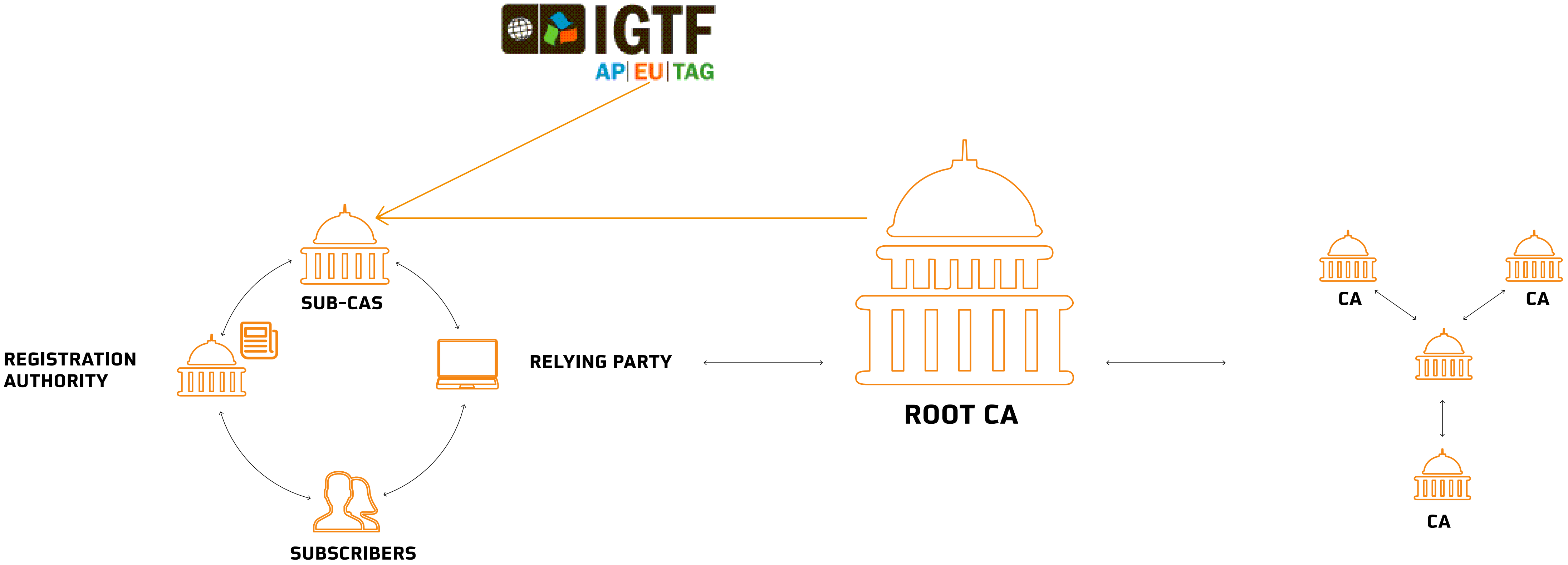
PKI Administration & Audit services

NATIONAL TRUST

NATIONAL TRUST ANCHORS – PUBLIC TRUST



NATIONAL TRUST ANCHORS - PRIVATE TRUST



NATIONAL CA OBJECTIVES

National CA program aims to provide interdisciplinary national trust establishment, achieve full international interoperability, and enable the foundational services required for a digital economy

National Trust Level Increase

- Establish national trust anchors that can be recognized by the international community
- Enable cross-certification with other countries or communities of trust

Interoperability

- Facilitate collaboration across public sector entities
- Facilitate collaboration between the public and private sectors

Electronic Service Enablement

- Enable the digital economy at a national level by securing electronic transactions across government, business and individual stakeholders

DARKMATTER CA TARGETED ACCREDITATIONS

IGTF Accredited Certification Authorities

Peer review is used to assess a CA’s controls against the IGTF Accreditation Guidelines. Only suitably accredited CAs will be trusted to issue grid certificates by added then to the IGTF distribution. IGTF Accreditation requires a bi-annual self audit.

WebTrust for Certification Authorities

WebTrust for CAs is the dominant commercial standard to assess the adequacy and effectiveness of controls deployed by a Certification Authority. Developed and managed jointly by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA), WebTrust for CAs requires an annual audit.

WebTrust for Extended Validation

WebTrust for Extended Validation is used to assess a CA’s controls against the CA/B Forum “Guidelines for the Issuance and Management of EV Certificates.” Only suitably accredited CAs may issue EV SSL. WebTrust for EV requires an annual audit.

WebTrust for Baseline Requirements

WebTrust for Baseline Requirements is used to assess a CA’s controls against the CA/B Forum “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”. WebTrust for BR requires an annual audit.

