

Certificate report

Account ACME Corporation (sample) <it-ops@acme-corp.example>
Period Oct 1, 2025 to Sep 30, 2026 (days in UTC)
Generated Oct 1, 2026 08:00 UTC by CertAvert (certavert.com)
Report ID **CA-LU4C-MY8P-T3NW** · to check that this file is unchanged, open certavert.com/verify and choose it

6 endpoints (6 monitored)	100% of days checked	4,106 checks run	5 endpoints with days not OK	24 certificate changes (1 unexpected)
------------------------------	-------------------------	---------------------	---------------------------------	--

Now: 0 expired · 0 revoked · 1 accepting TLS 1.0 or 1.1. · 6 of 6 with an owner.

Account note: Prepared by IT operations for the PCI DSS v4.0.1 assessment of ACME Corporation. Questions: it-ops@acme-corp.example.

1. Certificate inventory

Each endpoint's certificate as read at its last successful check.

Endpoint	Status	Issuer	Valid from	Valid to	Key · signature	Revocation	Last read
www.acme-corp.example 192.0.2.10	OK	Let's Encrypt	Sep 2, 2026	Dec 1, 2026	EC P-256 sha256WithRSAEncryption	Not revoked (CRL, r12.c.lencr.org).	Sep 30, 2026 21:14 UTC
Owner: Web team (J. Rivera) (web@acme-corp.example) · Purpose: Public website · Group: Retail Subject: CN=www.acme-corp.example · Issuer: C=US, O=Let's Encrypt, CN=R12 Names: www.acme-corp.example, acme-corp.example Serial 24:F3:EE:1E:A1:DF:F1:78:DF:DB:0D:46:93:DE:A6:6C · SHA-256 DC:E0:C0:A6:2F:F1:97:29:D1:2D:CE:74:BF:DC:43:8D:B5:D4:B3:E4:52:39:81:76:19:BC:4D:60:0B:E8:44:E4 Alert settings now: Expiry: 30, 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: unexpected only Alert settings in the period: Oct 1, 2025 – Jan 14, 2026: Expiry: 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: unexpected only Jan 15, 2026 – Sep 30, 2026: Expiry: 30, 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: unexpected only							
shop.acme-corp.example 192.0.2.11	OK	DigiCert Inc	Mar 14, 2026	Mar 29, 2027	RSA 2048 sha256WithRSAEncryption	Not revoked (OCSP, ocsp.digicert.com).	Sep 30, 2026 21:14 UTC
Owner: E-commerce (P. Shah) (ecommerce@acme-corp.example) · Purpose: Online store and checkout (card payments) · Group: Payments Subject: C=US, ST=Delaware, L=Wilmington, O=ACME Corporation, CN=shop.acme-corp.example · Issuer: C=US, O=DigiCert Inc, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1 Names: shop.acme-corp.example, checkout.acme-corp.example Serial 77:4F:B0:D9:13:24:9B:4D:A3:2D:6D:4E:B2:1A:33:09 · SHA-256 C8:2F:E7:94:4F:00:E4:67:0F:78:27:8B:8E:96:0E:78:55:09:E3:D3:6E:68:DE:22:36:19:34:CC:5D:95:D1:08 Alert settings now: Expiry: 30, 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: every change Alert settings in the period: The same as now on every day checked							

