DIGITALTRUST

DIGITALTRUST CA - a DarkMatter CA transition

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

Content

01 DarkMatter Trust Services

02 Introducing DigitalTrust LLC

03 DarkMatter IGTF CA Self-Audit

01

DarkMatter Trust Services

A Brief History of DarkMatter Trust Services

DARKMATTER TRUST SERVICES

- DarkMatter Established **Public Key Infrastructure** Business Unit in 2016 after award of UAE National PKI Operator contract
- DarkMatter PKI established UAE National Private Roots and Cross-signed Public ICAs in 2016 running in international WebTrust audited datacenters. Began outfit of in-country DCs.
- DM PKI obtained IGTF accreditation for Publicly Trusted Host and Client Issuing CAs in 2017 cross-signed under QV Roots
- DM PKI in-country operations achieved full WebTrust in 2017, subsequently moved all international operations to DM WebTrust certified datacenters & procedures.
- DM PKI changed name to **DarkMatter Trust Services** in response to expanded scope in 2017
- DM began UAE PASS initiative to establish national strong authentication and digital signing platform primarily based around mobile accessible DigitalIDs
- DM IGTF CA (Private Trust) established in 2018 and IGTF Accredited
- DM Trust Services achieved second consecutive WebTrust Audits in 2018

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 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 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
  - Public Trust grid certs can be facilitated for any global location

DARKMATTER + IGTF

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

DarkMatter IGTF CAs

1 DM Public Trust

- IGTF HOST Classic CA provider created 2016, accredited January 2017: **DarkMatter Secure CA**
  - QV CP/CPS + DM RA
  - DM CP/CPS & RAs
- IGTF CLIENT Classic CA provider created 2016, accredited January 2017: **DarkMatter Assured CA**
  - QV CP/CPS + DM RA
  - DM CP/CPS & RAs

2 DM IGTF Private

- IGTF CLIENT and HOST Classic CA provider created 2017, accredited 2018:
- **DarkMatter IGTF CA**
  - DM CP/CPS & RAs

3 DM Audits

- DarkMatter Trust Services is transitioning to **DigitalTrust LLC**
- Existing DM accredited CAs have completed self-audit review
- Results to be presented later in this presentation
- Future WebTrust audits will be completed under **DigitalTrust LLC**

4 DigitalTrust IGTF

- DarkMatter Trust Services is transitioning to **DigitalTrust LLC**
- Same personnel, same locations, different legal entity
- Next audits to be completed as **DigitalTrust**
- Namespace adjustment request pending

02

Introducing DigitalTrust

DIGITALTRUST

VISION

A world where the systems and processes underpinning digital transactions are secure and trusted to enable the full benefits of digital commerce.

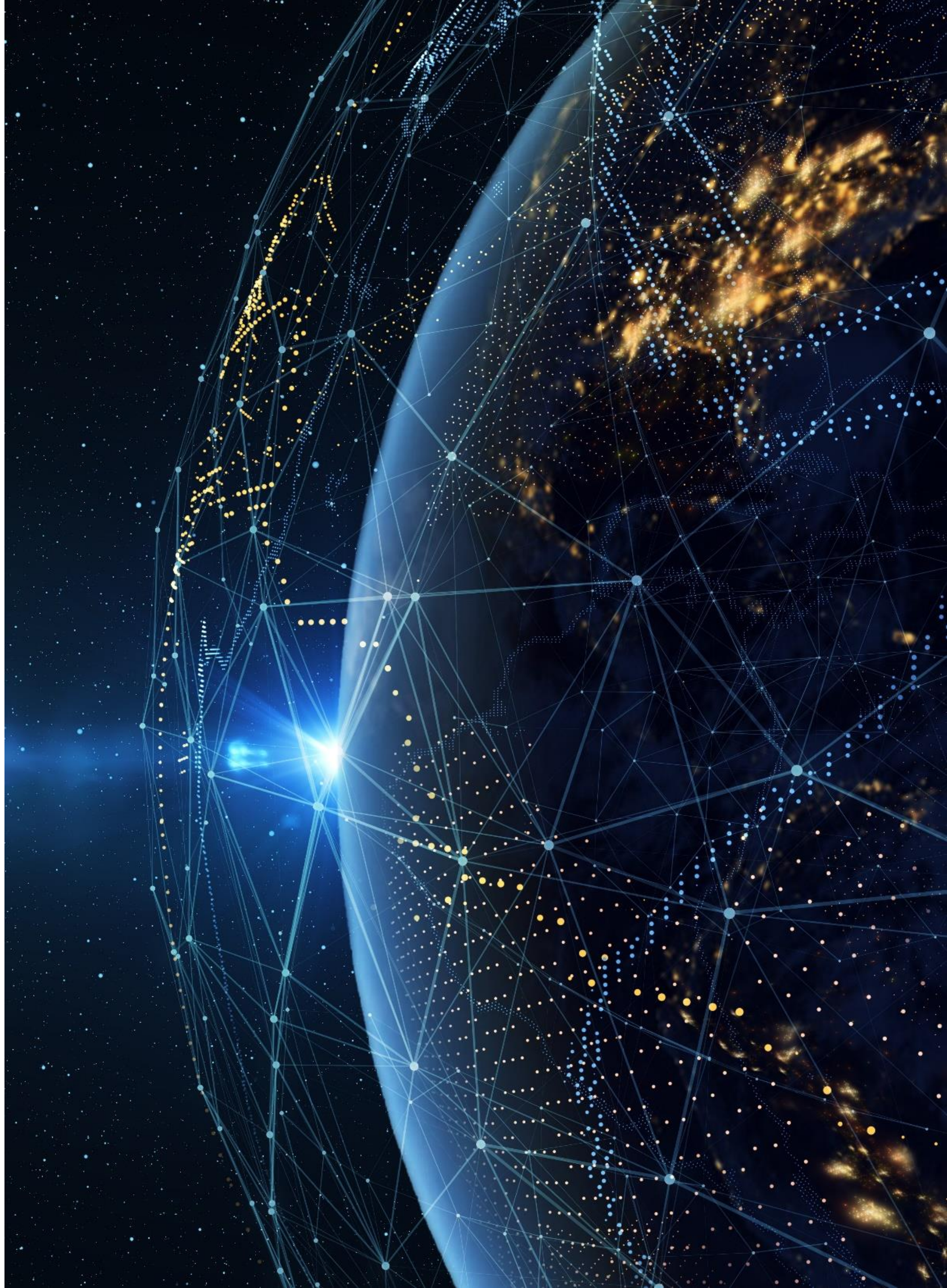
MISSION

To be the leading provider of the full spectrum of trust services in the region, enabling trust between parties for secure transactions.

STRATEGY

Our trust services are based on maintaining confidentiality and integrity of the data and strong authentication of parties to a transaction.

We are the only commercial Certification Authority (CA) based in the Middle East providing an end-to-end service with the credentials, signing system and supporting consultancy services. We provide the full spectrum of trust services to our customers so that they have a locally trusted source of all services.



DIGITALTRUST

The DIGITALTRUST business provides Public Key Infrastructure (PKI) and identity services, utilized to secure web sites, web services, TLS communications, supercomputing and research resources. PKI activities are an integral component of many unique solutions including Crypto Libraries, Blockchain Software Development kits, Secure Communications hardware and applications and advanced Big Data and Analytics tools.

ENABLING SECURE AND TRUSTED DIGITAL TRANSACTIONS

We offer **managed PKI services** at the enterprise, country and global community levels, able to prepare trust anchors and associated policy and processes necessary to meet certification requirements for targeted trust community.

We **manage National PKI services** for the UAE and Iraq supporting governments to establish a best-in-class national PKI infrastructure. We created and operate a national Root CA and sub-CAs for government and private sector entities. We support the design and roll-out of the hardware, certificate lifecycle and token management, registration and ongoing system monitoring.

We provide **professional PKI advisory and management services** to organisations implementing their own PKI architecture.

We are an official **WebTrust certified CA** granted WebTrust seals of assurance for two consecutive years of operations as a pre-requisite to being able to issue publicly-trusted digital certificates.

TRUSTED IN THE REGION

We are trusted in the Gulf region.

The CA business previously managed within DarkMatter LLC has been transferred to DIGITALTRUST, a Sole Proprietorship LLC established in the UAE in 2016.

Scott Rea manages the CA and trust services business for DIGITALTRUST. Scott has built his career on trust principles associated with PKI including requirements for publicly trusted, commercial CAs ranging from the first commercial CA in the US back in 2000, to the most recent three year process for DarkMatter Group (2016 to present). He has also shaped and developed national PKI initiatives including the US Federal PKI, UAE NPKI and Iraq NPKI.

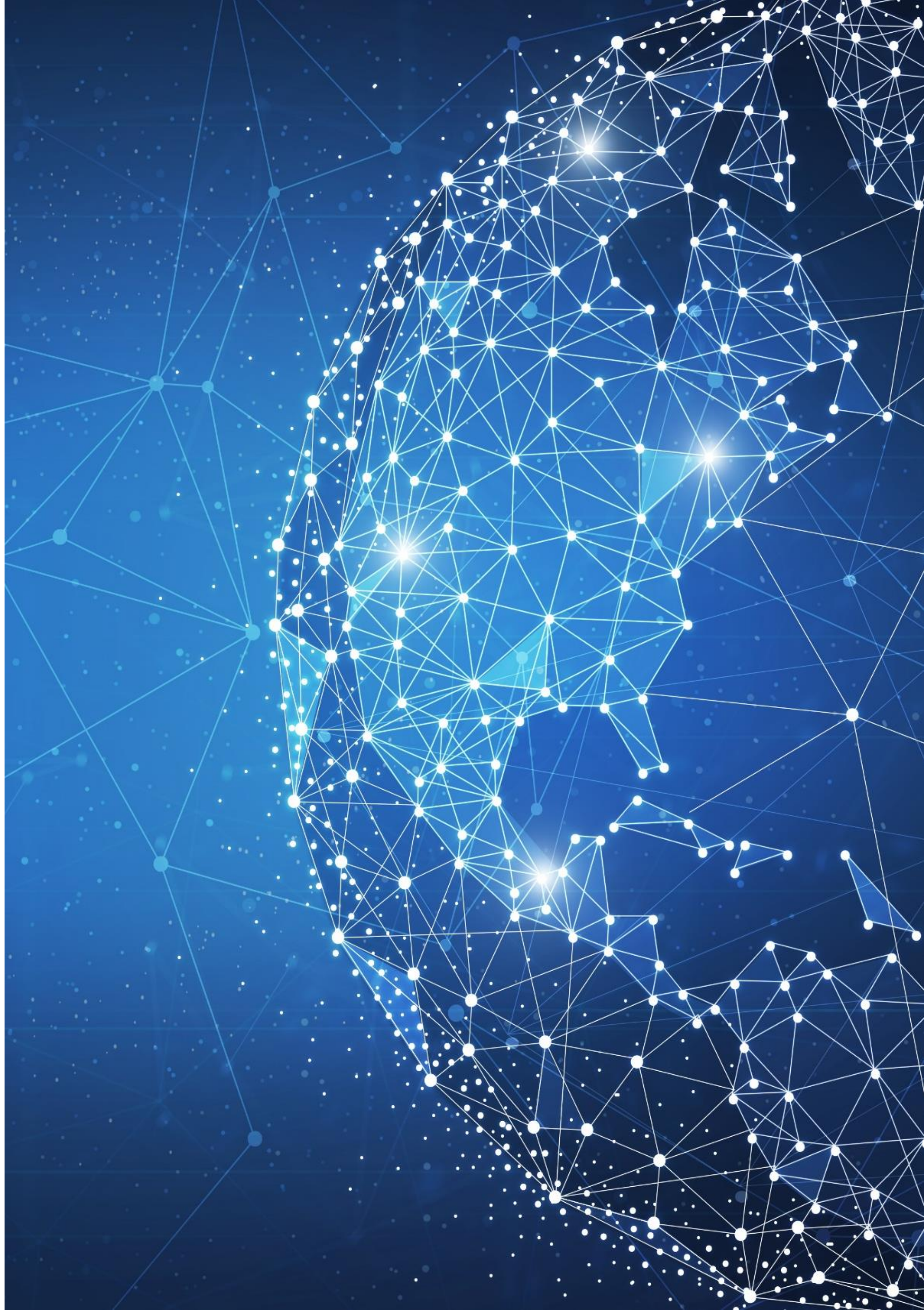
DigitalTrust is appointed by the UAE Telecommunications Regulatory Authority (TRA) to fulfill the following responsibilities in relation to the UAE National Public Key Infrastructure (NPKI):

