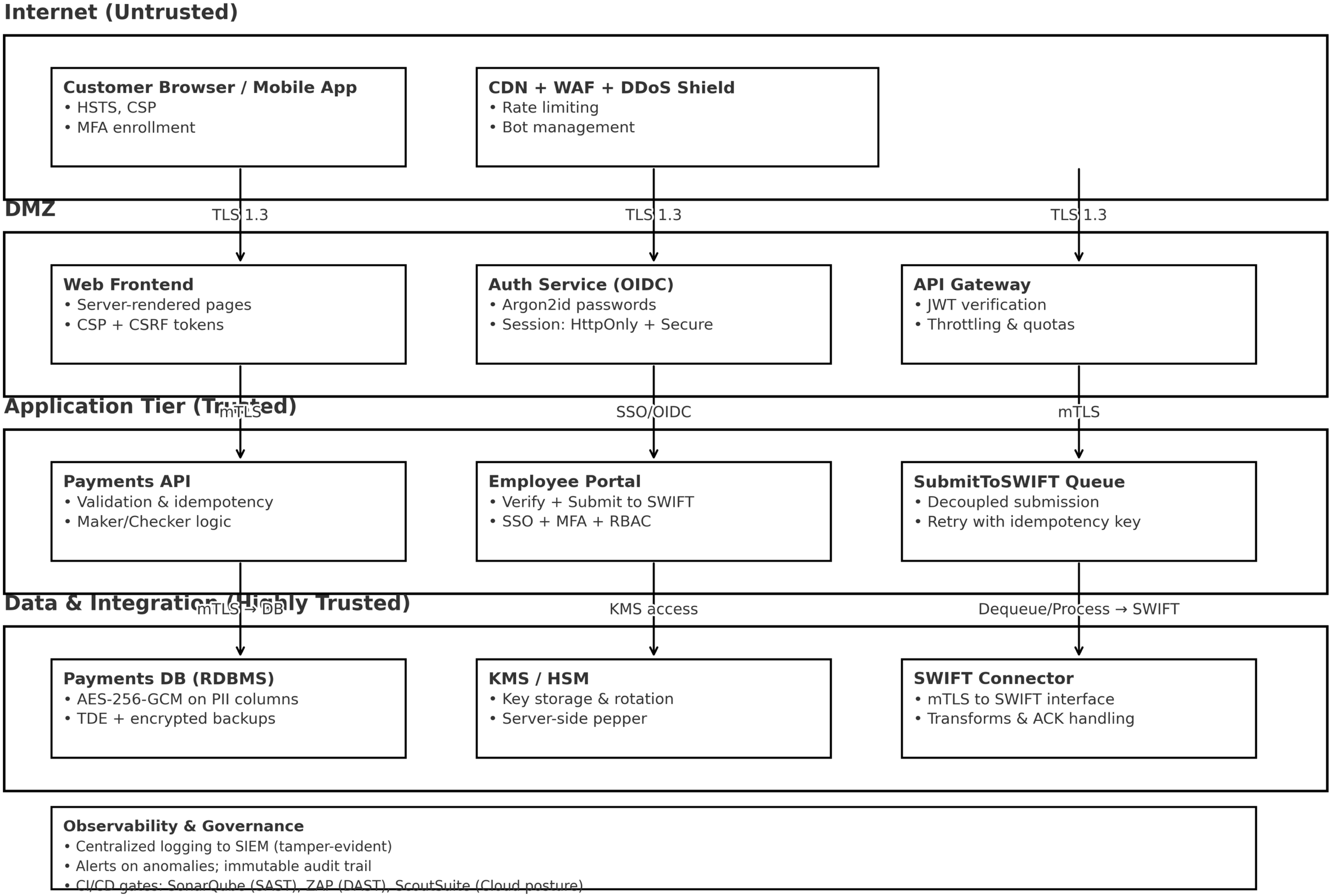
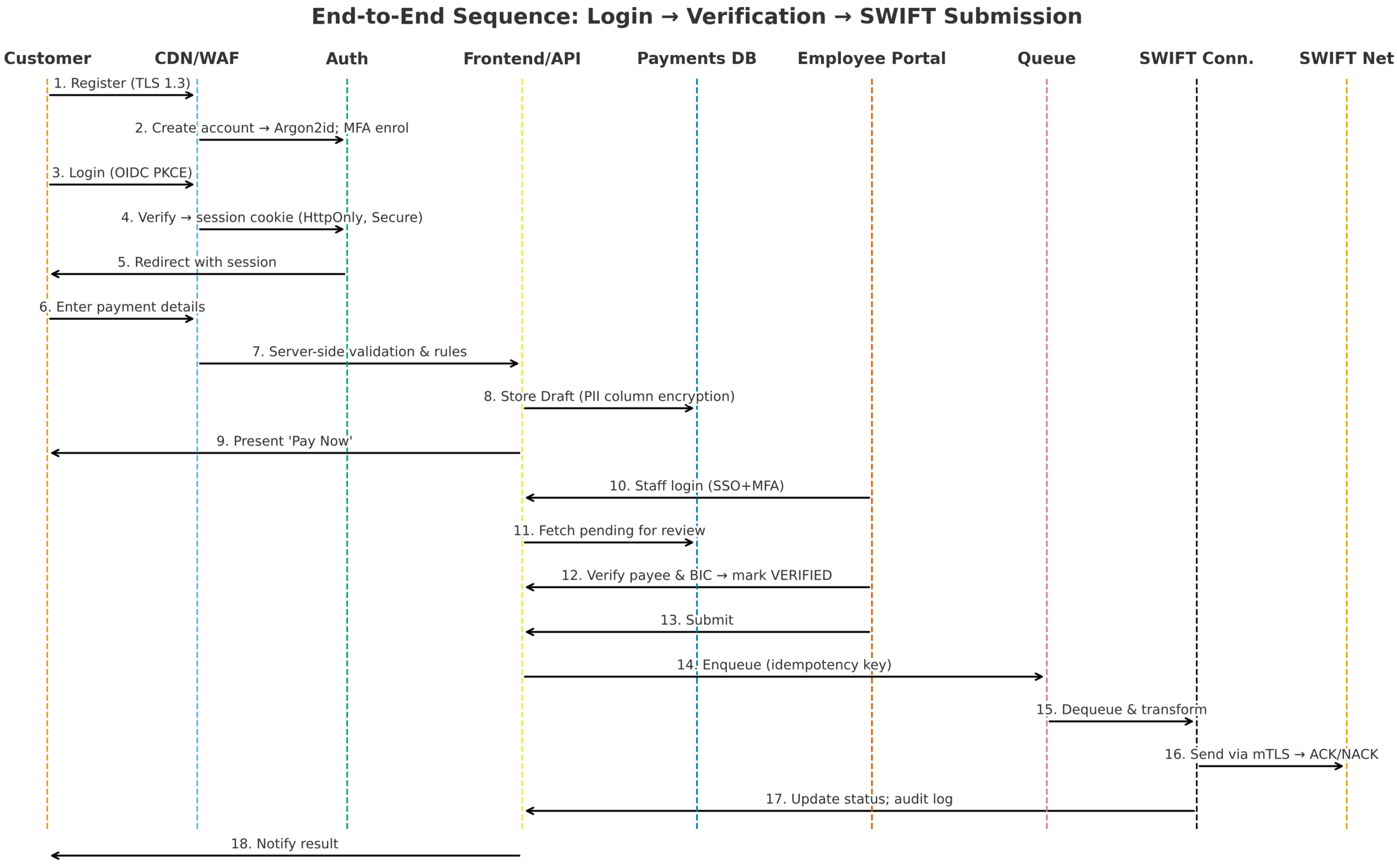
International Payments Portal — Security Architecture (Stacked Zones)

