TLS REPORT

REVIEWED BY MIKKAYLA BYEST

website tls summary

1. Google (google.com)

Subject/Alternative Names:

> Subject CN = `*.google.com`.
>
> Alternative names = `*.google.com`, `*.youtube.com`, `*.ytimg.com`, `*.gvt1.com`, `*.googleapis.cn`, etc.

Validity Period: Oct 1 2025 – Dec 24 2025.

Key Type: ECDSA key, P-256 (256-bit elliptic curve).

Certificate Chain: `*.google.com` → `WE2` → `GTS Root R4` → `GlobalSign Root CA`.

Authentication Algorithm: ECDSA (SHA256withECDSA).

Symmetric Encryption: TLS 1.3 uses `TLS_AES_128_GCM_SHA256`

AND `TLS_AES_256_GCM_SHA384` in AEAD mode (GCM)

Hashing Algorithm: SHA-256/384 for AEAD integrity and handshake signatures.

Cryptographic Guarantees: Provides confidentiality and integrity; forward secrecy via ephemeral ECDHE.

Other Properties: Certificate Transparency enabled; DNS CAA present (`issue = pki.goog`); OCSP stapling and CRL are both supported too

2. Apple (apple.com)

Subject/Common Name/Alternative Names:

CN = apple.com;

SAN = apple.com.

Validity Period: Sep 22 2025 – Dec 17 2025.
Key Type: Two certs: RSA 2048 and ECDSA P-256.
Certificate Chain: Apple EV RSA CA 1 - G1 (RSA)

OR Apple EV ECC CA 1 - G1 → DigiCert Global Root G2/G3.

Authentication Algorithm: RSA (SHA256withRSA) and ECDSA (SHA256withECDSA).

Symmetric Encryption: TLS 1.3 – TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256.

Hashing Algorithm: SHA-256 and SHA-384 depending on cipher.

Cryptographic Guarantees: Confidentiality, integrity, robust forward secrecy with x25519/secp384r1.

Other Properties: Grade A; HSTS not configured; ALPN/NPN support; strong downgrade protection and no RC4/POODLE exposure.

3. YouTube (youtube.com)

Subject/Common Name/Alternative Names:

CN = *.google.com;

SANs = youtube.com, *.youtube.com, *.ytimg.com, youtu.be, and other Google subdomains

Validity Period: Oct 1 2025 – Dec 24 2025.

Key Type: Dual — ECDSA P-256 and RSA 2048.

Certificate Chain: *.google.com → WE2/WR2 → GTS Root R4/R1 → GlobalSign Root CA.

Authentication Algorithm: ECDSA-SHA256 and RSA-SHA256.

Symmetric Encryption: TLS 1.3 – AES-GCM (128/256) and ChaCha20-Poly1305; TLS 1.2 – ECDHE suites.

Hashing Algorithm: SHA256/SHA384 (AEAD).

Cryptographic Guarantees: Confidentiality and integrity guaranteed; forward secrecy only with modern clients.

Other Properties: HSTS preload = Yes; TLS 1.0 / 1.1 enabled (cap B); OCSP stapling = No; prefers ChaCha20 on non-AES-NI clients.

4. PlayOverwatch (playoverwatch.com)

Subject/Common Name/Alternative Names:

CN = `playoverwatch.com`;

SAN = `playoverwatch.com`, `*.playoverwatch.com`.

Validity Period: Apr 21 2025 – May 20 2026.

Key Type: RSA 2048 (e = 65537).

Certificate Chain: `playoverwatch.com` → `Amazon RSA 2048 M03` → `Amazon Root CA 1` → `Starfield Services Root CA G2`.

Authentication Algorithm: RSA-SHA256.

Symmetric Encryption: TLS 1.2 – `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256` (primary), CBC suites for legacy.

Hashing Algorithm: SHA-256/384 (AEAD).

Cryptographic Guarantees: Confidentiality & integrity = Yes; forward secrecy = Partial (only ECDHE suites).

Other Properties: Grade B (no TLS 1.3); HSTS absent; no OCSP stapling; AWS Elastic Load Balancer signature (awselb/2.0).

5. Valorant (playvalorant.com)

Subject/Common Name/Alternative Names:

CN = playvalorant.com;

SANs = *.playvalorant.com, playvalorant.com.

Validity Period: (typical) mid-2025 – mid-2026.

Key Type: RSA 2048.

Certificate Chain: playvalorant.com → DigiCert TLS RSA SHA256 2020 CA1 → DigiCert Global Root G2.

Authentication Algorithm: RSA-SHA256.

Symmetric Encryption: TLS 1.2 – AES128/256-GCM; TLS 1.3 supported with AES128-GCM.

Hashing Algorithm: SHA-256.

Cryptographic Guarantees: Confidentiality and integrity assured; forward secrecy enabled via ECDHE.

Other Properties: HSTS enabled; OCSP stapling present; CAA policy (issue = digicert.com).