- Operation of the NPKI technical infrastructure
- Advisory services for governance activities
- Representing the NPKI in Industry Working groups and relevant Trust Communities
- Fulfill compliance and regulatory responsibilities for the NPKI operations

PROGRESS TO DATE

DIGITALTRUST has accomplished the following key milestones in respect to its commercial PKI activities and the UAE NPKI:

- Successfully audited multiple years to WebTrust for CA's, WebTrust for Baseline Requirements, and WebTrust for Extended Validation controls.
- ISO 27001 accredited operations.
- IGTF accredited (research and supercomputing trust communities).
- Trust Services Provider for UAE, under the Telecommunications Regulatory Authority (TRA).
- DigitalTrust PKI operates under Service Provider License CSP-[001\17] issued by TRA of the UAE on 18th May 2017.
- DigitalTrust Appointed UAE NPKI Operator by the TRA.
- DigitalTrust is a Member of the CA & Browser Forum and active in several Working Groups.
- Appointed as sole authorized Certification Authority for deployment of the Iraq National PKI.
- Provider of UAE NPKI DigitalIDs under the UAE PASS initiative through Managed PKI with Federal Agency for Identity and Citizenship (formerly Emirates ID).
- DigitalTrust commercial PKI has been providing public trusted certificates since 2016 through cross-signed intermediates since April 2016.



INCLUSION IN INDUSTRY TRUSTED ROOT PROGRAMS

As the UAE transitions from a petrochemical dominated economy to an information and finance driven economy, having a secure infrastructure is critical. DigitalTrust is managing and operating the National PKI for the UAE.

DIGITALTRUST operates four Root CAs seeking public trust recognition – 2 for the UAE and 2 for commercial purposes and other regions.

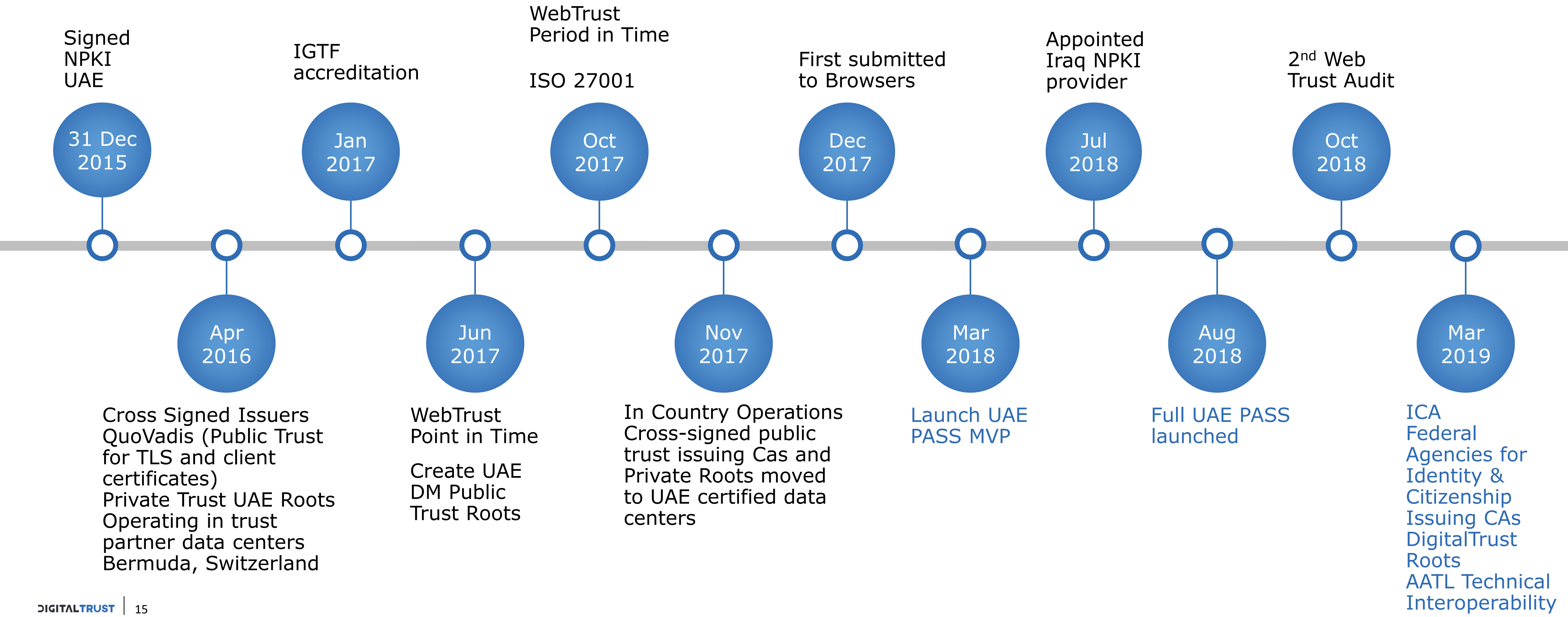
Embedding the UAE and DIGITALTRUST Roots will facilitate seamless trust and cyber security services as UAE residents and global DIGITALTRUST clients utilize common digital products and platforms.

DIGITALTRUST has completed its WebTrust Point in Time Audits for UAE and DIGITALTRUST Roots as well as its WebTrust Period of Time Audits (report from KPMG 27 October, 2017) with second WebTrust Audit completed on 2 October 2018.

DIGITALTRUST has completed technical interoperability with the Authorized Adobe Trust List program.

DIGITALTRUST

TIMELINE 2016-19



31 Dec 2015
Signed NPKI UAE

Apr 2016
Cross Signed Issuers QuoVadis (Public Trust for TLS and client certificates)
Private Trust UAE Roots
Operating in trust partner data centers Bermuda, Switzerland

Jan 2017
IGTF accreditation

Jun 2017
WebTrust Point in Time

Create UAE DM Public Trust Roots

Oct 2017
WebTrust Period in Time

ISO 27001

Nov 2017
In Country Operations
Cross-signed public trust issuing Cas and Private Roots moved to UAE certified data centers

Dec 2017
First submitted to Browsers

Mar 2018
Launch UAE PASS MVP

Jul 2018
Appointed Iraq NPKI provider

Aug 2018
Full UAE PASS launched

Oct 2018
2nd Web Trust Audit

Mar 2019
ICA
Federal Agencies for Identity & Citizenship Issuing CAs
DigitalTrust Roots
AATL Technical Interoperability

DARKMATTER GROUP: OUR PRACTICES

DarkMatter weaves digital enablement and cyber resilience seamlessly into the very fabric of an organization through its five practices:

DARKMATTER
CYBER DEFENSE

Provides an ‘always on’ cyber security transformation for businesses and governments so that they can safely perform their mission in the face of accelerating cyber risks.

DARKMATTER
SECURE SOLUTIONS

Offers ultra-secure unified communications solutions that allow businesses and governments to protect their business operations and data, giving them control and peace of mind.

DARKMATTER
GOVERNMENT SOLUTIONS

Tailors technologies to help governments strengthen their defence and security to mitigate risks.

DIGITALX1

Supports business and governments in digitally and smartly transforming their ways-of-working to achieve unprecedented levels of operational efficiency and effectiveness.

DIGITALE1

Enables businesses and governments in advancing the digital and cyber security dexterity of their human capital.

Additionally, DMG has three independent Affiliate businesses:

DIGITALTRUST

Provides PKI and identity services, utilised to secure web sites, web services and TLS communications.

xen1thLabs
A DARKMATTER COMPANY

Conducts vulnerability research, including the testing and validation activities it covers across software, hardware and telecommunication. xen1thLabs houses a team of world-class experts dedicated to providing high impact capabilities in cyber security, uncovering new vulnerabilities that combat tomorrow's threats today.

ajyal
Talent Management

Provides educational consultancy services and talent acceleration to strengthen the UAE’s future generations of human capital.

NEXT STEPS

- DarkMatter CAs and Trust Services complete transition to DIGITALTRUST LLC. Where appropriate, DM CAs will be retired and replaced with DIGITALTRUST counterparts.

- DIGITALTRUST to update accreditation bodies and Root Stores with timelines, plans and artifacts.

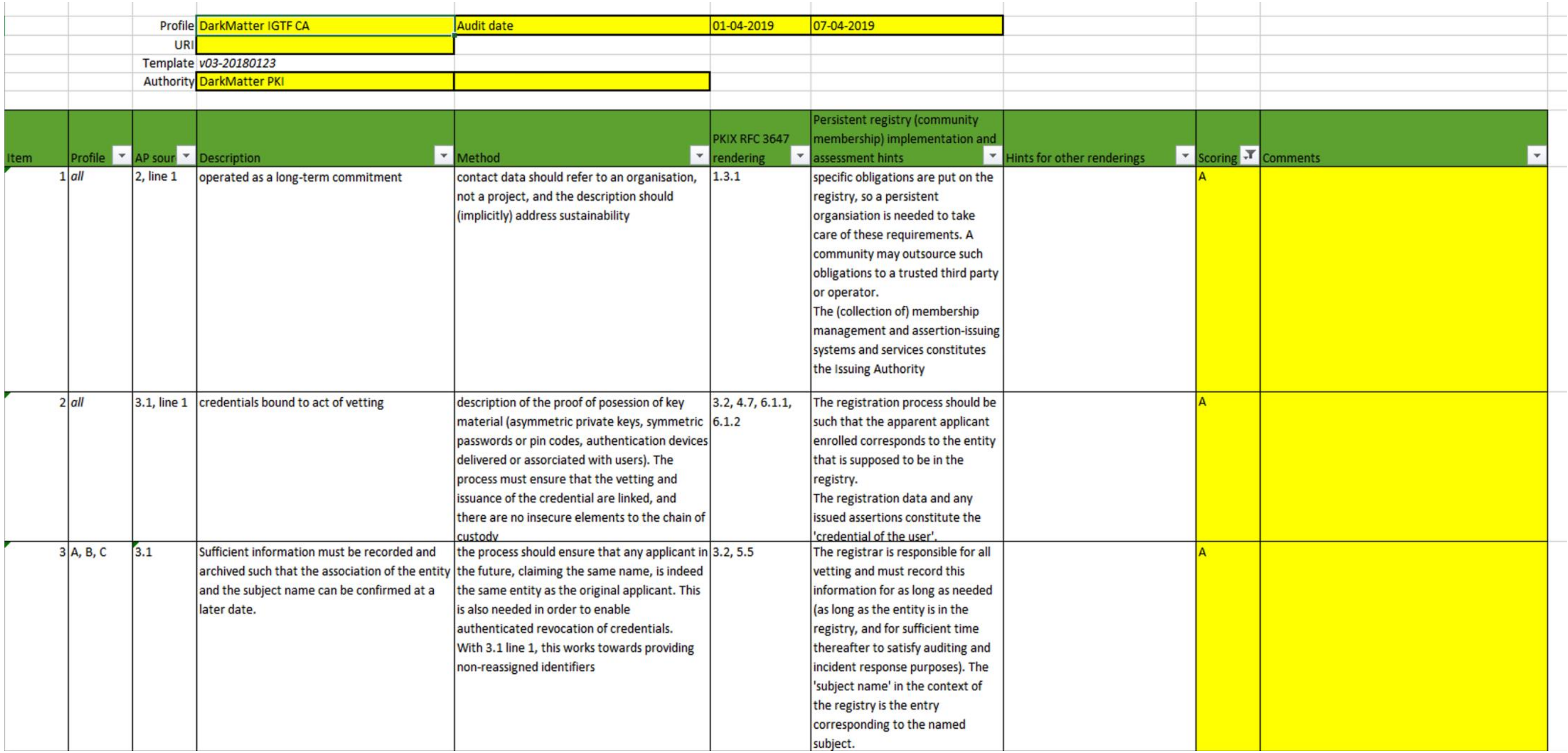
- DIGITALTRUST to transition QV-issued Public Trust cross-signed intermediate CAs to a dedicated Root CA under DigiCert [NOTE: DigiCert acquired QV TLS business in 2018]