Endpoint	Status	Issuer	Valid from	Valid to	Key · signature	Revocation	Last read
api.acme-corp.example 192.0.2.20 Owner: Platform team (L. Chen) (platform@acme-corp.example) · Purpose: Partner and mobile app API · Group: Payments Subject: CN=api.acme-corp.example · Issuer: C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV R36 Names: api.acme-corp.example Serial 69:C3:06:30:C8:1A:C0:26:E2:C4:D0:31:22:14:D5:40 · SHA-256 64:7F:0C:D8:0D:C6:52:12:28:44:2A:9E:85:63:7D:9D:93:E6:58:63:D6:2D:0C:0B:E1:8A:8F:2F:D8:9E:C9:7E Alert settings now: Expiry: 30, 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: unexpected only Alert settings in the period: The same as now on every day checked	OK	Sectigo Limited	Aug 20, 2026	Mar 7, 2027	RSA 2048 sha256WithRSAEncryption	Not revoked (CRL, crl.sectigo.com).	Sep 30, 2026 21:14 UTC
mail.acme-corp.example:465 192.0.2.25 Owner: IT operations (it-ops@acme-corp.example) · Purpose: Outgoing mail (SMTP) · Group: Retail Subject: CN=mail.acme-corp.example · Issuer: C=US, O=Let's Encrypt, CN=E7 Names: mail.acme-corp.example, smtp.acme-corp.example Serial EC:C8:24:4F:51:82:E1:DC:FC:73:E5:0A:49:A5:BA:7E · SHA-256 60:70:E1:A1:90:16:15:9C:5E:D0:30:7D:3B:1F:8C:79:B1:0B:95:84:C4:92:76:58:D7:BF:4E:F5:84:A3:9B:B2 Alert settings now: Expiry: 30, 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: unexpected only Alert settings in the period: The same as now on every day checked	Expiring	Let's Encrypt	Jul 28, 2026	Oct 26, 2026	EC P-384 ecdsa-with-SHA384	Not revoked (CRL, e7.c.lencr.org).	Sep 30, 2026 21:14 UTC
vpn.acme-corp.example:8443 198.51.100.7 Owner: IT operations (it-ops@acme-corp.example) · Purpose: Staff remote access · Group: — Subject: CN=vpn.acme-corp.example · Issuer: C=US, O=Google Trust Services, CN=WR3 Names: vpn.acme-corp.example Serial 23:A2:DE:93:BB:04:0F:14:26:89:25:B4:E2:E3:9C:B8 · SHA-256 A0:2F:43:E4:3E:F4:C2:F8:6F:5C:0E:1A:57:56:41:F1:25:42:FB:49:35:5A:A1:C9:8F:DB:46:5F:A5:C0:8C:1D Alert settings now: Expiry: 30, 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: unexpected only Alert settings in the period: The same as now on every day checked	OK	Google Trust Services	Sep 9, 2026	Dec 8, 2026	RSA 2048 sha256WithRSAEncryption	Not revoked (CRL, c.pki.goog).	Sep 30, 2026 21:14 UTC
legacy.acme-corp.example 198.51.100.40 Owner: Web team (J. Rivera) (web@acme-corp.example) · Purpose: Old ordering site, to be retired · Group: Retail Subject: CN=legacy.acme-corp.example · Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign GCC R6 AlphaSSL CA 2025 Names: legacy.acme-corp.example Serial 76:69:3C:57:CD:47:1F:20:F2:E0:DA:0B:17:23:64:21 · SHA-256 32:73:CE:70:71:61:8F:D9:43:13:46:07:BA:46:2C:52:9B:6C:84:2B:53:9D:B5:0E:4C:72:90:CE:B2:46:5D:E6 Alert settings now: Expiry: 30, 14, 7 days before and on expiry · Problems: on, reminder after 7 days · Changes: every change Alert settings in the period: The same as now on every day checked Account note: Accepted risk until the site is retired on Dec 15, 2026: its old load balancer cannot send the intermediate certificate or turn off TLS 1.0 and 1.1. No card data passes through it. Approved by J. Rivera, change CR-1987.	Warning Certificate chain incomplete	GlobalSign nv-sa	Nov 3, 2025	Nov 4, 2026	RSA 2048 sha256WithRSAEncryption	Not checked (only a trusted certificate is checked).	Sep 30, 2026 21:14 UTC

2. Daily record

Every monitored endpoint is checked about every 12 hours, and sooner while a problem is being confirmed; a day counts its worst check.