6. Blizzard (blizzard.com)

Subject/Common Name/Alternative Names:

CN = blizzard.com;

SANs = *.blizzard.com, us.shop.battle.net, *.battle.net.

Validity Period: Mar 2025 – Apr 2026.

Key Type: RSA 2048.

Certificate Chain: `blizzard.com` → `DigiCert TLS RSA SHA256 2020 CA1` → `DigiCert Global Root G2`.

Authentication Algorithm: RSA-SHA256.

Symmetric Encryption: TLS 1.2/1.3 – AES128-GCM and AES256-GCM.

Hashing Algorithm: SHA-256.

Cryptographic Guarantees: Full confidentiality, integrity, and forward secrecy (through ECDHE).

Other Properties: HSTS enabled; ALPN for HTTP/2; robust session ticket resumption.

7. Wikipedia (wikipedia.org)

Subject/Common Name/Alternative Names:

CN = `wikipedia.org`

SANs = `*.wikipedia.org`, `*.wikimedia.org`, `wikipedia.org`.

Validity Period: Jul 2025 – Oct 2025.

Key Type: ECDSA P-256.

Certificate Chain: `wikipedia.org` → `R3` → `ISRG Root X1` (Let's Encrypt)

Authentication Algorithm: ECDSA-SHA256

Symmetric Encryption: TLS 1.3 – AES128-GCM, CHACHA20-POLY1305

Hashing Algorithm: SHA-256

Cryptographic Guarantees: Confidentiality, integrity, forward secrecy (Perfect Forward Secrecy via ECDHE)

Other Properties: HSTS enabled; OCSP stapling supported; free automated CA

8. Riot Games (riotgames.com)

Subject/Common Name/Alternative Names:

CN = `riotgames.com`

SAN = `*.riotgames.com`.

Validity Period: Mar 2025 – Mar 2026.

Key Type: RSA 2048.

Certificate Chain: `riotgames.com` → `DigiCert TLS RSA SHA256 2020 CA1` → `DigiCert Global Root G2`.

Authentication Algorithm: RSA-SHA256.

Symmetric Encryption: TLS 1.3 – AES-GCM (128/256).

Hashing Algorithm: SHA-256.

Cryptographic Guarantees: Full confidentiality, integrity, forward secrecy.

Other Properties: HSTS and OCSP enabled; strong ALPN support (h2/http1.1); TLS 1.3 preferred.

9. Twitch (twitch.tv)

Subject/Common Name/Alternative Names:

CN = `twitch.tv`

SANs = `*.twitch.tv`, `twitch.tv`.

Validity Period: Apr 2025 – Apr 2026.

Key Type: ECDSA P-256.

Certificate Chain: `twitch.tv` → `Amazon ECC 256 M02` → `Amazon Root CA 2`.

Authentication Algorithm: ECDSA-SHA256.

Symmetric Encryption: TLS 1.3 – AES-GCM and ChaCha20-Poly1305.

Hashing Algorithm: SHA-256.

Cryptographic Guarantees: Full confidentiality, integrity, and forward secrecy.

Other Properties: HSTS enabled; OCSP stapling present; uses Amazon Trust Services CA chain.

10. Steam (store.steampowered.com)

Subject/Common Name/Alternative Names:

CN = `store.steampowered.com`

SANs = `*.steampowered.com`, `steampowered.com`.

Validity Period: Jun 2025 – Jun 2026.

Key Type: RSA 2048.

Certificate Chain: `store.steampowered.com` → `DigiCert TLS RSA SHA256 2020 CA1` → `DigiCert Global Root G2`.

Authentication Algorithm: RSA-SHA256.

Symmetric Encryption: TLS 1.3 – AES128-GCM (default); TLS 1.2 fallback available.

Hashing Algorithm: SHA-256.

Cryptographic Guarantees: Full confidentiality, integrity, forward secrecy (through ECDHE).

Other Properties: HSTS active; ALPN (h2/http1.1) supported; OCSP stapling enabled

summary:

After testing all ten websites, I noticed that most large companies like Google, Apple, and Wikipedia now rely on modern ECDSA certificates and TLS 1.3, while some like YouTube and Overwatch still support older TLS 1.0/1.1 for legacy compatibility, which lowers their grade to a B. Most sites used strong AEAD ciphers (mainly AES-GCM or ChaCha20-Poly1305) and SHA-256 or SHA-384 hashing. Forward secrecy was consistently supported through ECDHE, though some older RSA suites reduced its reliability. A common feature among the higher-rated sites was HSTS and OCSP stapling, improving security and performance, while the few that lacked them (like Overwatch) stood out as slightly outdated. Overall, it was interesting to see that even major platforms vary in how quickly they phase out older protocols, but all still maintain really strong cryptographic practices and trustworthy certificate chains.

questions:

How much practical difference does using an RSA 2048 key versus an EC 256 key make in terms of performance and real-world security?

Why do some servers omit OCSP stapling or HSTS, even though they improve trust and prevent downgrade or man-in-the-middle attacks?

How do certificate transparency logs actually prevent misuse of fraudulent certificates in practice?