- DIGITALTRUST to continue plans to roll out global retail capabilities for IGTF accredited HOST and CLIENT certifictes

03

DarkMatter CA Self-Audit

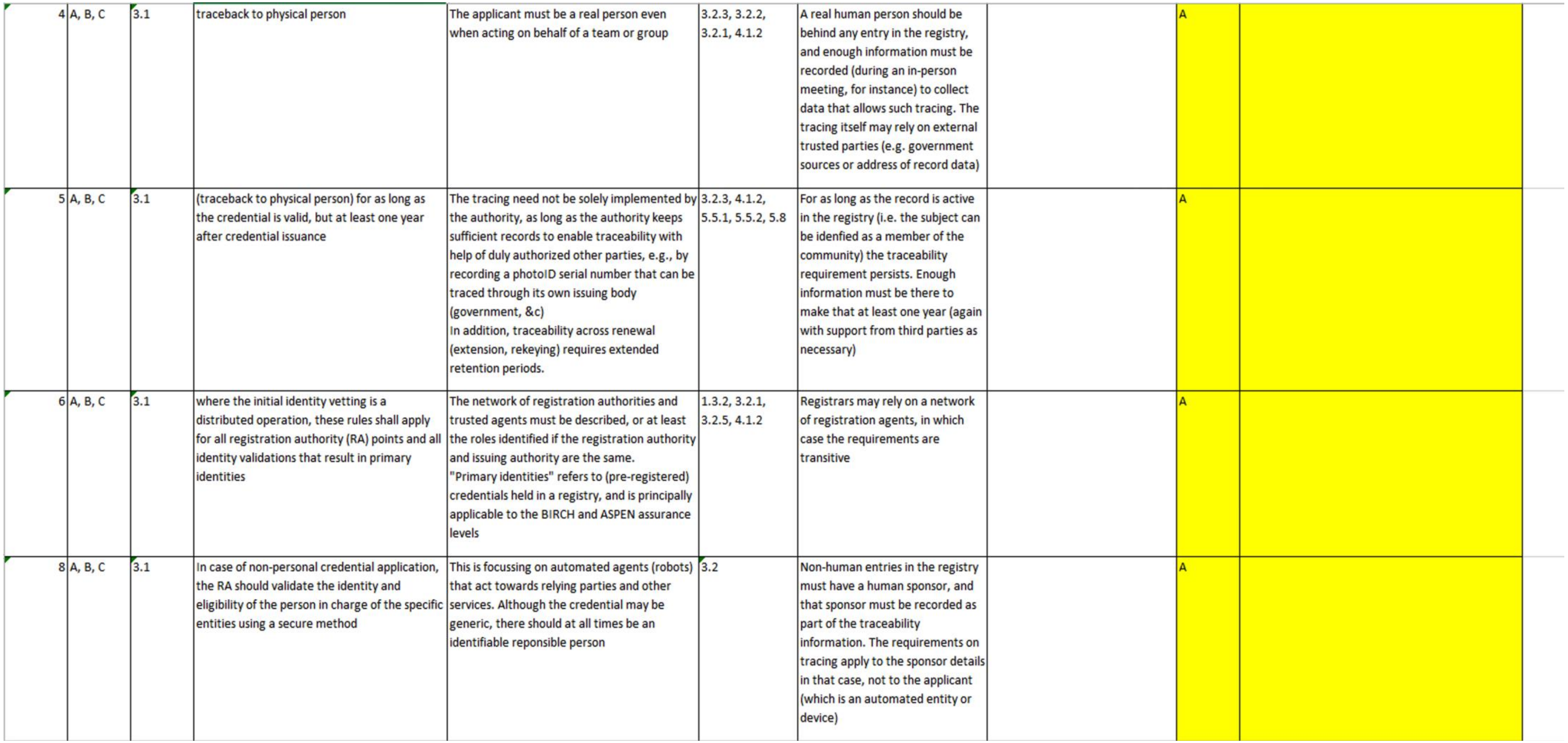
DIGITALTRUST Self Audit



Profile	DarkMatter IGTF CA	Audit date	01-04-2019	07-04-2019
URI				
Template	*v03-20180123*			
Authority	DarkMatter PKI			

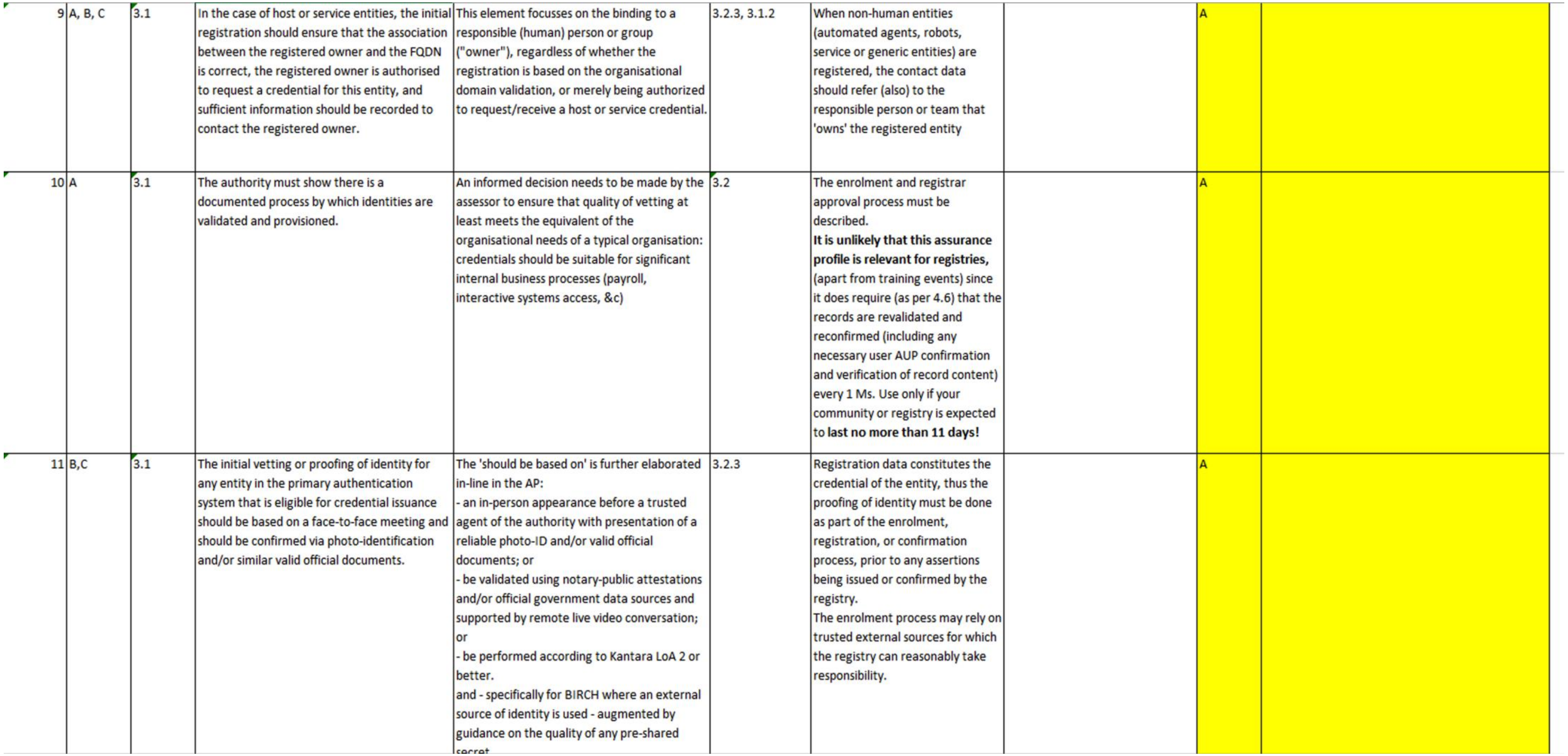
Item	Profile	AP sour	Description	Method	PKIX RFC 3647 rendering	Persistent registry (community membership) implementation and assessment hints	Hints for other renderings	Scoring	Comments
1	*all*	2, line 1	operated as a long-term commitment	contact data should refer to an organisation, not a project, and the description should (implicitly) address sustainability	1.3.1	specific obligations are put on the registry, so a persistent organisation is needed to take care of these requirements. A community may outsource such obligations to a trusted third party or operator. The (collection of) membership management and assertion-issuing systems and services constitutes the Issuing Authority		A	
2	*all*	3.1, line 1	credentials bound to act of vetting	description of the proof of posession of key material (asymmetric private keys, symmetric passwords or pin codes, authentication devices delivered or associated with users). The process must ensure that the vetting and issuance of the credential are linked, and there are no insecure elements to the chain of custody	3.2, 4.7, 6.1.1, 6.1.2	The registration process should be such that the apparent applicant enrolled corresponds to the entity that is supposed to be in the registry. The registration data and any issued assertions constitute the 'credential of the user'.		A	
3	A, B, C	3.1	Sufficient information must be recorded and archived such that the association of the entity and the subject name can be confirmed at a later date.	the process should ensure that any applicant in the future, claiming the same name, is indeed the same entity as the original applicant. This is also needed in order to enable authenticated revocation of credentials. With 3.1 line 1, this works towards providing non-reassigned identifiers	3.2, 5.5	The registrar is responsible for all vetting and must record this information for as long as needed (as long as the entity is in the registry, and for sufficient time thereafter to satisfy auditing and incident response purposes). The 'subject name' in the context of the registry is the entry corresponding to the named subject.		A	