Endpoint	Days in period	Days checked	Checks	OK	Expiring	Warning	Expired	Error	Revoked
www.acme-corp.example	365	365	737	364	0	0	0	1	0
shop.acme-corp.example	365	365	732	339	26	0	0	0	0
api.acme-corp.example	365	365	737	353	12	0	0	0	0
mail.acme-corp.example:465	365	365	737	360	5	0	0	0	0
vpn.acme-corp.example:8443	213	213	430	213	0	0	0	0	0
legacy.acme-corp.example	365	365	733	14	19	332	0	0	0

Days that were not OK

Endpoint	Days	Count	Status	Problem
www.acme-corp.example	Mar 2, 2026	1	Error	Connection failed (port 443)
Account note: Hosting provider maintenance window; provider ticket #4471.				
shop.acme-corp.example	Feb 17, 2026 to Mar 14, 2026	26	Expiring	30 days or less left
api.acme-corp.example	Aug 9, 2026 to Aug 20, 2026	12	Expiring	30 days or less left
Account note: Let's Encrypt renewals failed after a firewall change; moved to Sectigo under change CR-2041.				
mail.acme-corp.example:465	Sep 26, 2026 to Sep 30, 2026	5	Expiring	30 days or less left
Account note: Renewal broke after the Sep 24 OS upgrade; fix scheduled for Oct 1 (ticket #5120).				
legacy.acme-corp.example	Oct 15, 2025 to Nov 2, 2025	19	Expiring	30 days or less left
legacy.acme-corp.example	Nov 3, 2025 to Sep 30, 2026	332	Warning	Certificate chain incomplete

3. TLS versions

Tested once a day on each endpoint's own port with OpenSSL. SSL 2.0 and 3.0 are not tested: the OpenSSL on our servers cannot offer them.

Endpoint	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Weak cipher	Last test	Days with TLS 1.0/1.1
www.acme-corp.example	Refused	Refused	Accepted	Accepted	None	Sep 30, 2026 18:50 UTC	0 of 365
shop.acme-corp.example	Refused	Refused	Accepted	Accepted	None	Sep 30, 2026 18:50 UTC	0 of 365
api.acme-corp.example	Refused	Refused	Accepted	Accepted	None	Sep 30, 2026 18:50 UTC	0 of 365
mail.acme-corp.example:465	Refused	Refused	Accepted	Accepted	None	Sep 30, 2026 18:50 UTC	0 of 365

Endpoint	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	Weak cipher	Last test	Days with TLS 1.0/1.1
vpn.acme-corp.example:8443	Refused	Refused	Accepted	Accepted	None	Sep 30, 2026 18:50 UTC	0 of 213
legacy.acme-corp.example	Accepted	Accepted	Accepted	Refused	None	Sep 30, 2026 18:50 UTC	365 of 365