DARKMATTER CERTIFICATE PROVISIONING

TYPE OF CERTIFICATES

	Type	Definition	Function
1	**Root Certificate**	▪ Self signed certificate issued by the Root CA that acts as an anchor for trust	Certificate used primarily to certify Sub-CAs and establish a trust anchor for the National CA program
2	**Intermediate Certificate**	▪ Signed by either the Root CA or a parent Sub-CA ▪ Issued only to Sub-CAs, not to end users	Certificate acts as a link between Sub-CAs and the Root CA that enables validation of Sub-CA certificates by the Root CA
3	**End User Certificate**	▪ Signed by either the Root CA or a parent Sub-CA ▪ Issued directly to subscribers or end users (which may include services or devices)	Certificate issued to end users or services to facilitate the secure use of digital services

CERTIFICATES PROVIDED BY DARKMATTER – PRIVATE DOMAIN

IGTF ✓

Private CA

Custom Branded Root CA
(including custom crypto)

IoT Cerftificates

Iot Private Root, Iot Private Issuing
CA, IoT Service, Iot Client

IGTF ✓

Private TLS

Single Domain/Multi-domain,
ECC or RSA, Wildcard, etc …

Derived Client

Derived Mobile, Derived
Browser, Derived Cloud

WiFi as a Service

WiFi Authentication Services

IGTF ✓

Private Client Certificates

Authentication Certificate, SMIME
Signing / Encryption, Document Signing,
SMIME SmartCard, etc …

CERTIFICATES PROVIDED BY DARKMATTER – PUBLIC DOMAIN

IGTF ✓

Retail TLS

EV Single Domain/Multi-domain,
OV RSA Wildcard, etc …

IGTF ✓

Retail Client Certificates

Authentication Certificate, SMIME
Signing / Encryption, Document Signing,
SMIME SmartCard, etc …

Code Signing

EV Code Signing, Code Signing

IGTF ✓

Branded Public CA

Custom Branded Root CA (globally trusted)

IDENTITY CREDENTIALS

Enabling Services

IGTF ✓

Private Client Certificates

Authentication Certificate, SMIME Signing / Encryption, Document Signing, SMIME SmartCard, etc …

IGTF ✓

Retail Client Certificates

Authentication Certificate, SMIME Signing / Encryption, Document Signing, SMIME SmartCard, etc …

Derived Client

Derived Mobile, Derived Browser, Derived Cloud

WEB SITE SECURITY

Enabling Services

IGTF ✓

Private TLS`

Single Domain/Multi-domain,
ECC or RSA, Wildcard, etc …

IGTF ✓

Retail TLS

EV Single Domain/Multi-domain,
OV RSA Wildcard, etc …

SECURE COMMUNICATIONS

Enabling Services

IGTF ✓

Private TLS`

Single Domain/Multi-domain,
ECC or RSA, Wildcard, etc …

IGTF ✓

Private CA

Custom Branded Root CA
(including custom crypto)

IGTF ✓

Branded Public CA

Custom Branded Root CA
(globally trusted)

DEVICE SECURITY

Enabling Services

IoT Cerftificates

Iot Private Root, Iot Private Issuing CA, IoT Service, Iot Client

DOCUMENT SIGNING

Enabling Services

IGTF ✓

Private Client Certificates

Authentication Certificate, SMIME Signing / Encryption, Document Signing, SMIME SmartCard, etc …

IGTF ✓

Retail Client Certificates

Authentication Certificate, SMIME Signing / Encryption, Document Signing, SMIME SmartCard, etc …

CODE SIGNING

Enabling Services

Code Signing

EV Code Signing, Code Signing

DARKMATTER PROFESSIONAL SERVICES

PROFESSIONAL SERVICES

Managed PKI Integration

MPKI Design/Architecture, MPKI Enablement, MPKI Training

PKI Professional Services

MPKI Design/Architecture
Public Key Enablement, PKI 101 Training

PKI Audit

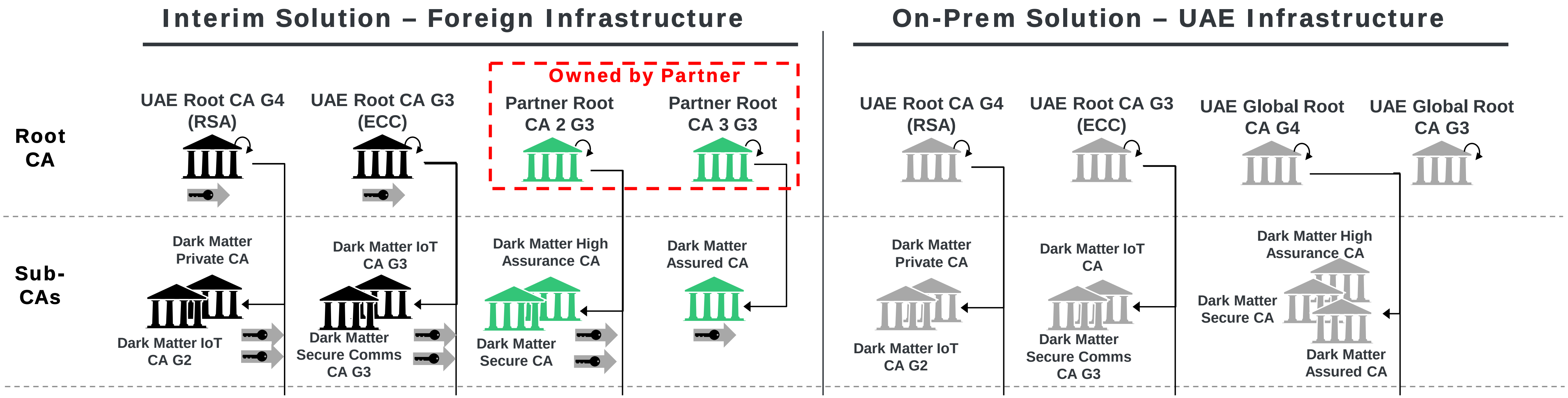
Log Audit, Process Audit, Site Audit
CP to CPS Mapping, RPS TO CPS Mapping