DIGITALTRUST Self Audit



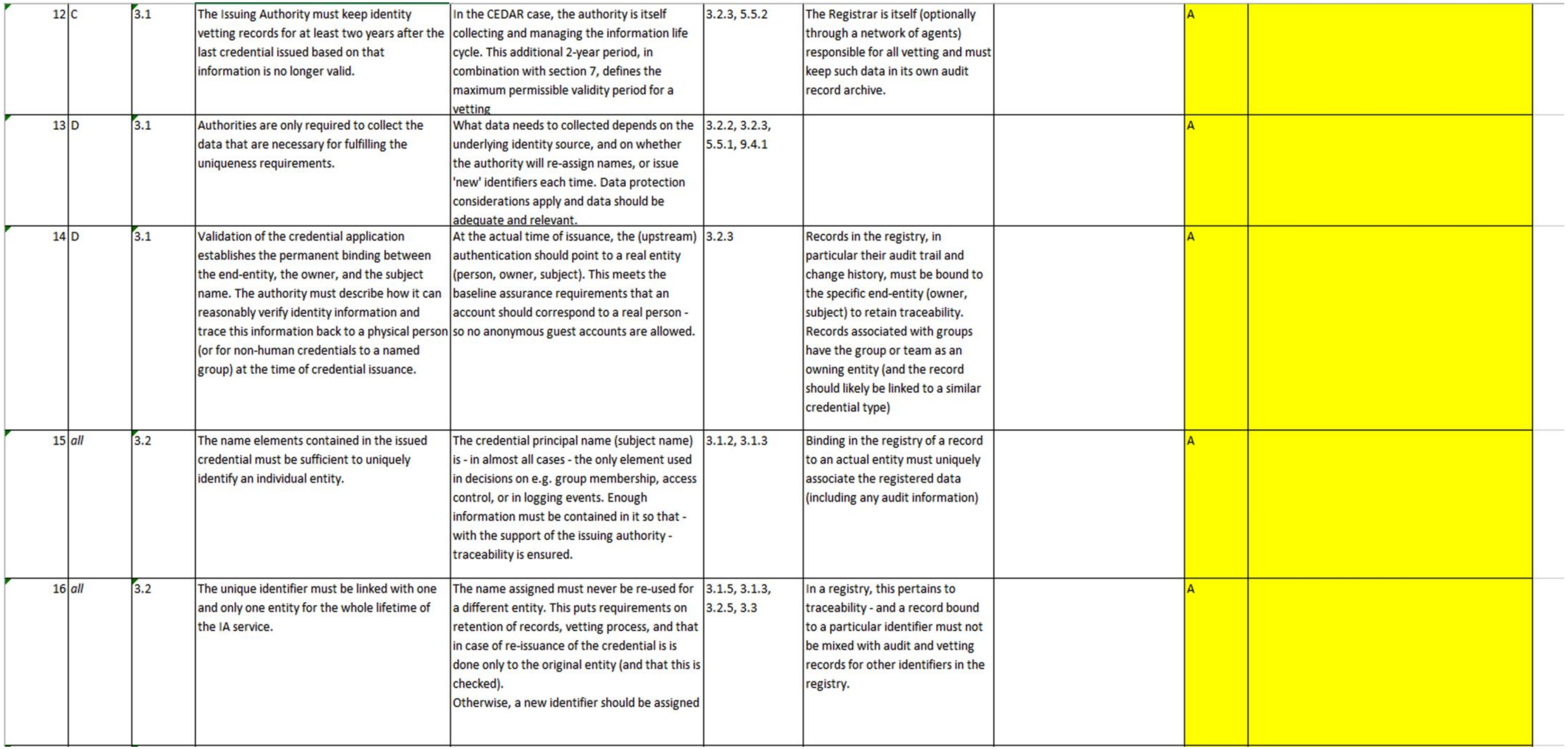
4	A, B, C	3.1	traceback to physical person	The applicant must be a real person even when acting on behalf of a team or group	3.2.3, 3.2.2, 3.2.1, 4.1.2	A real human person should be behind any entry in the registry, and enough information must be recorded (during an in-person meeting, for instance) to collect data that allows such tracing. The tracing itself may rely on external trusted parties (e.g. government sources or address of record data)		A	
5	A, B, C	3.1	(traceback to physical person) for as long as the credential is valid, but at least one year after credential issuance	The tracing need not be solely implemented by the authority, as long as the authority keeps sufficient records to enable traceability with help of duly authorized other parties, e.g., by recording a photoID serial number that can be traced through its own issuing body (government, &c) In addition, traceability across renewal (extension, rekeying) requires extended retention periods.	3.2.3, 4.1.2, 5.5.1, 5.5.2, 5.8	For as long as the record is active in the registry (i.e. the subject can be idenfied as a member of the community) the traceability requirement persists. Enough information must be there to make that at least one year (again with support from third parties as necessary)		A	
6	A, B, C	3.1	where the initial identity vetting is a distributed operation, these rules shall apply for all registration authority (RA) points and all identity validations that result in primary identities	The network of registration authorities and trusted agents must be described, or at least the roles identified if the registration authority and issuing authority are the same. "Primary identities" refers to (pre-registered) credentials held in a registry, and is principally applicable to the BIRCH and ASPEN assurance levels	1.3.2, 3.2.1, 3.2.5, 4.1.2	Registrars may rely on a network of registration agents, in which case the requirements are transitive		A	
8	A, B, C	3.1	In case of non-personal credential application, the RA should validate the identity and eligibility of the person in charge of the specific entities using a secure method	This is focussing on automated agents (robots) that act towards relying parties and other services. Although the credential may be generic, there should at all times be an identifiable reponsible person	3.2	Non-human entries in the registry must have a human sponsor, and that sponsor must be recorded as part of the traceability information. The requirements on tracing apply to the sponsor details in that case, not to the applicant (which is an automated entity or device)		A	

DIGITALTRUST Self Audit



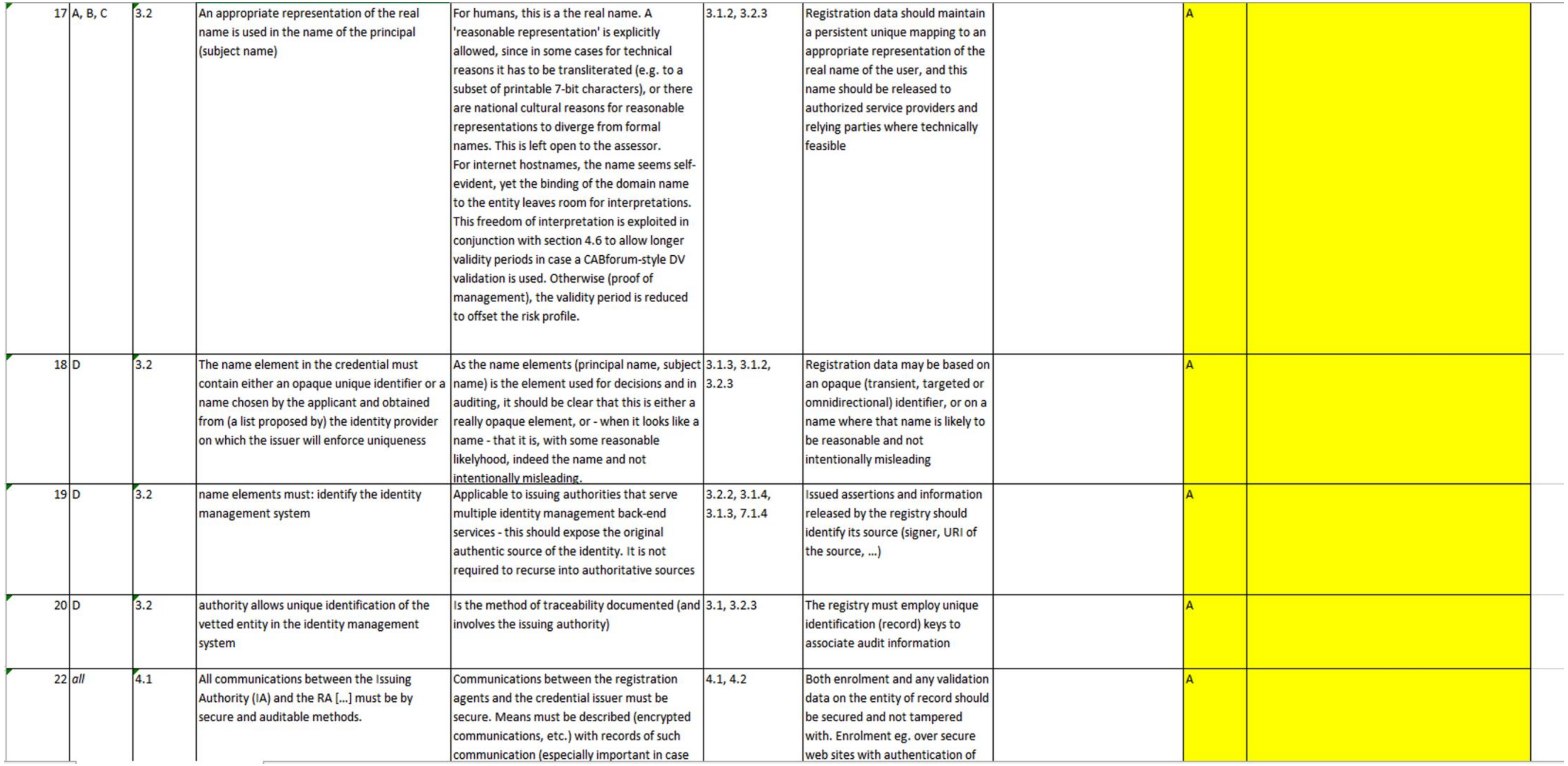
9	A, B, C	3.1	In the case of host or service entities, the initial registration should ensure that the association between the registered owner and the FQDN is correct, the registered owner is authorised to request a credential for this entity, and sufficient information should be recorded to contact the registered owner.	This element focusses on the binding to a responsible (human) person or group ("owner"), regardless of whether the registration is based on the organisational domain validation, or merely being authorized to request/receive a host or service credential.	3.2.3, 3.1.2	When non-human entities (automated agents, robots, service or generic entities) are registered, the contact data should refer (also) to the responsible person or team that 'owns' the registered entity		A	
10	A	3.1	The authority must show there is a documented process by which identities are validated and provisioned.	An informed decision needs to be made by the assessor to ensure that quality of vetting at least meets the equivalent of the organisational needs of a typical organisation: credentials should be suitable for significant internal business processes (payroll, interactive systems access, &c)	3.2	The enrolment and registrar approval process must be described. **It is unlikely that this assurance profile is relevant for registries,** (apart from training events) since it does require (as per 4.6) that the records are revalidated and reconfirmed (including any necessary user AUP confirmation and verification of record content) every 1 Ms. Use only if your community or registry is expected to **last no more than 11 days!**		A	
11	B,C	3.1	The initial vetting or proofing of identity for any entity in the primary authentication system that is eligible for credential issuance should be based on a face-to-face meeting and should be confirmed via photo-identification and/or similar valid official documents.	The 'should be based on' is further elaborated in-line in the AP: - an in-person appearance before a trusted agent of the authority with presentation of a reliable photo-ID and/or valid official documents; or - be validated using notary-public attestations and/or official government data sources and supported by remote live video conversation; or - be performed according to Kantara LoA 2 or better. and - specifically for BIRCH where an external source of identity is used - augmented by guidance on the quality of any pre-shared secret.	3.2.3	Registration data constitutes the credential of the entity, thus the proofing of identity must be done as part of the enrolment, registration, or confirmation process, prior to any assertions being issued or confirmed by the registry. The enrolment process may rely on trusted external sources for which the registry can reasonably take responsibility.		A	

