Cryptographic Protocol Design for LocalMart

KV6009 Advanced Security

Abdulla AlBassam · W23055814 · May 4th 2026

Confidentiality: Protecting Customer Data

Key Exchange

ECDHE on NIST P-256

Asymmetric · forward secrecy

NIST SP 800-56A

Bulk Encryption

AES-256-GCM

Symmetric AEAD · per-record nonce

FIPS 197

TLS Cipher Suite

TLS_AES_256_GCM_SHA384

Negotiated in TLS 1.3 handshake

RFC 8446

Forward secrecy: per-session ECDHE produces shared secret S = d_A · Q_B and is discarded after the handshake. Past traffic stays safe even if long-term keys leak.

Key Custody

Who	Long-term keys	Per-session keys	Sees
Certificate Authority	Root signing key	—	Issues server certs
LocalMart server	X.509 private key	Ephemeral ECDHE pair	Cart, address, never PAN
Customer browser	—	Ephemeral ECDHE pair	LocalMart public key + AES key
Stripe gateway	TLS + tokenisation keys	—	PAN (tokenised)

When? Keys generated at handshake → derived via HKDF → AES-256-GCM per record → discarded at session end.

TLS 1.3 Handshake

How the secure channel is established

1

Client Hello

Client offers AEAD ciphers, signature schemes, and an ephemeral ECDHE public key.

2

Server Hello

Server picks TLS_AES_256_GCM_SHA384, sends its ECDHE share, X.509 certificate, and CertificateVerify signature.

3

Shared Secret

Both sides compute S = d_A · Q_B and derive handshake + traffic keys via HKDF.

4

Encrypted Records

Client Finished + first request encrypted under AES-256-GCM. Ephemeral keys destroyed at session end.

RFC 8446 · Rescorla, 2018 · RFC 5869 · Krawczyk & Eronen, 2010 (HKDF) · Sullivan, 2018

Integrity: Detecting Tampering

In Transit

AES-256-GCM Authentication Tag

128-bit GHASH tag over GF(2^{128}), computed across ciphertext + AAD per record. Random forgery probability: $1 / 2^{128}$.

NIST SP 800-38D · Dworkin, 2007

At Rest

HMAC-SHA-256 Audit Tag

Per-order tag, server-held key. 256-bit output → birthday bound 2^{128}. Avalanche: ~half the bits flip per single-bit change in input.

FIPS 198-1 · NIST, 2008

Avalanche example: Flipping quantity 3 → 30 produces a completely different audit tag

```
"Order #1234: 2x cat food, 3x pickles, 2x trash bags - £20.00"
openssl dgst -sha256 -hmac "localmart-audit-key"
SHA2-256(stdin)= 7e2aad94679ef4c1b963870a28...

"Order #1224: 2x cat food, 30x pickles, 2x trash bags - £20.00"
openssl dgst -sha256 -hmac "localmart-audit-key"
SHA2-256(stdin)= a4f2e8d9c1bfgu7tfdt7dv87...  (completely different)
```

Cafe Wi-Fi MITM: flips 3 → 30: GCM tag check fails, record dropped, connection torn down.

Authentication: Verifying Identities

Server → Customer

X.509 Certificates

CA signs the certificate → server presents it on TLS handshake → browser verifies via the trust chain (root pre-installed).

Attack

Phishing site impersonates localmart.com to harvest credentials.

Why it fails

Forging a valid cert = breaking RSA-2048 (2^{112} operations) or finding a SHA-256 collision (2^{128}). Both infeasible. Browser detects the mismatch → TLS aborts before the password leaves the device.

RFC 5280 · Cooper et al., 2008

Customer → Server

bcrypt + JWT

1. Customer submits email + password over TLS.
2. Server verifies against bcrypt hash (cost 12).
3. Server issues HMAC-SHA-256 signed JWT (15–30 min).
4. Browser sends JWT per request; signature validated.

Attack

Stolen credential database → brute-force on password hashes.

Why it fails

bcrypt cost 12 = 4 hashes/sec/core. An 8-char alphanumeric password ($62^8 = 2.2\times10^{14}$ candidates) takes 1.7 million CPU years to exhaust. JWT forgery requires a 256-bit HMAC key = 2^{256} opperations.

RFC 7519 · Jones, Bradley & Sakimura, 2015

Security Analysis: Threat Defences

Eavesdropping

TLS 1.3 encrypts all data with AES-256-GCM; handshake itself is encrypted after Server Hello.

RFC 8446 · Rescorla, 2018

Man-in-the-Middle

X.509 certs verified via CA trust chain; CertificateVerify proves the server holds the private key.

RFC 5280; RFC 8446 §4.4.3

Replay Attack

TLS sequence numbers in IV; ephemeral session keys.

RFC 8446 §5.3 · Rescorla, 2018

Tampering

GCM auth tag detects in-transit modification; HMAC-SHA-256 audit tag protects stored orders.

