DARKMATTER: A UAE BASED CYBER SECURITY COMPANY

IGTF UPDATE

JAN 2017

DARKMATTER

GUARDED BY GENIUS

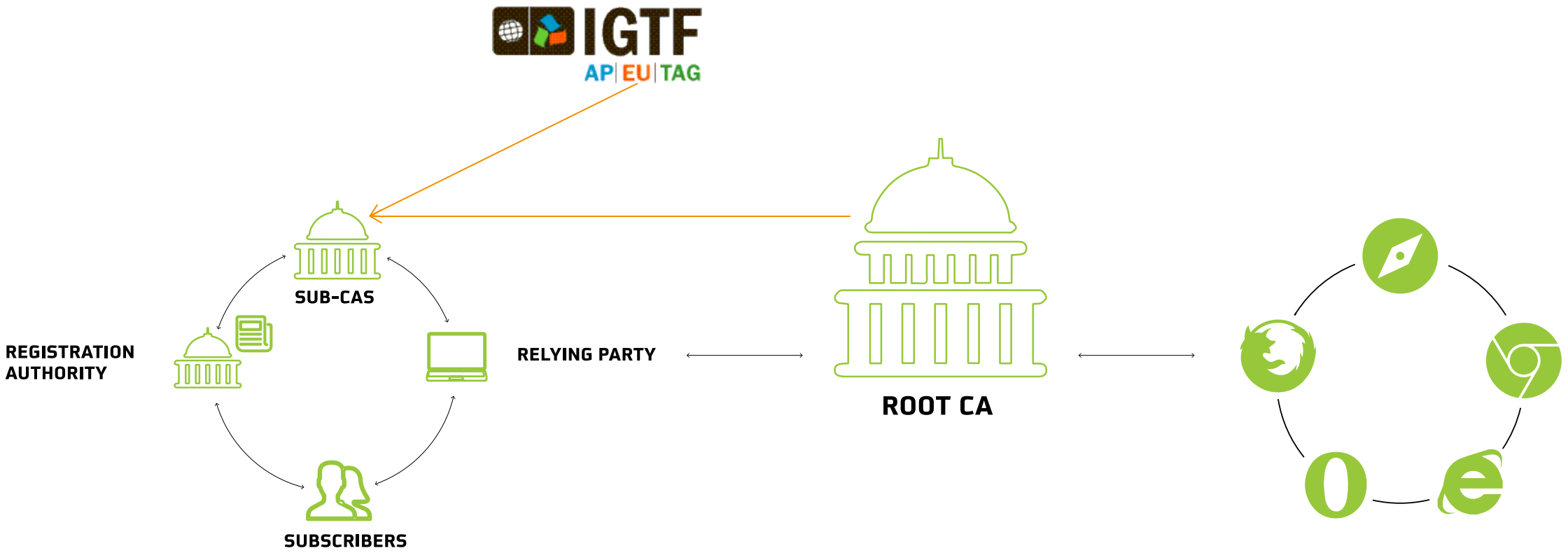
CONTENTS

DARKMATTER

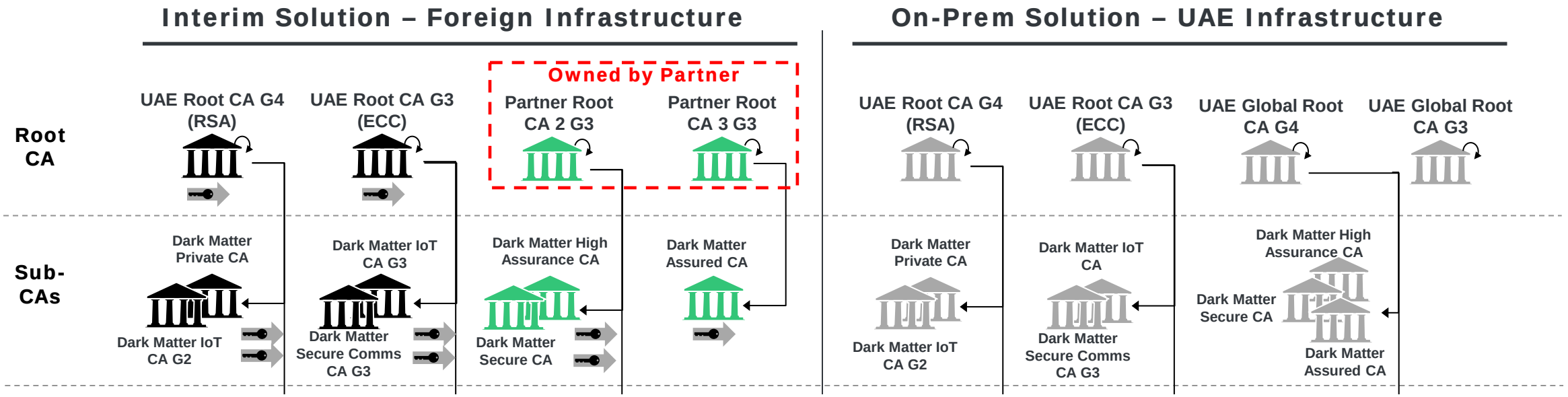
DARKMATTER PKI STATUS UPDATE

DARKMATTER

NATIONAL TRUST ANCHORS – PUBLIC TRUST



UAE NATIONAL CA ARCHITECTURE



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 completed
  - DR site: core CA/RA/VA infrastructure in acceptance testing phase
  - DR site: network config and end to end validation – 2 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 complete. Major upgrade by expected April 2017
  - Significant expansion of RA module to facilitate Managed PKI use cases expected in March 2017
  - Expected to be operational on UAE infrastructure March 2017
  - Expected to be WebTrust audited April 2017