DIGITALTRUST Self Audit



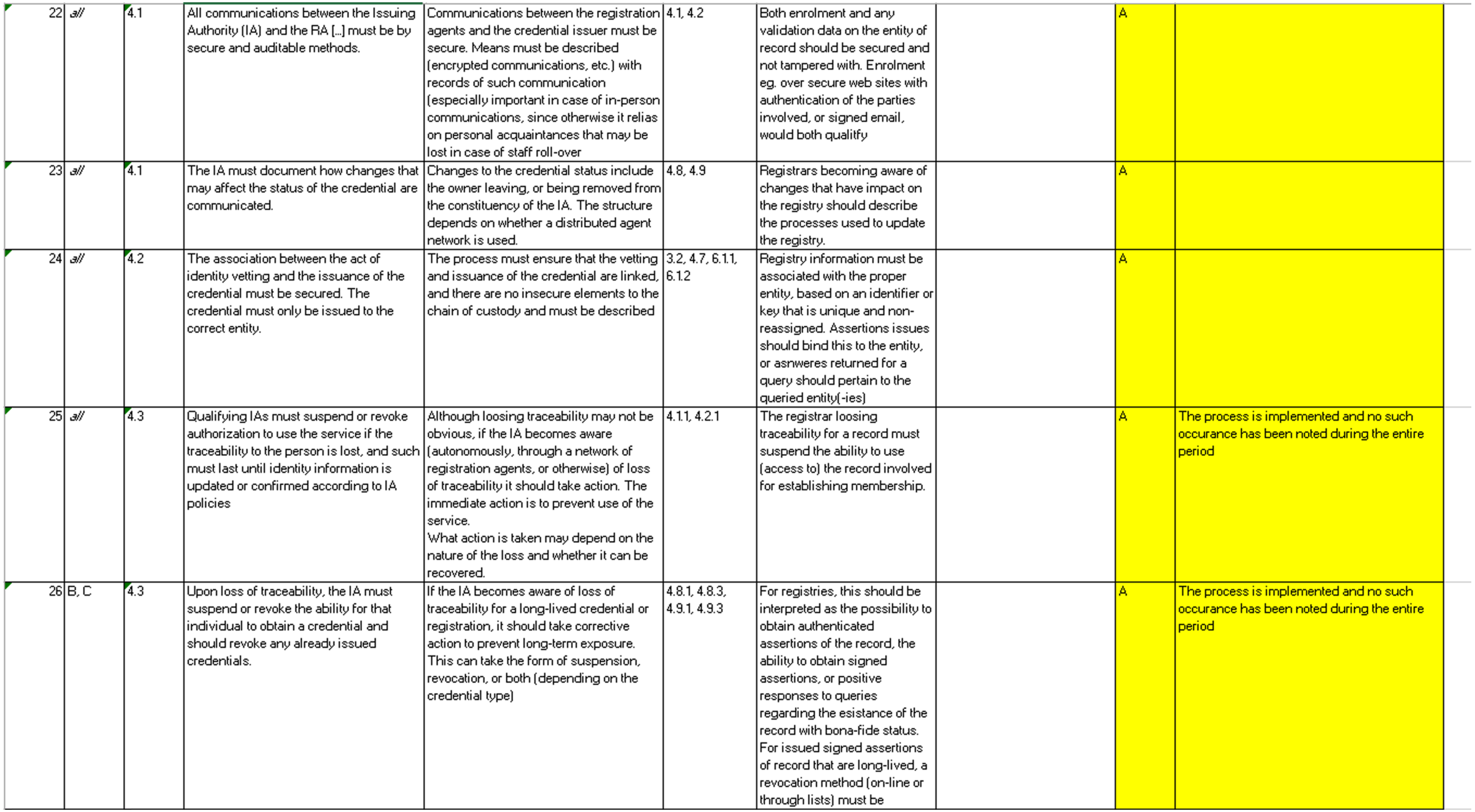
12	C	3.1	The Issuing Authority must keep identity vetting records for at least two years after the last credential issued based on that information is no longer valid.	In the CEDAR case, the authority is itself collecting and managing the information life cycle. This additional 2-year period, in combination with section 7, defines the maximum permissible validity period for a vetting	3.2.3, 5.5.2	The Registrar is itself (optionally through a network of agents) responsible for all vetting and must keep such data in its own audit record archive.		A	
13	D	3.1	Authorities are only required to collect the data that are necessary for fulfilling the uniqueness requirements.	What data needs to collected depends on the underlying identity source, and on whether the authority will re-assign names, or issue 'new' identifiers each time. Data protection considerations apply and data should be adequate and relevant.	3.2.2, 3.2.3, 5.5.1, 9.4.1			A	
14	D	3.1	Validation of the credential application establishes the permanent binding between the end-entity, the owner, and the subject name. The authority must describe how it can reasonably verify identity information and trace this information back to a physical person (or for non-human credentials to a named group) at the time of credential issuance.	At the actual time of issuance, the (upstream) authentication should point to a real entity (person, owner, subject). This meets the baseline assurance requirements that an account should correspond to a real person - so no anonymous guest accounts are allowed.	3.2.3	Records in the registry, in particular their audit trail and change history, must be bound to the specific end-entity (owner, subject) to retain traceability. Records associated with groups have the group or team as an owning entity (and the record should likely be linked to a similar credential type)		A	
15	*all*	3.2	The name elements contained in the issued credential must be sufficient to uniquely identify an individual entity.	The credential principal name (subject name) is - in almost all cases - the only element used in decisions on e.g. group membership, access control, or in logging events. Enough information must be contained in it so that - with the support of the issuing authority - traceability is ensured.	3.1.2, 3.1.3	Binding in the registry of a record to an actual entity must uniquely associate the registered data (including any audit information)		A	
16	*all*	3.2	The unique identifier must be linked with one and only one entity for the whole lifetime of the IA service.	The name assigned must never be re-used for a different entity. This puts requirements on retention of records, vetting process, and that in case of re-issuance of the credential is is done only to the original entity (and that this is checked). Otherwise, a new identifier should be assigned	3.1.5, 3.1.3, 3.2.5, 3.3	In a registry, this pertains to traceability - and a record bound to a particular identifier must not be mixed with audit and vetting records for other identifiers in the registry.		A	

DIGITALTRUST Self Audit



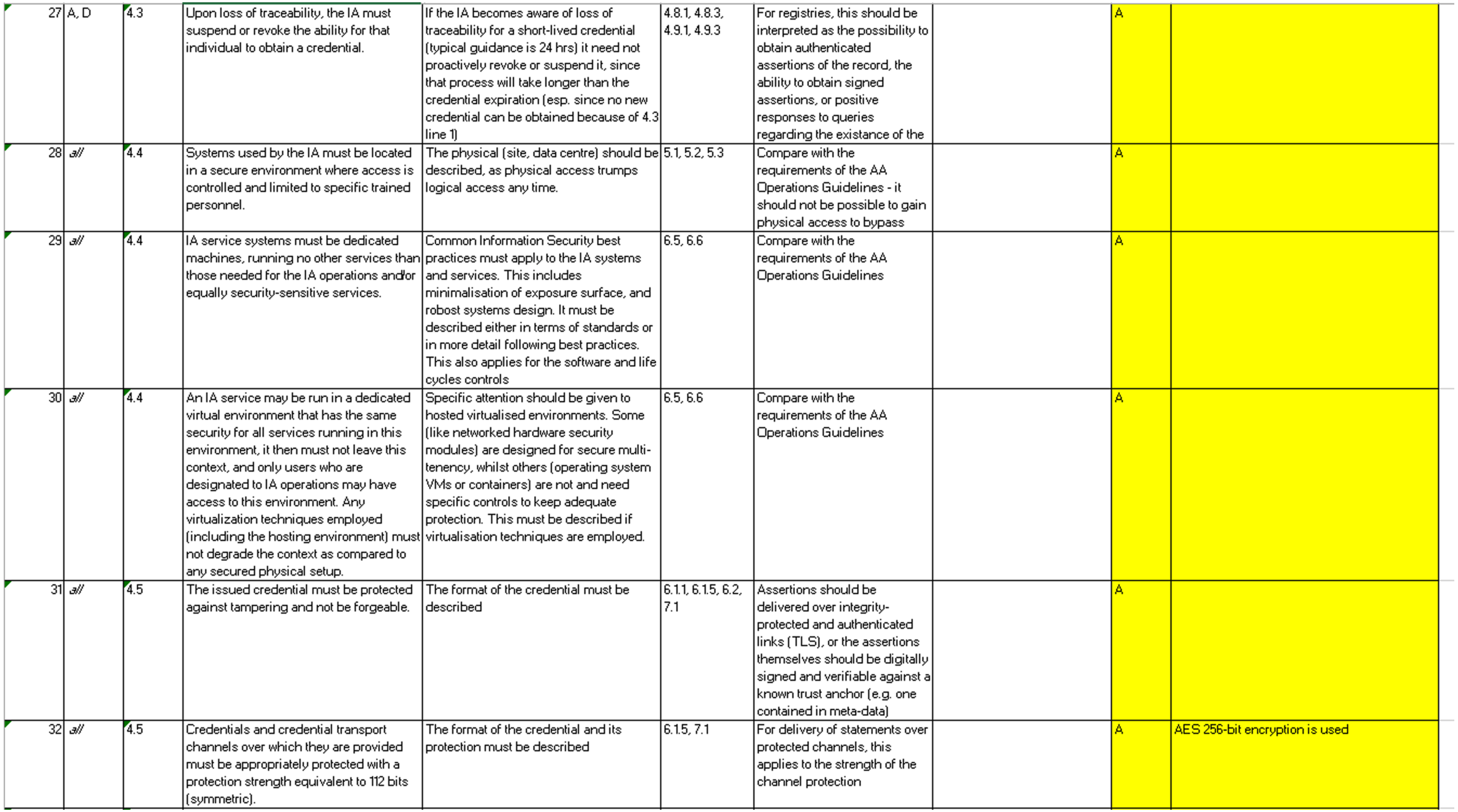
17	A, B, C	3.2	An appropriate representation of the real name is used in the name of the principal (subject name)	For humans, this is a the real name. A 'reasonable representation' is explicitly allowed, since in some cases for technical reasons it has to be transliterated (e.g. to a subset of printable 7-bit characters), or there are national cultural reasons for reasonable representations to diverge from formal names. This is left open to the assessor. For internet hostnames, the name seems self-evident, yet the binding of the domain name to the entity leaves room for interpretations. This freedom of interpretation is exploited in conjunction with section 4.6 to allow longer validity periods in case a CABforum-style DV validation is used. Otherwise (proof of management), the validity period is reduced to offset the risk profile.	3.1.2, 3.2.3	Registration data should maintain a persistent unique mapping to an appropriate representation of the real name of the user, and this name should be released to authorized service providers and relying parties where technically feasible		A	
18	D	3.2	The name element in the credential must contain either an opaque unique identifier or a name chosen by the applicant and obtained from (a list proposed by) the identity provider on which the issuer will enforce uniqueness	As the name elements (principal name, subject name) is the element used for decisions and in auditing, it should be clear that this is either a really opaque element, or - when it looks like a name - that it is, with some reasonable likelihood, indeed the name and not intentionally misleading.	3.1.3, 3.1.2, 3.2.3	Registration data may be based on an opaque (transient, targeted or omnidirectional) identifier, or on a name where that name is likely to be reasonable and not intentionally misleading		A	
19	D	3.2	name elements must: identify the identity management system	Applicable to issuing authorities that serve multiple identity management back-end services - this should expose the original authentic source of the identity. It is not required to recurse into authoritative sources	3.2.2, 3.1.4, 3.1.3, 7.1.4	Issued assertions and information released by the registry should identify its source (signer, URI of the source, ...)		A	
20	D	3.2	authority allows unique identification of the vetted entity in the identity management system	Is the method of traceability documented (and involves the issuing authority)	3.1, 3.2.3	The registry must employ unique identification (record) keys to associate audit information		A	
22	*all*	4.1	All communications between the Issuing Authority (IA) and the RA [...] must be by secure and auditable methods.	Communications between the registration agents and the credential issuer must be secure. Means must be described (encrypted communications, etc.) with records of such communication (especially important in case	4.1, 4.2	Both enrolment and any validation data on the entity of record should be secured and not tampered with. Enrolment eg. over secure web sites with authentication of		A	