NIST SP 800-38D; FIPS 198-1

Session Hijacking

Short-lived JWTs (15–30 min) over TLS only; HMAC-SHA-256 signed; refresh-token rotation.

RFC 7519; RFC 9700

Brute Force

bcrypt cost 12 (3–4 attempts/sec); rate limiting on login; optional MFA.

Provos & Mazières, 1999; OWASP, n.d.

Defence-in-depth

Transport	Credential	Session	Record	At-rest	PCI scope
TLS 1.3	bcrypt	JWT	GCM tag	HMAC-SHA-256	tokenisation

Limitations & Compliance

Limitations

No Client Certificates

Security rests on password strength; mitigated by MFA.

CA Trust Dependency

Compromised CA → MITM (DigiNotar). Fix: CT logs + CAA.

Hoogstraaten, 2012; RFC 6962; RFC 8659

Payment Gateway Trust

Stripe breach risk; PCI-DSS Level 1 + SLAs.

PCI SSC, 2024

TLS 1.3 0-RTT Risk

0-RTT is replay-vulnerable; disabled for state changes.

RFC 8446 §8 · Rescorla, 2018

bcrypt over Argon2id

Argon2id = OWASP first pick; bcrypt cost 12 above min.

RFC 9106; OWASP, n.d.

Compliance

PCI-DSS Req 4.2.1

Strong cryptography for PAN in transit (TLS 1.3 + AES-256-GCM).

PCI SSC, 2024

PCI-DSS Req 8

Strong authentication (bcrypt cost 12 + signed JWT).

PCI SSC, 2024

GDPR Art. 32

Appropriate technical measures (AES-256-GCM, audit trail).

EU Parliament & Council, 2016

GDPR Art. 25

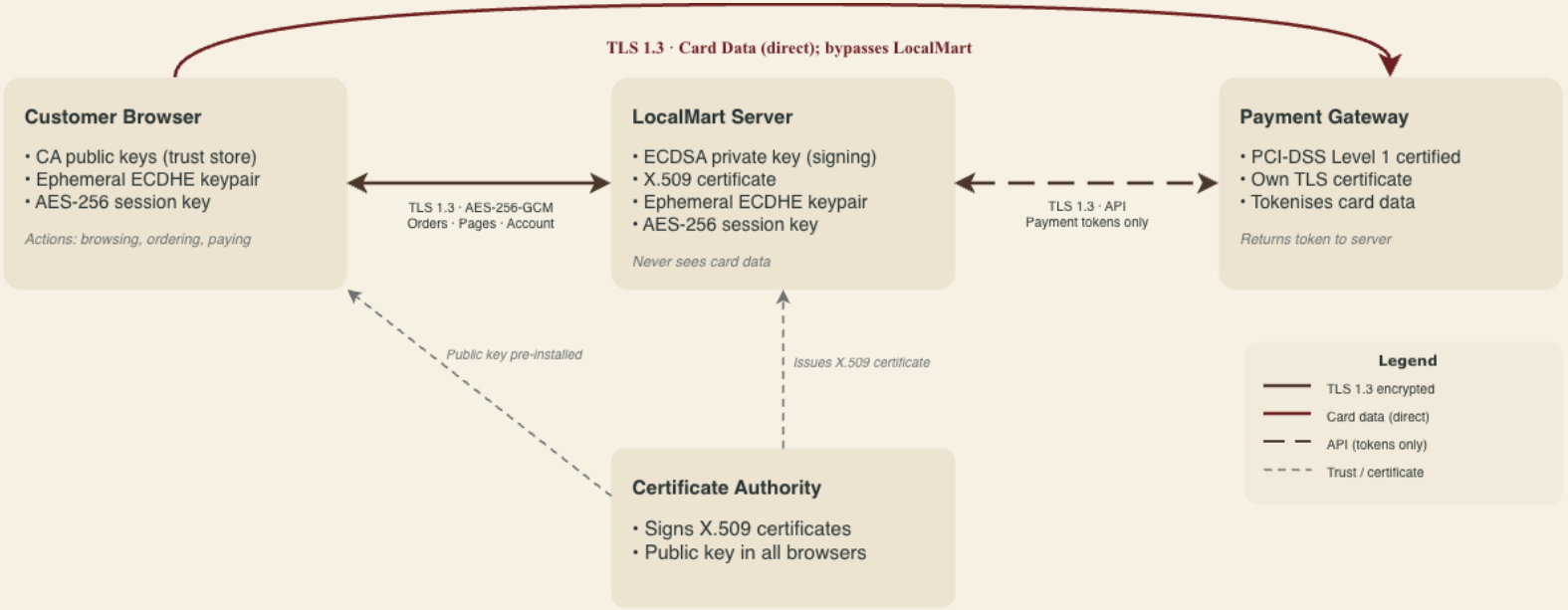
Privacy by design; data minimisation; tokenised PANs.