International Payments Portal — Security Architecture (Stacked Zones)



End-to-End Sequence — Login to SWIFT Submission



Security Controls vs Threats — Readable Cards

Security Controls vs Threats — Readable Cards

Session Hijacking

Key Controls:

- Short-lived sessions; rotate on auth and privilege change
- Cookies: Secure + HttpOnly + SameSite
- MFA; device/IP binding (careful for NAT)
- Inactivity + absolute timeouts

Test Methods / Evidence:

- Run ZAP session attacks; try cookie theft (no JS access)
- Replay session from second device → should be rejected
- Verify session rotation events in logs

Clickjacking

Key Controls:

- X-Frame-Options: DENY; CSP frame-ancestors 'none'
- Step-up auth for critical actions; explicit confirmations

Test Methods / Evidence:

- Host in malicious iframe on staging → should not render
- Confirm headers present on all routes

SQL Injection

Key Controls:

- ORM/parameterized queries only
- Server-side validation; least-privilege DB users
- WAF SQLi rules; read-only reporting

Test Methods / Evidence:

- Automated SQLmap/ZAP scans
- Unit tests with known payload sets
- Code review to ensure no string concatenation

Cross-Site Scripting (XSS)

Key Controls:

- Contextual output encoding; auto-escaping templates
- Strict CSP with nonces; sanitize rich text
- HttpOnly cookies; SRI for 3rd-party scripts

Test Methods / Evidence:

- ZAP active scans; manual payloads (SVG, onerror, handlers)
- Review CSP violation reports and address any allows

Man-in-the-Middle (MITM)

Key Controls:

- TLS 1.3 + HSTS; mTLS internally; DNSSEC
- Certificate pinning for mobile; no mixed content

Test Methods / Evidence:

- Burp-in-the-middle blocked by mTLS/pinning
- A+ score on SSL Labs; strict HSTS present

DDoS Attacks

Key Controls:

- CDN/WAF rate limits & bot controls; autoscaling
- Connection & slowloris protection; back-pressure
- Queue-based SWIFT submission

Test Methods / Evidence:

- Load tests at ≥2× peak; WAF blocks observed
- Stable p95 latency; queue drains without backlog