DIGITALTRUST Self Audit



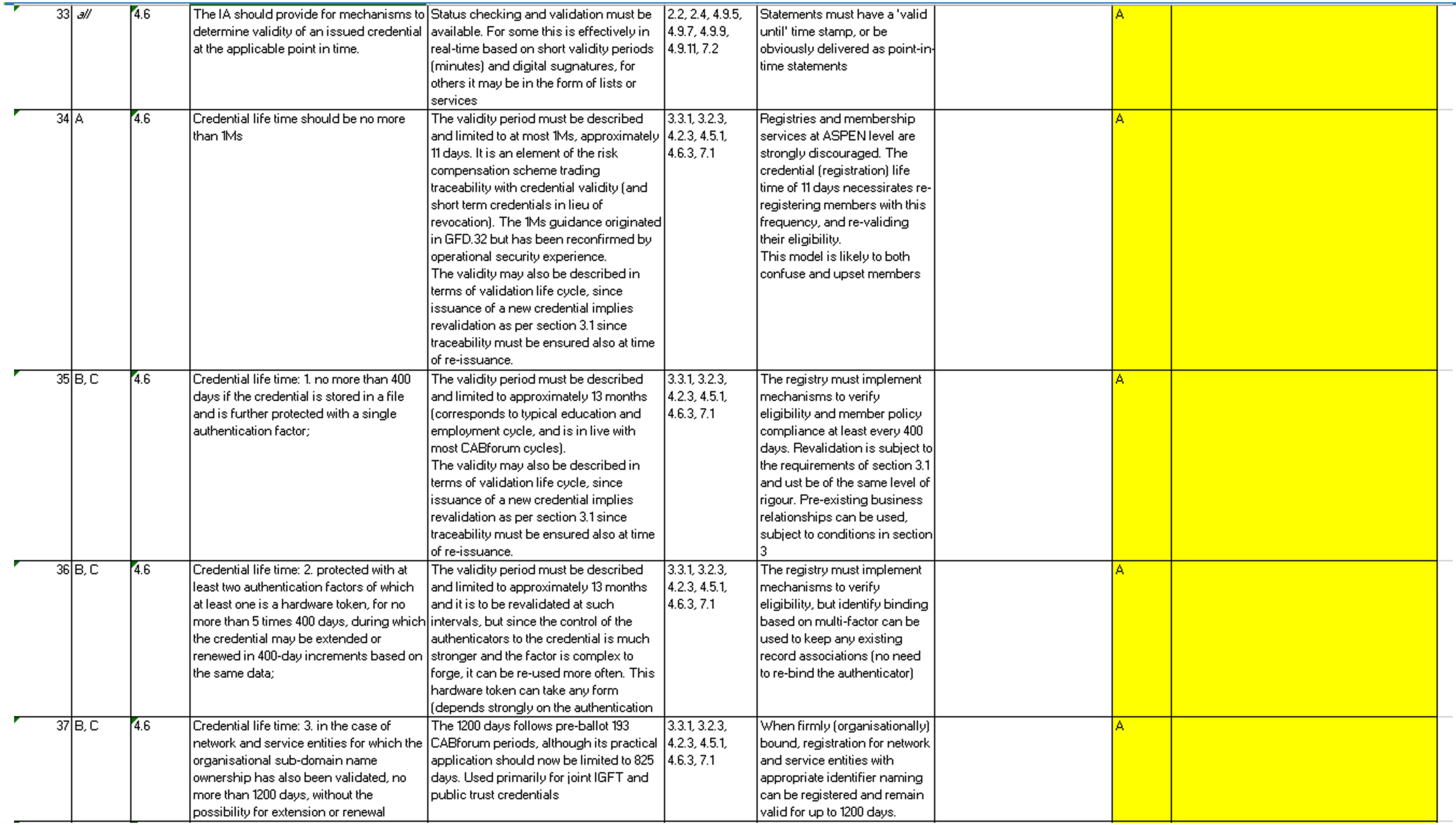
22	*all*	4.1	All communications between the Issuing Authority (IA) and the RA [...] must be by secure and auditable methods.	Communications between the registration agents and the credential issuer must be secure. Means must be described (encrypted communications, etc.) with records of such communication (especially important in case of in-person communications, since otherwise it relias on personal acquaintances that may be lost in case of staff roll-over	4.1, 4.2	Both enrolment and any validation data on the entity of record should be secured and not tampered with. Enrolment eg. over secure web sites with authentication of the parties involved, or signed email, would both qualitfy		A	
23	*all*	4.1	The IA must document how changes that may affect the status of the credential are communicated.	Changes to the credential status include the owner leaving, or being removed from the constituency of the IA. The structure depends on whether a distributed agent network is used.	4.8, 4.9	Registrars becoming aware of changes that have impact on the registry should describe the processes used to update the registry.		A	
24	*all*	4.2	The association between the act of identity vetting and the issuance of the credential must be secured. The credential must only be issued to the correct entity.	The process must ensure that the vetting and issuance of the credential are linked, and there are no insecure elements to the chain of custody and must be described	3.2, 4.7, 6.1.1, 6.1.2	Registry information must be associated with the proper entity, based on an identifier or key that is unique and non-reassigned. Assertions issues should bind this to the entity, or asnweres returned for a query should pertain to the queried entity(-ies)		A	
25	*all*	4.3	Qualifying IAs must suspend or revoke authorization to use the service if the traceability to the person is lost, and such must last until identity information is updated or confirmed according to IA policies	Although loosing traceability may not be obvious, if the IA becomes aware (autonomously, through a network of registration agents, or otherwise) of loss of traceability it should take action. The immediate action is to prevent use of the service. What action is taken may depend on the nature of the loss and whether it can be recovered.	4.1.1, 4.2.1	The registrar loosing traceability for a record must suspend the ability to use (access to) the record involved for establishing membership.		A	The process is implemented and no such occurance has been noted during the entire period
26	B, C	4.3	Upon loss of traceability, the IA must suspend or revoke the ability for that individual to obtain a credential and should revoke any already issued credentials.	If the IA becomes aware of loss of traceability for a long-lived credential or registration, it should take corrective action to prevent long-term exposure. This can take the form of suspension, revocation, or both (depending on the credential type)	4.8.1, 4.8.3, 4.9.1, 4.9.3	For registries, this should be interpreted as the possibility to obtain authenticated assertions of the record, the ability to obtain signed assertions, or positive responses to queries regarding the esistance of the record with bona-fide status. For issued signed assertions of record that are long-lived, a revocation method (on-line or through lists) must be		A	The process is implemented and no such occurance has been noted during the entire period

DIGITALTRUST Self Audit



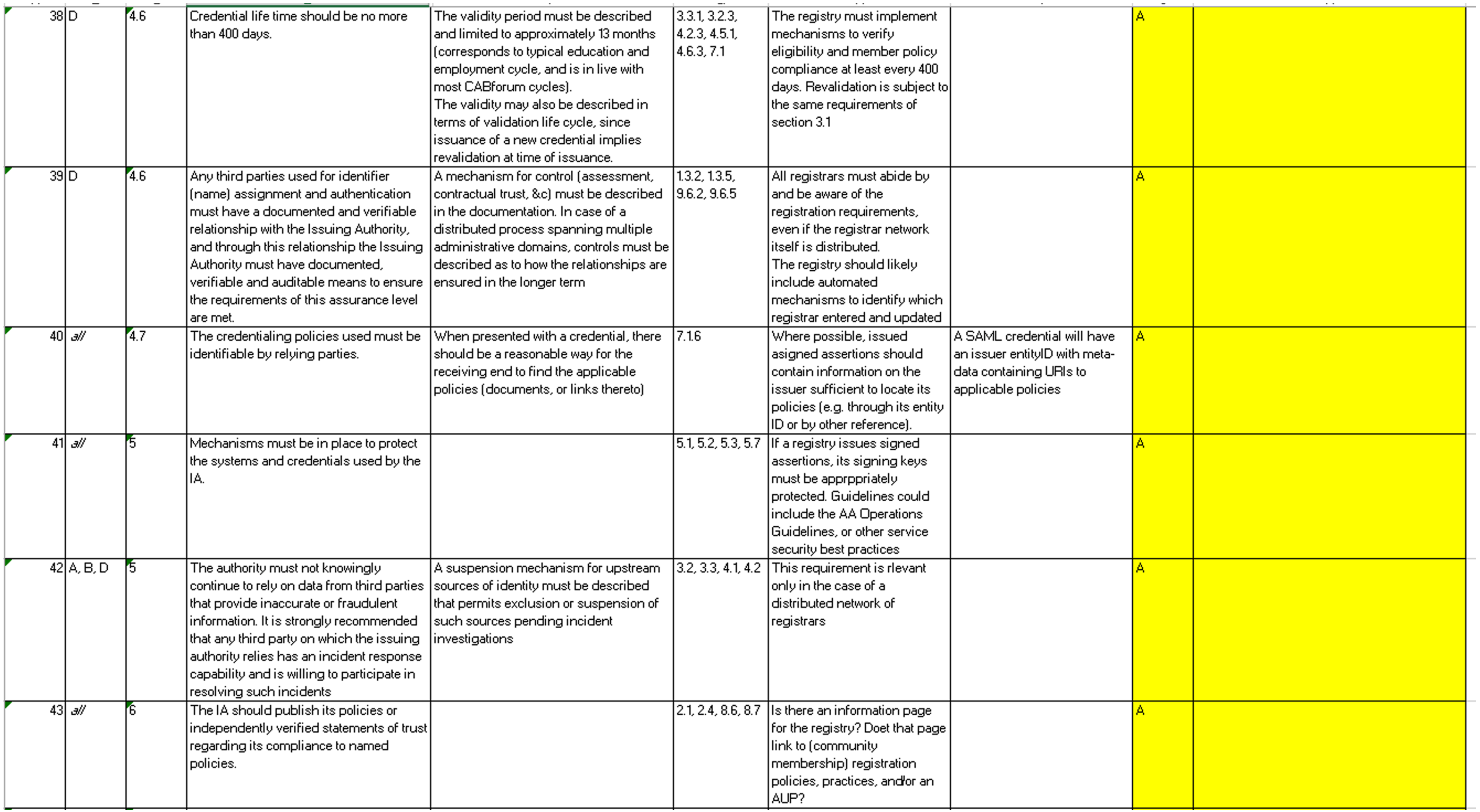
27	A, D	4.3	Upon loss of traceability, the IA must suspend or revoke the ability for that individual to obtain a credential.	If the IA becomes aware of loss of traceability for a short-lived credential (typical guidance is 24 hrs) it need not proactively revoke or suspend it, since that process will take longer than the credential expiration (esp. since no new credential can be obtained because of 4.3 line 1)	4.8.1, 4.8.3, 4.9.1, 4.9.3	For registries, this should be interpreted as the possibility to obtain authenticated assertions of the record, the ability to obtain signed assertions, or positive responses to queries regarding the existance of the		A	
28	all	4.4	Systems used by the IA must be located in a secure environment where access is controlled and limited to specific trained personnel.	The physical (site, data centre) should be described, as physical access trumps logical access any time.	5.1, 5.2, 5.3	Compare with the requirements of the AA Operations Guidelines - it should not be possible to gain physical access to bypass		A	
29	all	4.4	IA service systems must be dedicated machines, running no other services than those needed for the IA operations and/or equally security-sensitive services.	Common Information Security best practices must apply to the IA systems and services. This includes minimalisation of exposure surface, and robost systems design. It must be described either in terms of standards or in more detail following best practices. This also applies for the software and life cycles controls	6.5, 6.6	Compare with the requirements of the AA Operations Guidelines		A	
30	all	4.4	An IA service may be run in a dedicated virtual environment that has the same security for all services running in this environment, it then must not leave this context, and only users who are designated to IA operations may have access to this environment. Any virtualization techniques employed (including the hosting environment) must not degrade the context as compared to any secured physical setup.	Specific attention should be given to hosted virtualised environments. Some (like networked hardware security modules) are designed for secure multi-tenancy, whilst others (operating system VMs or containers) are not and need specific controls to keep adequate protection. This must be described if virtualisation techniques are employed.	6.5, 6.6	Compare with the requirements of the AA Operations Guidelines		A	
31	all	4.5	The issued credential must be protected against tampering and not be forgeable.	The format of the credential must be described	6.1.1, 6.1.5, 6.2, 7.1	Assertions should be delivered over integrity-protected and authenticated links (TLS), or the assertions themselves should be digitally signed and verifiable against a known trust anchor (e.g. one contained in meta-data)		A	
32	all	4.5	Credentials and credential transport channels over which they are provided must be appropriately protected with a protection strength equivalent to 112 bits (symmetric).	The format of the credential and its protection must be described	6.1.5, 7.1	For delivery of statements over protected channels, this applies to the strength of the channel protection		A	AES 256-bit encryption is used