EU Parliament & Council, 2016

Security Posture

Criteria	Before	After
Data in Transit	Plaintext HTTP. Orders, passwords, card fields readable in transit.	TLS 1.3: ECDHE (P-256) + AES-256-GCM record encryption. RFC 8446; FIPS 197
Server Identity	Not verified. Customers cannot tell LocalMart from an imposter.	X.509 cert signed by trusted CA; trust chain validated by browser. RFC 5280
Customer Login	Passwords transmitted in plaintext; replayable; no brute-force protection.	bcrypt (cost 12) + HMAC-SHA-256 JWT (15–30 min). Provos & Mazières, 1999; RFC 7519
Order Integrity	Modifiable in transit and at rest; no detection; no audit trail.	AES-256-GCM auth tag in transit; HMAC-SHA-256 audit tag at rest. NIST SP 800-38D; FIPS 198-1
Card Data	PANs stored on the local server (in PCI scope; breach risk).	Tokenised via PCI-DSS Level 1 gateway; PANs never touch server. PCI SSC, 2024
Compliance	Fails PCI-DSS and GDPR baseline obligations.	PCI-DSS Req 4.2.1 & Req 8 met; GDPR Art. 25 & Art. 32 met. PCI SSC, 2024; EU, 2016

System Architecture Overview



Transaction Flow

1. Browse	2. Order	3. Pay	4. Confirm
TLS 1.3 · public catalogue · no auth	bcrypt login · HMAC-SHA256 JWT · encrypted cart	Browser → Stripe direct · token to server	signed confirmation · HMAC-SHA-256 audit log

Cipher Suite: **TLS_AES_256_GCM_SHA384** · Key Exchange: **ECDHE** · Signatures: **ECDSA** · All transport via TLS 1.3

References

Barker, E., Chen, L., Roginsky, A., Vassilev, A. and Davis, R. (2018) Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography (Revision 3). NIST SP 800-56A Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology.

Biryukov, A., Dinu, D., Khovratovich, D. and Josefsson, S. (2021) Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications. RFC 9106. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc9106 (Accessed: 25 April 2026).

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W. (2008) Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 5280. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc5280 (Accessed: 24 April 2026).

Dworkin, M. (2007) Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST SP 800-38D. Gaithersburg, MD: National Institute of Standards and Technology.

EU Parliament and Council (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union, L 119, pp. 1–88.

Hallam-Baker, P., Stradling, R. and Hoffman-Andrews, J. (2019) DNS Certification Authority Authorization (CAA) Resource Record. RFC 8659. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc8659 (Accessed: 24 April 2026).

Hoogstraaten, H., Prins, R., Niggebrugge, D., Heppener, D., Groenewegen, F. and Janssen, J. (2012) Black Tulip: Report of the Investigation into the DigiNotar Certificate Authority Breach. Delft: Fox-IT BV. Available at: https://www.researchgate.net/publication/269333601 (Accessed: 24 April 2026).

Jones, M. (2015) JSON Web Algorithms (JWA). RFC 7518. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc7518 (Accessed: 24 April 2026).

Jones, M., Bradley, J. and Sakimura, N. (2015) JSON Web Token (JWT). RFC 7519. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc7519 (Accessed: 24 April 2026).

Krawczyk, H. and Eronen, P. (2010) HMAC-based Extract-and-Expand Key Derivation Function (HKDF). RFC 5869. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc5869 (Accessed: 25 April 2026).

Laurie, B., Langley, A. and Käsper, E. (2013) Certificate Transparency. RFC 6962. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc6962 (Accessed: 24 April 2026).

Lodderstedt, T., Bradley, J., Labunets, A. and Fett, D. (2025) Best Current Practice for OAuth 2.0 Security. RFC 9700. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc9700 (Accessed: 24 April 2026).

NIST (2008) The Keyed-Hash Message Authentication Code (HMAC). FIPS 198-1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://csrc.nist.gov/pubs/fips/198/1/final (Accessed: 25 April 2026).

NIST (2023) Advanced Encryption Standard (AES). FIPS 197 (Update 1). Gaithersburg, MD: National Institute of Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf (Accessed: 24 April 2026).

OWASP (no date) Password Storage Cheat Sheet. OWASP Cheat Sheet Series. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html (Accessed: 24 April 2026).

PCI Security Standards Council (2024) Payment Card Industry Data Security Standard, Version 4.0.1. Available at: https://www.middlebury.edu/sites/default/files/2025-01/PCI-DSS-v4_0_1.pdf (Accessed: 24 April 2026).

Provos, N. and Mazières, D. (1999) 'A Future-Adaptable Password Scheme', Proceedings of the USENIX Annual Technical Conference, FREENIX Track, pp. 81–91.

Rescorla, E. (2018) The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. Internet Engineering Task Force. Available at: https://datatracker.ietf.org/doc/html/rfc8446 (Accessed: 24 April 2026).

Sullivan, N. (2018) 'A detailed look at RFC 8446 (a.k.a. TLS 1.3)', Cloudflare Blog, 10 August. Available at: https://blog.cloudflare.com/rfc-8446-aka-tls-1-3/ (Accessed: 25 April 2026).