**Group name: AppTitude**

**Members (David Dingani-st10358804, Cebo Nyawo-st10293982, Lethabo Penniston-st10302369, Luke James Lutchmaih-st10288560 and Okuhle Nyawo-st10299658)**

**Information System 3D**

**INSY7314**

**POE PART 1**

**A person sitting at a desk with two computer screens

Description automatically generated**

**Task 1:**

**International Payments Portal — Security Architecture & Test Plan:**

**Introduction:**  
This report presents the security architecture and testing approach for an International Payments Portal developed for a commercial bank. The portal enables retail customers to register and initiate international payments from online banking and allows pre-registered bank employees to verify payee details and submit transactions to SWIFT. Because the solution processes highly sensitive data (ID numbers, account numbers, authentication secrets, payment instructions), it must be secure by design and verifiable through rigorous testing. (SWIFT, 2023; ISO/IEC, 2022; OWASP Foundation, 2021; NIST, 2020).

**Problem statement.**  
We must design a web system that protects customer data and payment integrity from the moment a user signs in, through payment creation, employee verification, and final submission to SWIFT, while remaining usable and highly available. The system must resist common web threats (session hijacking, clickjacking, SQLi, XSS, Man-in-the-Middle, and DDoS) and produce a complete, tamper-evident audit trail suitable for banking compliance.

**Security objectives.**  
• Confidentiality of PII and account data (encryption in transit and at rest).  
• Integrity of transactions (idempotency, maker/checker, signed audit events).  
• Availability under normal and peak loads (WAF/CDN protection and autoscaling).  
• Authentication & authorization with MFA, least privilege, and role separation.  
• Non-repudiation & auditability via immutable logs and traceable approvals.  
(IETF, 2018; ISO/IEC, 2022; NIST, 2020; SWIFT, 2023; NIST, 2006).

**Design principles.**

1. **Layered security (defense-in-depth).**  
   Four tiers with clear trust boundaries: **Internet → DMZ → Application tier → Data & Integration**.
2. **Zero-trust segmentation.**  
   Default-deny between services; authenticated, authorized, and encrypted calls only; **mTLS** for all service-to-service traffic.
3. **Edge protection.**  
   **WAF** in front of the web tier; browser-side hardening with **CSP**; anti-forgery protection via **CSRF tokens**.
4. **Identity & sessions.**  
   Centralized auth using **OIDC with PKCE**; MFA enforced; short-lived, HttpOnly/Secure cookies; server-side session controls.
5. **Data protection by design.**  
   Sensitive fields are **minimized, validated, and encrypted per column**; keys held in **KMS/HSM**; encryption in transit and at rest.
6. **Secrets & key management.**  
   Secrets managed centrally (no secrets in code/CI); rotation policies governed by **KMS/HSM**.
7. **Authorization & duty separation.**  
   **RBAC** throughout the stack; critical payment actions use **maker/checker** (four-eyes) control.
8. **Auditability & accountability.**  
   All state-changing events are **logged immutably** for traceability and compliance.

(NIST, 2020; W3C, 2021; IETF, 2018; OpenID Foundation, 2014 (errata set 2021); OWASP Foundation, 2021; SWIFT, 2023; ISO/IEC, 2022).

**Scope & assumptions.**  
The portal is web-based (with optional mobile access), employees are provisioned by HR/IT, and SWIFT submission occurs through a secure connector in a restricted network segment. Regulatory alignment (e.g., POPIA and banking security standards) is assumed; cardholder data is out of scope unless explicitly stated. (SWIFT, 2023; Republic of South Africa, 2013; ISO/IEC, 2022).

**Testing methodology.**  
Security is enforced in code and verified continuously:  
• SAST (SonarQube) and dependency/image scans in CI.  
• DAST (OWASP ZAP) against an authenticated staging environment.  
• Cloud posture assessment (ScoutSuite) for misconfigurations.  
• Mobile hardening checks (MobSF) if a mobile client is used.  
• Evidence is captured via quality gates, scan reports, and load-test results.  
(SonarSource, 2025; OWASP Foundation, 2025; NCC Group, 2024; Mobile Security Framework (MobSF), 2025; Aqua Security, 2025; ISO/IEC, 2022; NIST, 2020).