4. Certificate changes

Detected (UTC)	Endpoint	Issuer	New valid to	Key	Routine or unexpected
Oct 6, 2025 06:20	mail.acme-corp.example:465	Let's Encrypt	Jan 4, 2026	New	Routine
New SHA-256 1B:EF:11:00:81:5A:2D:91:3F:F8:7F:0F:FE:89:97:60:89:21:4B:B7:78:5E:5B:71:6D:BE:5B:6D:66:EB:22:03 · read from 192.0.2.25					
Oct 17, 2025 05:12	api.acme-corp.example	Let's Encrypt	Jan 15, 2026	New	Routine
New SHA-256 E7:2E:ED:20:45:C5:89:FC:DB:72:73:C0:6E:B8:3E:20:13:FF:E8:34:58:FA:A2:BA:04:9B:F8:3B:0D:BE:ED:2E · read from 192.0.2.20					
Nov 3, 2025 10:20	legacy.acme-corp.example	GlobalSign nv-sa	Nov 4, 2026	New	Routine
New SHA-256 32:73:CE:70:71:61:8F:D9:43:13:46:07:BA:46:2C:52:9B:6C:84:2B:53:9D:B5:0E:4C:72:90:CE:B2:46:5D:E6 · read from 198.51.100.40					
Nov 11, 2025 03:41	www.acme-corp.example	Let's Encrypt	Feb 9, 2026	New	Routine
New SHA-256 3C:11:FA:C9:74:2F:CF:9D:94:69:5F:DD:46:B6:F9:28:F5:C0:CF:03:24:E1:A5:89:98:31:D3:E2:23:D8:9F:37 · read from 192.0.2.10					
Dec 4, 2025 06:20	mail.acme-corp.example:465	Let's Encrypt	Mar 4, 2026	New	Routine
New SHA-256 29:77:65:F4:75:88:22:F0:96:E0:14:8A:B9:05:D6:77:1E:25:CE:A7:A8:0F:21:63:88:DB:44:BD:FE:36:38:BD · read from 192.0.2.25					
Dec 15, 2025 05:12	api.acme-corp.example	Let's Encrypt	Mar 15, 2026	New	Routine
New SHA-256 78:16:2E:91:ED:2B:C2:F8:7D:1D:32:4A:A1:5D:75:52:BC:26:40:9B:15:AA:69:3C:7A:3E:51:3F:6E:EE:93:2A · read from 192.0.2.20					
Jan 9, 2026 03:41	www.acme-corp.example	Let's Encrypt	Apr 9, 2026	New	Routine
New SHA-256 03:49:26:20:6D:65:3A:16:D8:4F:4B:8B:9D:8C:FB:0E:87:20:87:C2:14:3D:A4:20:D4:A1:42:CF:40:8E:2B:A1 · read from 192.0.2.10					
Feb 1, 2026 06:20	mail.acme-corp.example:465	Let's Encrypt	May 2, 2026	New	Routine
New SHA-256 E0:74:0F:DD:0E:6A:37:03:65:74:50:16:D1:7A:57:23:BF:36:C9:AF:5F:24:EF:C9:01:D2:48:68:CE:59:8B:BA · read from 192.0.2.25					
Feb 12, 2026 05:12	api.acme-corp.example	Let's Encrypt	May 13, 2026	New	Routine
New SHA-256 45:13:98:5A:A7:6A:C1:96:DD:7A:C1:18:7B:09:46:5D:3F:E8:34:DB:43:D5:80:B4:5E:B7:C5:5A:59:F8:E5:0A · read from 192.0.2.20					
Mar 9, 2026 03:41	www.acme-corp.example	Let's Encrypt	Jun 7, 2026	New	Routine
New SHA-256 4E:FC:DE:A0:F3:33:70:BC:F4:43:13:02:59:45:37:A5:0E:67:6C:F9:D7:B0:C3:15:21:E5:FB:DD:91:A2:0D:D6 · read from 192.0.2.10					
Mar 14, 2026 09:12	shop.acme-corp.example	DigiCert Inc	Mar 29, 2027	New	Routine
Added: checkout.acme-corp.example					
New SHA-256 C8:2F:E7:94:4F:00:E4:67:0F:78:27:8B:8E:96:0E:78:55:09:E3:D3:6E:68:DE:22:36:19:34:CC:5D:95:D1:08 · read from 192.0.2.11					
Mar 16, 2026 04:05	vpn.acme-corp.example:8443	Google Trust Services	Jun 14, 2026	New	Routine
New SHA-256 18:A4:F0:D0:E7:61:23:40:68:6F:D1:D6:CC:4D:37:CD:D2:3D:95:D0:42:CF:AF:DF:4F:8E:E6:D2:73:05:B2:90 · read from 198.51.100.7					

