Certified DNS & Email Security Architect

Examination Scope: 30 Questions | 35 Minutes | Passing Standard: 80%

1. EXECUTIVE OVERVIEW & CREDENTIAL STANDARDS

Specialist certification covering DNSSEC cryptographic trust chains, CAA policy configuration, SPF 10-lookup limits, 2048-bit DK

2. KEY TOPICS & SYLLABUS

* DNSSEC root trust anchors, RRSIG, DNSKEY, and DS record chains
* CAA records: issue, issuewild, and iodef alerting
* SPF syntax, include loops, and the 10-DNS-lookup limit
* DKIM public-key cryptography, selector rotation, and canonicalization
* DMARC policy enforcement (p=none vs quarantine vs reject) and rua/ruf telemetry
* MTA-STS, TLS-RPT, and BIMI (Brand Indicators for Message Identification)

Examination Integrity & Anti-Cheat Protocols:

* Correct answer keys are evaluated strictly server-side and never sent to client devices.
* Questions and multiple-choice options are dynamically shuffled per individual session.
* Time limits are strictly enforced on the server; background blur/tab switches are audited.

CHAPTER 1: DNSSEC: Securing the Domain Name System

Cryptographic authentication of DNS records preventing DNS cache poisoning.

Standard DNS lookups are unauthenticated UDP packets easily forged by on-path attackers (Kaminsky-style DNS cache poisoning). DNSSEC signs all DNS records with asymmetric cryptography:

- RRSIG: A cryptographic signature for a specific record set (e.g. your A or MX records).
- DNSKEY: Contains the public key used by resolvers to verify RRSIG signatures.
- DS (Delegation Signer): A hash of the child zone's DNSKEY published in the parent zone (.com, .org, or country TLD), creating an unbroken cryptographic Chain of Trust leading all the way up to the ICANN Root Anchor.

```
# Querying DNSSEC validated records
dig +dnssec example.com A
# Verifying DS record presence in parent zone
dig example.com DS +trace
```

CHAPTER 2: Certification Authority Authorization (CAA)

Restricting which CAs may issue certificates and setting alert endpoints.

CAA (RFC 8659) prevents unauthorized Certificate Authorities from issuing fraudulent SSL certificates for your domain name:

- issue: Authorizes specific CAs (e.g. letsencrypt.org, digicert.com) for standard hostnames.
- issuewild: Restricts wildcard (*.domain.com) issuance specifically.
- iodef: URL or email address where CAs must report policy violation attempts.

All trusted CAs are legally mandated by the CA/Browser Forum to check CAA records before issuing certificates.

```
example.com. IN CAA 0 issue "letsencrypt.org"
example.com. IN CAA 0 issuewild ";"
example.com. IN CAA 0 iodef "mailto:security@example.com"
```

CHAPTER 3: SPF & The Strict 10-Lookup Limit

Configuring SPF syntax and avoiding broken SPF states caused by lookup exhaustion.

RFC 7208 mandates that evaluating an SPF record must not exceed 10 DNS lookups (mechanisms: include, a, mx, ptr, exists, redirect). If an SPF record requires 11 or more lookups:

Receiving mail servers immediately evaluate SPF as PermError and may reject or flag your legitimate emails as spam.

Best practice: Flatten nested SPF includes, remove unused third-party services, and terminate the record with -all (hard fail) or ~all (soft fail), never +all.

```
v=spf1 include:_spf.google.com include:mailgun.org ~all
```

© 2026 SurfaceScan · CDESA Certification Curriculum

CHAPTER 4: DKIM & DMARC Enforcement

Cryptographic email signing and enforcing p=reject against domain spoofing.

DKIM (DomainKeys Identified Mail) signs outgoing emails with a private cryptographic key, verified via public keys published in DNS TXT records.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) unifies SPF and DKIM:

- p=none: Monitoring only; no emails are blocked.
- p=quarantine: Suspicious emails failing alignment are moved to Spam folders.
- p=reject: Strictly blocks unauthorized emails at the SMTP gateway, protecting customers from phishing.

To achieve A+ on SurfaceScan, DMARC must be set to p=reject with a valid rua reporting address.

```
_dmarc.example.com. IN TXT "v=DMARC1; p=reject; sp=reject; pct=100; rua=mailto:dmarc-reports@example.com"
```