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 above DM CAs operating on DM owned hardware, QV infrastructure under WebTrust
  - Further private roots and subs operating on prem at DM to support DM enterprise trust
- Transition from Partner infrastructure to DarkMatter
  - Transition will be completed prior to Q1 2017
  - 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 STATUS UPDATE

DARKMATTER

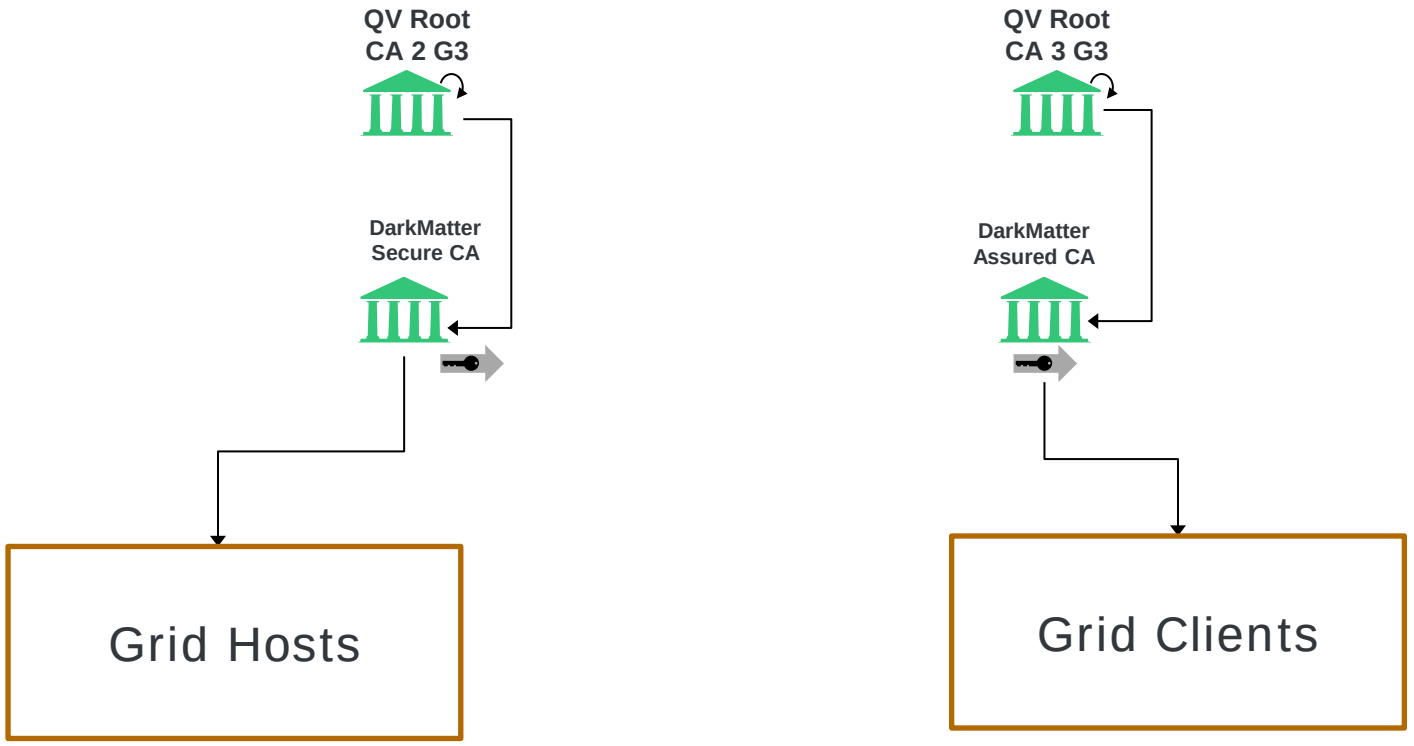
DARKMATTER + IGTF

- 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
  - Later this year, Public Trust grid certs can be facilitated for any global location

DARKMATTER + IGTF

- DarkMatter is currently seeking IGTF accreditation of 3 Classic CAs
  - (Today) Public Trust CP/CPS operated by QV with DM RAs
    - DarkMatter Assured CA (Grid Client)
    - DarkMatter Secure CA (Grid Host)
  - (Later) 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
  - Really need the Public Trust hierarchy approved this week – please…

PUBLIC TRUST HIERARCHY



DARKMATTER

DarkMatter PKI Services Grid Repository

Welcome to the DarkMatter Grid portal. DarkMatter is seeking to be an accredited IGTF CA via EUGridPMA.
In June 2016, DarkMatter launched it's PKI Services when it created a number of Trust Anchors (root and sub CAs) for the provisioning of certificates. DarkMatter anticipates two different hierarchies for the issuance of IGTF accredited grid certificates - one that operates only within the IGTF, and another that also chains to publicly trusted Root CAs. DarkMatter is currently seeking the accreditation of the Public Trust hierarchy.

Certificates may be requested at Trustlink

Certificates are issued under polices and procedures referenced below.

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 | 69105f4f.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 | a442a424.0

Questions?

Scott.Rea@DarkMatter.ae

THANK YOU

DARKMATTER

GUARDED BY GENIUS