Detected (UTC)	Endpoint	Issuer	New valid to	Key	Routine or unexpected
Apr 1, 2026 06:20	mail.acme-corp.example:465	Let's Encrypt	Jun 30, 2026	New	Routine
New SHA-256 60:82:2A:CC:46:E6:9A:E9:D1:0A:D8:91:FE:5B:C1:C1:85:4D:DB:32:56:B9:E6:18:7A:08:C7:42:FB:DB:26:57 · read from 192.0.2.25					
Apr 12, 2026 05:12	api.acme-corp.example	Let's Encrypt	Jul 11, 2026	New	Routine
New SHA-256 E5:E1:3A:A3:57:80:10:6B:B3:E0:AC:62:4B:14:11:0A:D5:7E:10:45:40:78:CA:EB:4C:1F:88:57:00:AC:83:96 · read from 192.0.2.20					
May 7, 2026 03:41	www.acme-corp.example	Let's Encrypt	Aug 5, 2026	New	Routine
New SHA-256 71:55:A3:53:08:23:61:8E:5F:84:26:5C:16:FC:62:00:B6:F6:7C:20:6C:7F:48:10:D9:D6:AB:59:61:44:3F:0A · read from 192.0.2.10					
May 14, 2026 04:05	vpn.acme-corp.example:8443	Google Trust Services	Aug 12, 2026	New	Routine
New SHA-256 F5:F5:C3:7A:35:AF:A6:00:B2:B4:F7:A1:7C:9A:8E:4B:5A:9E:2C:80:90:AB:A6:44:85:95:E2:7C:32:DA:5F:A8 · read from 198.51.100.7					
May 30, 2026 06:20	mail.acme-corp.example:465	Let's Encrypt	Aug 28, 2026	New	Routine
New SHA-256 80:FF:E3:73:2D:7D:47:96:0A:46:C5:2D:93:35:D1:54:82:42:EA:35:6B:1C:2E:B4:AA:03:C9:8C:62:BF:CD:D5 · read from 192.0.2.25					
Jun 10, 2026 05:12	api.acme-corp.example	Let's Encrypt	Sep 8, 2026	New	Routine
New SHA-256 9C:46:E4:34:7F:4D:E8:58:A3:F1:F8:4D:03:23:E7:57:39:72:69:EE:D9:75:84:BF:5F:6A:EA:CC:1F:B0:58:BD · read from 192.0.2.20					
Jul 5, 2026 03:41	www.acme-corp.example	Let's Encrypt	Oct 3, 2026	New	Routine
New SHA-256 D1:D5:14:7A:3F:46:3C:BE:75:33:DB:CA:89:D7:A0:E7:C0:88:30:DA:3B:A7:45:7B:70:5D:B2:C6:BB:6A:08:99 · read from 192.0.2.10					
Jul 12, 2026 04:05	vpn.acme-corp.example:8443	Google Trust Services	Oct 10, 2026	New	Routine
New SHA-256 64:7E:DB:7A:E7:99:09:94:D8:A7:16:A5:50:70:E6:B0:7C:FF:ED:B8:29:DE:5F:68:B5:08:1A:D0:46:A9:3A:03 · read from 198.51.100.7					
Jul 28, 2026 06:20	mail.acme-corp.example:465	Let's Encrypt	Oct 26, 2026	New	Routine
New SHA-256 60:70:E1:A1:90:16:15:9C:5E:D0:30:7D:3B:1F:8C:79:B1:0B:95:84:C4:92:76:58:D7:BF:4E:F5:84:A3:9B:B2 · read from 192.0.2.25					
Aug 20, 2026 14:03	api.acme-corp.example	Let's Encrypt → Sectigo Limited	Mar 7, 2027	New	Unexpected: Issued by a different certificate authority; Names were removed Removed: api-v1.acme-corp.example
New SHA-256 64:7F:0C:D8:0D:C6:52:12:28:44:2A:9E:85:63:7D:9D:93:E6:58:63:D6:2D:0C:0B:E1:8A:8F:2F:D8:9E:C9:7E · read from 192.0.2.20					
Account note: Planned move to Sectigo, change CR-2041. api-v1 was retired on Aug 1.					
Sep 2, 2026 03:41	www.acme-corp.example	Let's Encrypt	Dec 1, 2026	New	Routine
New SHA-256 DC:E0:C0:A6:2F:F1:97:29:D1:2D:CE:74:BF:DC:43:8D:B5:D4:B3:E4:52:39:81:76:19:BC:4D:60:0B:E8:44:E4 · read from 192.0.2.10					
Sep 9, 2026 04:05	vpn.acme-corp.example:8443	Google Trust Services	Dec 8, 2026	New	Routine
New SHA-256 A0:2F:43:E4:3E:F4:C2:F8:6F:5C:0E:1A:57:56:41:F1:25:42:FB:49:35:5A:A1:C9:8F:DB:46:5F:A5:C0:8C:1D · read from 198.51.100.7					