DIGITALTRUST Self Audit



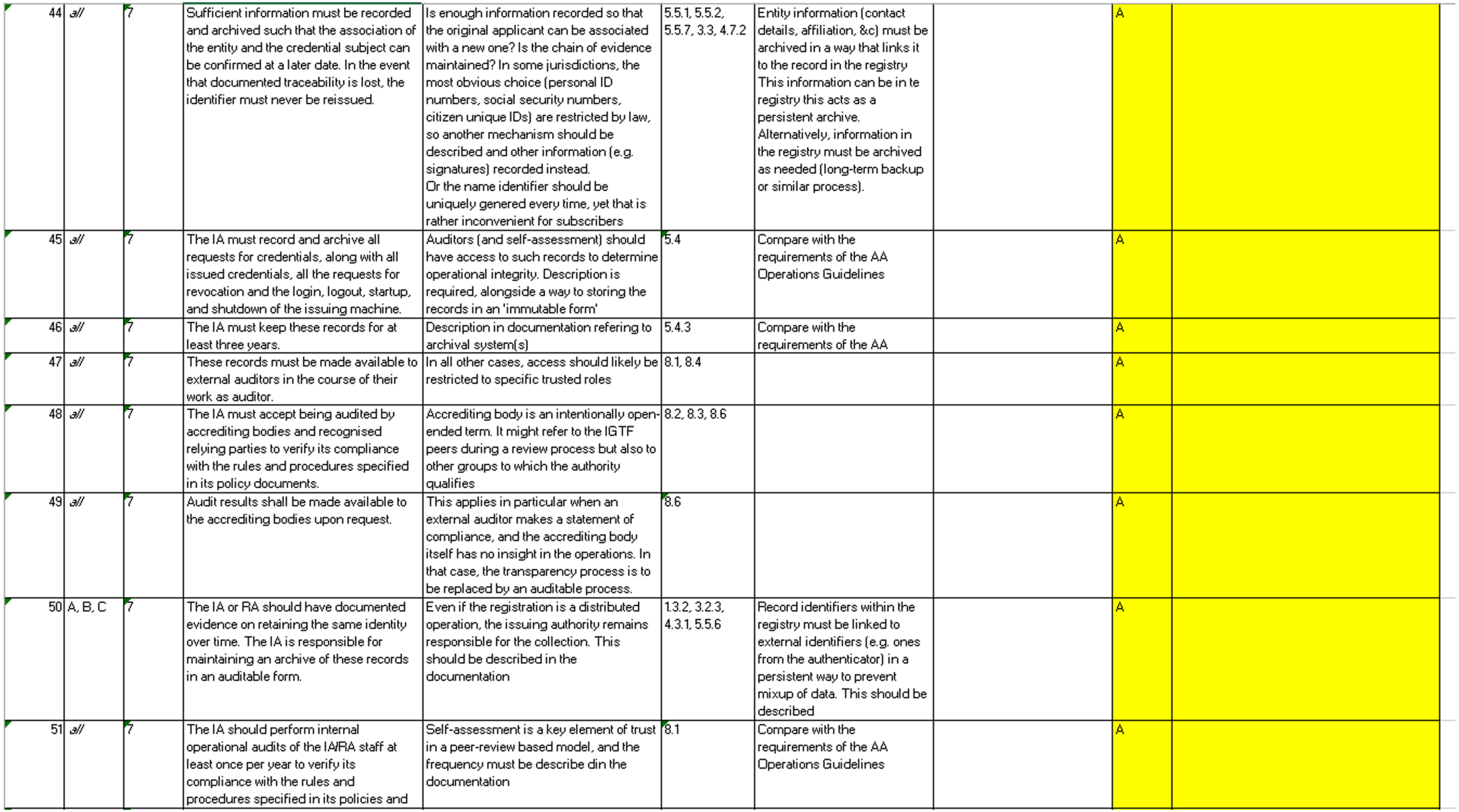
33	all	4.6	The IA should provide for mechanisms to determine validity of an issued credential at the applicable point in time.	Status checking and validation must be available. For some this is effectively in real-time based on short validity periods (minutes) and digital sugnatures, for others it may be in the form of lists or services	2.2, 2.4, 4.9.5, 4.9.7, 4.9.9, 4.9.11, 7.2	Statements must have a 'valid until' time stamp, or be obviously delivered as point-in-time statements		A	
34	A	4.6	Credential life time should be no more than 1Ms	The validity period must be described and limited to at most 1Ms, approximately 11 days. It is an element of the risk compensation scheme trading traceability with credential validity (and short term credentials in lieu of revocation). The 1Ms guidance originated in GFD.32 but has been reconfirmed by operational security experience. The validity may also be described in terms of validation life cycle, since issuance of a new credential implies revalidation as per section 3.1 since traceability must be ensured also at time of re-issuance.	3.3.1, 3.2.3, 4.2.3, 4.5.1, 4.6.3, 7.1	Registries and membership services at ASPEN level are strongly discouraged. The credential (registration) life time of 11 days necessirates re-registering members with this frequency, and re-validing their eligibility. This model is likely to both confuse and upset members		A	
35	B, C	4.6	Credential life time: 1. no more than 400 days if the credential is stored in a file and is further protected with a single authentication factor;	The validity period must be described and limited to approximately 13 months (corresponds to typical education and employment cycle, and is in live with most CABforum cycles). The validity may also be described in terms of validation life cycle, since issuance of a new credential implies revalidation as per section 3.1 since traceability must be ensured also at time of re-issuance.	3.3.1, 3.2.3, 4.2.3, 4.5.1, 4.6.3, 7.1	The registry must implement mechanisms to verify eligibility and member policy compliance at least every 400 days. Revalidation is subject to the requirements of section 3.1 and ust be of the same level of rigour. Pre-existing business relationships can be used, subject to conditions in section 3		A	
36	B, C	4.6	Credential life time: 2. protected with at least two authentication factors of which at least one is a hardware token, for no more than 5 times 400 days, during which the credential may be extended or renewed in 400-day increments based on the same data;	The validity period must be described and limited to approximately 13 months and it is to be revalidated at such intervals, but since the control of the authenticators to the credential is much stronger and the factor is complex to forge, it can be re-used more often. This hardware token can take any form (depends strongly on the authentication	3.3.1, 3.2.3, 4.2.3, 4.5.1, 4.6.3, 7.1	The registry must implement mechanisms to verify eligibility, but identify binding based on multi-factor can be used to keep any existing record associations (no need to re-bind the authenticator)		A	
37	B, C	4.6	Credential life time: 3. in the case of network and service entities for which the organisational sub-domain name ownership has also been validated, no more than 1200 days, without the possibility for extension or renewal	The 1200 days follows pre-ballot 193 CABforum periods, although its practical application should now be limited to 825 days. Used primarily for joint IGFT and public trust credentials	3.3.1, 3.2.3, 4.2.3, 4.5.1, 4.6.3, 7.1	When firmly (organisationally) bound, registration for network and service entities with appropriate identifier naming can be registered and remain valid for up to 1200 days.		A	

DIGITALTRUST Self Audit



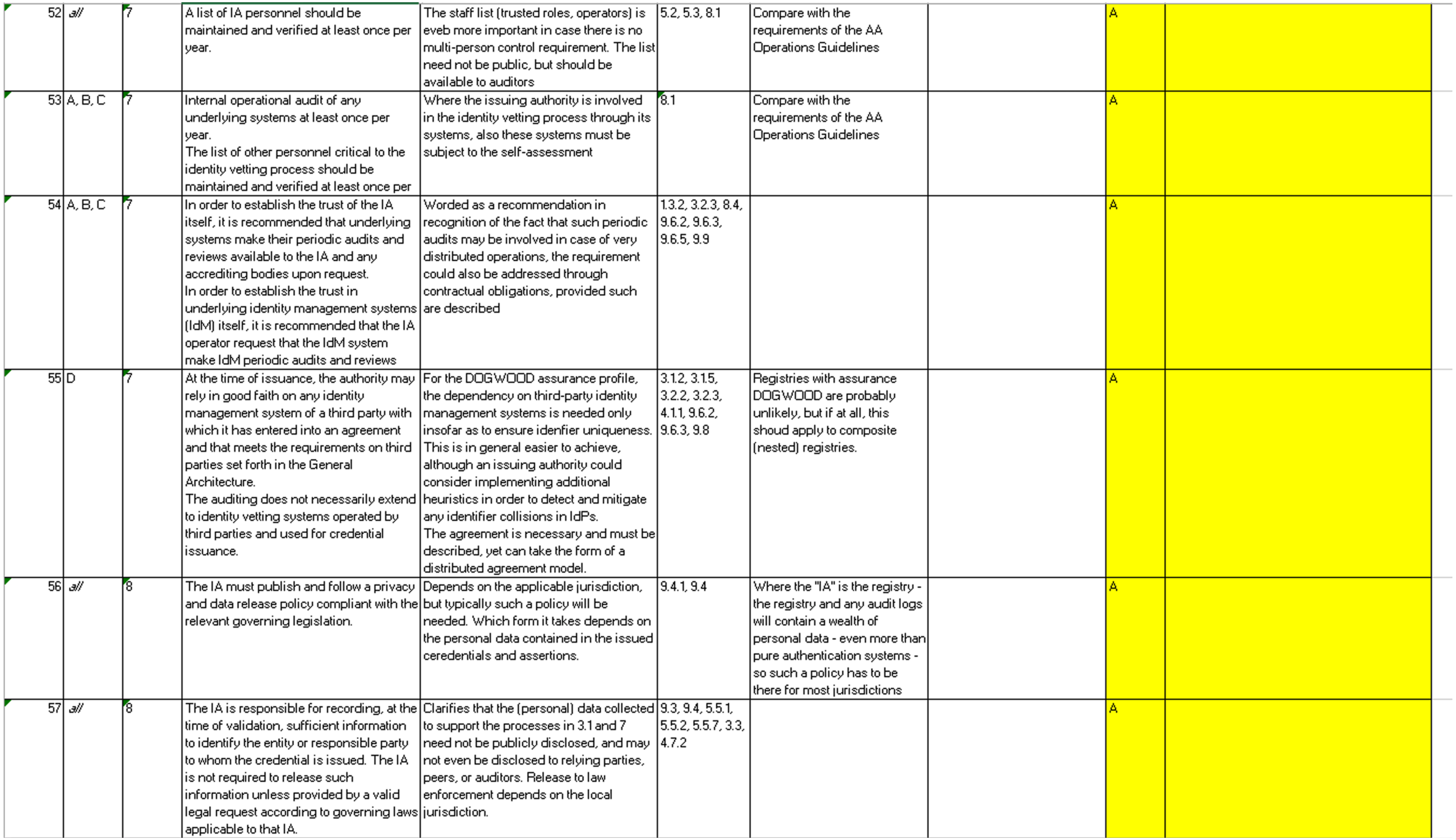
38	D	4.6	Credential life time should be no more than 400 days.	The validity period must be described and limited to approximately 13 months (corresponds to typical education and employment cycle, and is in live with most CABforum cycles). The validity may also be described in terms of validation life cycle, since issuance of a new credential implies revalidation at time of issuance.	3.3.1, 3.2.3, 4.2.3, 4.5.1, 4.6.3, 7.1	The registry must implement mechanisms to verify eligibility and member policy compliance at least every 400 days. Revalidation is subject to the same requirements of section 3.1		A	
39	D	4.6	Any third parties used for identifier (name) assignment and authentication must have a documented and verifiable relationship with the Issuing Authority, and through this relationship the Issuing Authority must have documented, verifiable and auditable means to ensure the requirements of this assurance level are met.	A mechanism for control (assessment, contractual trust, &c) must be described in the documentation. In case of a distributed process spanning multiple administrative domains, controls must be described as to how the relationships are ensured in the longer term	1.3.2, 1.3.5, 9.6.2, 9.6.5	All registrars must abide by and be aware of the registration requirements, even if the registrar network itself is distributed. The registry should likely include automated mechanisms to identify which registrar entered and updated		A	
40	all	4.7	The credentialing policies used must be identifiable by relying parties.	When presented with a credential, there should be a reasonable way for the receiving end to find the applicable policies (documents, or links thereto)	7.1.6	Where possible, issued asigned assertions should contain information on the issuer sufficient to locate its policies (e.g. through its entity ID or by other reference).	A SAML credential will have an issuer entityID with meta-data containing URIs to applicable policies	A	
41	all	5	Mechanisms must be in place to protect the systems and credentials used by the IA.		5.1, 5.2, 5.3, 5.7	If a registry issues signed assertions, its signing keys must be apprppriately protected. Guidelines could include the AA Operations Guidelines, or other service security best practices		A	
42	A, B, D	5	The authority must not knowingly continue to rely on data from third parties that provide inaccurate or fraudulent information. It is strongly recommended that any third party on which the issuing authority relies has an incident response capability and is willing to participate in resolving such incidents	A suspension mechanism for upstream sources of identity must be described that permits exclusion or suspension of such sources pending incident investigations	3.2, 3.3, 4.1, 4.2	This requirement is rlevant only in the case of a distributed network of registrars		A	
43	all	6	The IA should publish its policies or independently verified statements of trust regarding its compliance to named policies.		2.1, 2.4, 8.6, 8.7	Is there an information page for the registry? Doet that page link to (community membership) registration policies, practices, and/or an AUP?		A	