PKI Policy Services

CP, CPS & RPS Development,
CP Mapping, PKI Charter Development,
Policy Authority Support Services

DARKMATTER STATUS UPDATE

UAE NATIONAL CA ARCHITECTURE



Interim Solution – Foreign Infrastructure

On-Prem Solution – UAE Infrastructure

Root CA

Sub-CAs

UAE Root CA G4 (RSA)

UAE Root CA G3 (ECC)

Owned by Partner

Partner Root CA 2 G3

Partner Root CA 3 G3

Dark Matter Private CA

Dark Matter IoT CA G2

Dark Matter IoT CA G3

Dark Matter Secure Comms CA G3

Dark Matter High Assurance CA

Dark Matter Secure CA

Dark Matter Assured CA

UAE Root CA G4 (RSA)

UAE Root CA G3 (ECC)

UAE Global Root CA G4

UAE Global Root CA G3

Dark Matter Private CA

Dark Matter IoT CA G2

Dark Matter IoT CA

Dark Matter Secure Comms CA G3

Dark Matter High Assurance CA

Dark Matter Secure CA

Dark Matter Assured CA

➔ Related Key to be potentially transferred to On-Prem	■ Private CA	🟩 Public CA	▨ Planned CA

DARKMATTER PKI STATUS

- **UAE Infrastructure build out**
  - Production site: core CA/RA/VA infrastructure in acceptance testing phase
  - Production site: network security infrastructure build phase – 4 weeks to completion
  - DR site: core CA/RA/VA infrastructure in partitioned acceptance testing phase
  - DR site: network config and end to end validation – 6 weeks to completion
  - EJBCA platform with FIPS140 Level 3 HSMs
  - Modular architecture with separation of CA, RA, VA modules where needed
  - Offline Root on separate HSM
  - Online RA requiring PKI based authentication, even for local access
  - High capacity VAs for OCSP and CRL distribution
  - Web landing page/Repository in-process. Initial version in 4 weeks. Major upgrade by expected December 2017
  - Significant expansion of RA module to facilitate Managed PKI use cases expected in March 2017
  - Expected to be operational on UAE infrastructure November 2016
  - Expected to be WebTrust audited December 2016

DARKMATTER PKI STATUS

- Engagement of International Trust Partner to bootstrap trust
  - DarkMatter has partnered with QuoVadis to bootstrap trust for a few years while UAE Roots are embedded and deployed in Apps and OSes in parallel
  - Gradual cut over to UAE Roots
  - 2 Private Roots & 4 Private subCAs created in June 2016 – Operational today
  - 3 Public subCAs created in June 2016 – Operational today
  - All DarkMatter CAs operating on DarkMatter owned hardware, QV infrastructure under WebTrust Audit
- Transition from Partner infrastructure to DarkMatter
  - Transition will be completed prior to end of 2016
  - Once DM is WebTrust audited and capable of receiving transfer of publicly trusted CAs
  - Backup of QV operated CAs to be restored to DM infrastructure
  - De-provisioning of QV services, hardware shipped to DM
  - Public Trust relationship for 5 years

DARKMATTER + IGTF

DARKMATTER + 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
  - Wish to provide members access to National Grid Initiatives and also EGI participation
- DarkMatter is primarily seeking IGTF Accreditation so it is 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 bird with one stone?
- DarkMatter is open to providing certificate services to other national grid communities
  - Today, Public Trust grid certs will only be issued within UAE
  - IGTF or Private Trust grid certs can be issued globally if desired by contract of appropriate RA
  - Next year, Public Trust grid certs can be facilitated for any global location

DARKMATTER + IGTF

- DarkMatter is currently seeking IGTF accreditation of 3 Classic CAs
  - Public Trust CP/CPS operated by QV with DM RAs
    - DarkMatter Assured CA (Grid Client)
    - DarkMatter Secure CA (Grid Host)
  - IGTF Trust Only under UAE CP with DM CPS is a Work-In-Progress
    - CA is not yet created, depending on timing, may wait until DM infrastructure is operational
    - Could create under QV CP/CPS in 3 weeks and then include in transfer to DM infrastructure in December

Questions?

Scott.Rea@DarkMatter.ae

THANK YOU

DARKMATTER

GUARDED BY GENIUS