5. Names in the public certificate logs that are not monitored

Names with certificates in the Certificate Transparency logs (crt.sh, Cert Spotter) under this account's domains that none of its domains or certificates cover.

Domain	Name	Acknowledged	Note	Looked up
acme-corp.example	staging.acme-corp.example	No	—	Sep 30, 2026 06:15 UTC
acme-corp.example	status.acme-corp.example	Yes	Hosted by our status page provider	Sep 30, 2026 06:15 UTC

6. Alerts sent

Every email went to all of the account's alert addresses at the time, and to its Slack or Discord channels. Each endpoint's alert settings, as they are now, are in section 1.

Sent (UTC)	Endpoint	Alert	To	Channels
Oct 15, 2025 07:02	legacy.acme-corp.example	SSL expiring in 30 days	it-ops@acme-corp.example, security@acme-corp.example	1
Oct 31, 2025 07:01	legacy.acme-corp.example	SSL expiring in 14 days	it-ops@acme-corp.example, security@acme-corp.example	1
Nov 3, 2025 10:50	legacy.acme-corp.example	Certificate changed	it-ops@acme-corp.example, security@acme-corp.example	1
Nov 3, 2025 10:51	legacy.acme-corp.example	SSL problem	it-ops@acme-corp.example, security@acme-corp.example	1
Nov 10, 2025 10:55	legacy.acme-corp.example	SSL problem still there	it-ops@acme-corp.example, security@acme-corp.example	1
Feb 17, 2026 07:00	shop.acme-corp.example	SSL expiring in 30 days	it-ops@acme-corp.example, security@acme-corp.example	1
Mar 2, 2026 08:31	www.acme-corp.example	SSL problem	it-ops@acme-corp.example, security@acme-corp.example	1
Mar 2, 2026 20:04	www.acme-corp.example	SSL problem resolved	it-ops@acme-corp.example, security@acme-corp.example	1
Mar 5, 2026 07:00	shop.acme-corp.example	SSL expiring in 14 days	it-ops@acme-corp.example, security@acme-corp.example	1
Mar 12, 2026 07:01	shop.acme-corp.example	SSL expiring in 7 days	it-ops@acme-corp.example, security@acme-corp.example	1
Mar 14, 2026 09:44	shop.acme-corp.example	Certificate changed	it-ops@acme-corp.example, security@acme-corp.example	1
Aug 9, 2026 07:03	api.acme-corp.example	SSL expiring in 30 days	it-ops@acme-corp.example, security@acme-corp.example	1
Aug 20, 2026 14:35	api.acme-corp.example	Unexpected certificate change	it-ops@acme-corp.example, security@acme-corp.example	1
Sep 26, 2026 07:04	mail.acme-corp.example:465	SSL expiring in 30 days	it-ops@acme-corp.example, security@acme-corp.example	1

7. Scope and method

- Endpoints are the domains and ports added to this account; deleted domains are not included. Each is checked from CertAvert's servers on the public internet, like any visitor.
- Trust: verified with OpenSSL against the server's trusted root certificates (the ca-certificates package, built from Mozilla's root store), including the name match. TLS 1.2 or newer is required to read a certificate.