DIGITALTRUST Self Audit



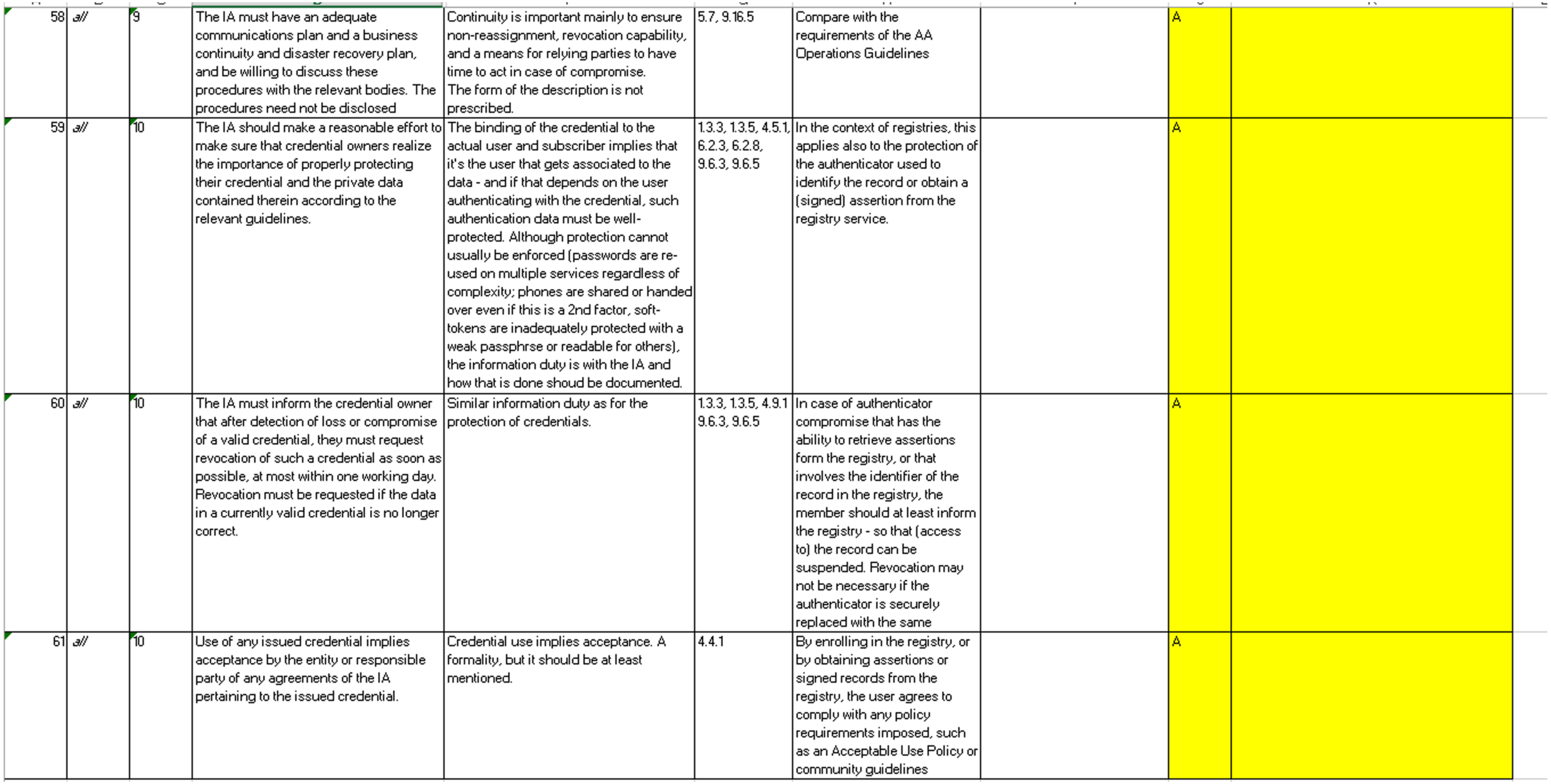
44	all	7	Sufficient information must be recorded and archived such that the association of the entity and the credential subject can be confirmed at a later date. In the event that documented traceability is lost, the identifier must never be reissued.	Is enough information recorded so that the original applicant can be associated with a new one? Is the chain of evidence maintained? In some jurisdictions, the most obvious choice (personal ID numbers, social security numbers, citizen unique IDs) are restricted by law, so another mechanism should be described and other information (e.g. signatures) recorded instead. Or the name identifier should be uniquely genered every time, yet that is rather inconvenient for subscribers	5.5.1, 5.5.2, 5.5.7, 3.3, 4.7.2	Entity information (contact details, affiliation, &c) must be archived in a way that links it to the record in the registry This information can be in te registry this acts as a persistent archive. Alternatively, information in the registry must be archived as needed (long-term backup or similar process).		A	
45	all	7	The IA must record and archive all requests for credentials, along with all issued credentials, all the requests for revocation and the login, logout, startup, and shutdown of the issuing machine.	Auditors (and self-assessment) should have access to such records to determine operational integrity. Description is required, alongside a way to storing the records in an 'immutable form'	5.4	Compare with the requirements of the AA Operations Guidelines		A	
46	all	7	The IA must keep these records for at least three years.	Description in documentation refering to archival system(s)	5.4.3	Compare with the requirements of the AA		A	
47	all	7	These records must be made available to external auditors in the course of their work as auditor.	In all other cases, access should likely be restricted to specific trusted roles	8.1, 8.4			A	
48	all	7	The IA must accept being audited by accrediting bodies and recognised relying parties to verify its compliance with the rules and procedures specified in its policy documents.	Accrediting body is an intentionally open-ended term. It might refer to the IGTF peers during a review process but also to other groups to which the authority qualifies	8.2, 8.3, 8.6			A	
49	all	7	Audit results shall be made available to the accrediting bodies upon request.	This applies in particular when an external auditor makes a statement of compliance, and the accrediting body itself has no insight in the operations. In that case, the transparency process is to be replaced by an auditable process.	8.6			A	
50	A, B, C	7	The IA or RA should have documented evidence on retaining the same identity over time. The IA is responsible for maintaining an archive of these records in an auditable form.	Even if the registration is a distributed operation, the issuing authority remains responsible for the collection. This should be described in the documentation	1.3.2, 3.2.3, 4.3.1, 5.5.6	Record identifiers within the registry must be linked to external identifiers (e.g. ones from the authenticator) in a persistent way to prevent mixup of data. This should be described		A	
51	all	7	The IA should perform internal operational audits of the IA/RA staff at least once per year to verify its compliance with the rules and procedures specified in its policies and	Self-assessment is a key element of trust in a peer-review based model, and the frequency must be describe din the documentation	8.1	Compare with the requirements of the AA Operations Guidelines		A	

DIGITALTRUST Self Audit



52	all	7	A list of IA personnel should be maintained and verified at least once per year.	The staff list (trusted roles, operators) is eveb more important in case there is no multi-person control requirement. The list need not be public, but should be available to auditors	5.2, 5.3, 8.1	Compare with the requirements of the AA Operations Guidelines		A	
53	A, B, C	7	Internal operational audit of any underlying systems at least once per year. The list of other personnel critical to the identity vetting process should be maintained and verified at least once per	Where the issuing authority is involved in the identity vetting process through its systems, also these systems must be subject to the self-assessment	8.1	Compare with the requirements of the AA Operations Guidelines		A	
54	A, B, C	7	In order to establish the trust of the IA itself, it is recommended that underlying systems make their periodic audits and reviews available to the IA and any accrediting bodies upon request. In order to establish the trust in underlying identity management systems (IdM) itself, it is recommended that the IA operator request that the IdM system make IdM periodic audits and reviews	Worded as a recommendation in recognition of the fact that such periodic audits may be involved in case of very distributed operations, the requirement could also be addressed through contractual obligations, provided such are described	1.3.2, 3.2.3, 8.4, 9.6.2, 9.6.3, 9.6.5, 9.9			A	
55	D	7	At the time of issuance, the authority may rely in good faith on any identity management system of a third party with which it has entered into an agreement and that meets the requirements on third parties set forth in the General Architecture. The auditing does not necessarily extend to identity vetting systems operated by third parties and used for credential issuance.	For the DOGWOOD assurance profile, the dependency on third-party identity management systems is needed only insofar as to ensure idenfier uniqueness. This is in general easier to achieve, although an issuing authority could consider implementing additional heuristics in order to detect and mitigate any identifier collisions in IdPs. The agreement is necessary and must be described, yet can take the form of a distributed agreement model.	3.1.2, 3.1.5, 3.2.2, 3.2.3, 4.1.1, 9.6.2, 9.6.3, 9.8	Registries with assurance DOGWOOD are probably unlikely, but if at all, this shoud apply to composite (nested) registries.		A	
56	all	8	The IA must publish and follow a privacy and data release policy compliant with the relevant governing legislation.	Depends on the applicable jurisdiction, but typically such a policy will be needed. Which form it takes depends on the personal data contained in the issued ceredentials and assertions.	9.4.1, 9.4	Where the "IA" is the registry - the registry and any audit logs will contain a wealth of personal data - even more than pure authentication systems - so such a policy has to be there for most jurisdictions		A	
57	all	8	The IA is responsible for recording, at the time of validation, sufficient information to identify the entity or responsible party to whom the credential is issued. The IA is not required to release such information unless provided by a valid legal request according to governing laws applicable to that IA.	Clarifies that the (personal) data collected to support the processes in 3.1 and 7 need not be publicly disclosed, and may not even be disclosed to relying parties, peers, or auditors. Release to law enforcement depends on the local jurisdiction.	9.3, 9.4, 5.5.1, 5.5.2, 5.5.7, 3.3, 4.7.2			A	

DIGITALTRUST Self Audit



58	all	9	The IA must have an adequate communications plan and a business continuity and disaster recovery plan, and be willing to discuss these procedures with the relevant bodies. The procedures need not be disclosed	Continuity is important mainly to ensure non-reassignment, revocation capability, and a means for relying parties to have time to act in case of compromise. The form of the description is not prescribed.	5.7, 9.16.5	Compare with the requirements of the AA Operations Guidelines		A	
59	all	10	The IA should make a reasonable effort to make sure that credential owners realize the importance of properly protecting their credential and the private data contained therein according to the relevant guidelines.	The binding of the credential to the actual user and subscriber implies that it's the user that gets associated to the data - and if that depends on the user authenticating with the credential, such authentication data must be well-protected. Although protection cannot usually be enforced (passwords are re-used on multiple services regardless of complexity; phones are shared or handed over even if this is a 2nd factor, soft-tokens are inadequately protected with a weak passphrse or readable for others), the information duty is with the IA and how that is done shoud be documented.	1.3.3, 1.3.5, 4.5.1, 6.2.3, 6.2.8, 9.6.3, 9.6.5	In the context of registries, this applies also to the protection of the authenticator used to identify the record or obtain a (signed) assertion from the registry service.		A	
60	all	10	The IA must inform the credential owner that after detection of loss or compromise of a valid credential, they must request revocation of such a credential as soon as possible, at most within one working day. Revocation must be requested if the data in a currently valid credential is no longer correct.	Similar information duty as for the protection of credentials.	1.3.3, 1.3.5, 4.9.1 9.6.3, 9.6.5	In case of authenticator compromise that has the ability to retrieve assertions form the registry, or that involves the identifier of the record in the registry, the member should at least inform the registry - so that (access to) the record can be suspended. Revocation may not be necessary if the authenticator is securely replaced with the same		A	
61	all	10	Use of any issued credential implies acceptance by the entity or responsible party of any agreements of the IA pertaining to the issued credential.	Credential use implies acceptance. A formality, but it should be at least mentioned.	4.4.1	By enrolling in the registry, or by obtaining assertions or signed records from the registry, the user agrees to comply with any policy requirements imposed, such as an Acceptable Use Policy or community guidelines		A	

DIGITALTRUST Self Audit

1 Self Audit completed through independent auditors

2 No control deemed lower than Grade A

3 Namespace may be adjusted in future

DIGITALTRUST Self Audit

Questions?

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

http://digitaltrust.ae