- **Revocation:** asked of the certificate authority, through the OCSP responder (RFC 6960) or else the CRL (RFC 5280) the certificate names; every answer's signature is verified. Only trusted certificates are checked.
- **Certificate changes:** a new SHA-256 fingerprint at a check; routine when the same authority renewed it near its end, with no names removed.
- **Not covered:** certificates on internal networks or not added to this account, private key storage and handling, and your own procedures.
- **Account notes** are written by the account holder and printed as written; CertAvert does not check them.
- **Integrity:** CertAvert keeps the SHA-256 fingerprint of every file of this report, not the report itself. Anyone can check that a copy is unchanged at certavert.com/verify.

8. References

Where the sections above may serve as evidence. This report records what CertAvert observed; it is not an assessment or attestation of compliance with any standard, and your assessor decides what evidence is sufficient.

Standard	Reference	In short	Sections
PCI DSS v4.0.1	4.2.1	Strong cryptography and security protocols safeguard PAN during transmission over open, public networks; this includes confirming that certificates are valid and not expired or revoked, and that only secure protocol versions are supported.	1, 2, 3
PCI DSS v4.0.1	4.2.1.1	An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	1, 4, 5
ISO/IEC 27001:2022	Annex A 5.9	Inventory of information and other associated assets.	1, 5
ISO/IEC 27001:2022	Annex A 8.24	Use of cryptography.	1, 3, 4
SOC 2 (AICPA Trust Services Criteria)	CC6.7	Restricting and protecting information during transmission, movement or removal; its points of focus include encryption or secure channels for data in transmission.	2, 3

9. How to read this report

Endpoint	A domain name and port added to the account, checked as a visitor from the internet would reach it.
Status (section 1)	The endpoint's status at its last check.
Alert settings now	The endpoint's alert settings when the report was generated: the days before expiry that send an email, problem emails and their reminder, and which certificate changes are emailed. Section 6 lists the alerts actually sent.
Alert settings in the period	The alert settings recorded with each day's checks, as date ranges. Days before CertAvert began recording them show none.
Days in period	The days of the period the endpoint was in the account (from the day it was added).
Days checked	The days with at least one check.
Checks	Every check run in the period: about two a day, and one more each time a problem or a new certificate is confirmed.
OK, Expiring, Warning, Expired, Error	How many days had that status. Each day counts once, under its worst check of the day; the days need not be in a row. "Days that were not OK" lists each run of days in a row.
OK	Trusted, the name matches, and more than 30 days left.
Expiring	30 days or less left (whole days, rounded down).

Warning	A certificate was read but is not trusted (self-signed, unknown issuer, name mismatch), or its certificate chain has a problem.
Expired	Past its end date.
Error	No certificate could be read (name not found, connection refused or timed out, TLS older than 1.2), or the certificate was revoked.
Revoked	Days the certificate authority answered that the certificate was revoked. They are also counted under Error.
Started	In "Days that were not OK": the run began before the period, on that day.
Days with TLS 1.0/1.1	Of the days the daily TLS test ran, those on which the endpoint accepted TLS 1.0 or 1.1.
Routine change	Renewed by the same certificate authority near its end, with no names removed.
Unexpected change	Issued by another certificate authority, names removed, replaced long before its end, or older than the certificate it replaced.
Key	New: the certificate has a new key pair. Same: the previous key was kept.
Acknowledged (section 5)	The account marked the name as known and not needing monitoring.
Account note	Written by the account holder for the reader of this report. Printed as written; CertAvert does not check it.
Report ID	Identifies this report. CertAvert keeps the SHA-256 fingerprint of each of its files; at certavert.com/verify anyone can check that a file is the one CertAvert generated, unchanged.