The following pages provide: (1) a layered Security Architecture diagram, (2) an end-to-end Sequence Diagram (login → verification → SWIFT submission), and (3) a one-page Controls vs. Threats matrix that maps each risk to the concrete controls and test evidence used to validate them. (OWASP Foundation, 2021; NIST, 2020; SWIFT, 2023).

**A diagram of a security architecture

Description automatically generated**

**A white paper with black text

Description automatically generated**

**A close-up of a document

Description automatically generated**

### **References**

Aqua Security, 2025. Trivy — Scanner for Vulnerabilities, Misconfigurations, and SBOMs. [online] Available at: <https://trivy.dev> [Accessed 14 September 2025].  
Bridgecrew by Prisma Cloud, 2025. Checkov — Infrastructure as Code (IaC) Static Analysis. [online] Available at: <https://www.checkov.io> [Accessed 14 September 2025].  
Internet Engineering Task Force (IETF), 2012. HTTP Strict Transport Security (HSTS) (RFC 6797). RFC Editor: IETF.  
Internet Engineering Task Force (IETF), 2015. HTTP Header Field X-Frame-Options (RFC 7034). RFC Editor: IETF.  
Internet Engineering Task Force (IETF), 2015. JSON Web Token (JWT) (RFC 7519). RFC Editor: IETF.  
Internet Engineering Task Force (IETF), 2015. Proof Key for Code Exchange by OAuth Public Clients (PKCE) (RFC 7636). RFC Editor: IETF.  
Internet Engineering Task Force (IETF), 2018. The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). RFC Editor: IETF.  
Internet Engineering Task Force (IETF), 2021. The Argon2 Memory-Hard Function for Password Hashing (RFC 9106). RFC Editor: IETF.  
ISO/IEC, 2022. ISO/IEC 27001:2022 Information Security Management Systems — Requirements. Geneva: ISO.  
ISO/IEC, 2022. ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Controls. Geneva: ISO.  
Mobile Security Framework (MobSF), 2025. MobSF Documentation. [online] Available at: <https://mobsf.github.io/docs/> [Accessed 14 September 2025].  
Mozilla Developer Network (MDN), 2025. Referrer-Policy — HTTP. [online] Available at: <https://developer.mozilla.org/docs/Web/HTTP/Headers/Referrer-Policy> [Accessed 14 September 2025].  
NCC Group, 2024. ScoutSuite — Cloud Security Auditing Tool. [online] Available at: <https://github.com/nccgroup/ScoutSuite> [Accessed 14 September 2025].  
National Institute of Standards and Technology (NIST), 2006. Guide to Computer Security Log Management (SP 800-92). Gaithersburg, MD: NIST.  
National Institute of Standards and Technology (NIST), 2017 (updated 2023). Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B). Gaithersburg, MD: NIST.  
National Institute of Standards and Technology (NIST), 2020. Recommendation for Key Management — Part 1: General (SP 800-57 Part 1 Rev.5). Gaithersburg, MD: NIST.  
National Institute of Standards and Technology (NIST), 2020. Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev.5). Gaithersburg, MD: NIST.  
National Institute of Standards and Technology (NIST), 2020. Zero Trust Architecture (SP 800-207). Gaithersburg, MD: NIST.  
OpenID Foundation, 2014 (errata set 2021). OpenID Connect Core 1.0. San Ramon, CA: OpenID Foundation.  
OWASP Foundation, 2021. OWASP Application Security Verification Standard (ASVS) v4.0.3. London: OWASP.  
OWASP Foundation, 2021. OWASP Top 10: The Ten Most Critical Web Application Security Risks. London: OWASP.  
OWASP Foundation, 2024. OWASP Secure Headers Project. [online] Available at: <https://owasp.org/www-project-secure-headers/> [Accessed 14 September 2025].  
OWASP Foundation, 2025. OWASP Zed Attack Proxy (ZAP) Project. [online] Available at: <https://www.zaproxy.org> [Accessed 14 September 2025].  
Republic of South Africa, 2013. Protection of Personal Information Act 4 of 2013 (POPIA). Pretoria: Government Gazette.  
SonarSource, 2025. SonarQube Documentation. [online] Available at: <https://docs.sonarsource.com/sonarqube> [Accessed 14 September 2025].  
SWIFT, 2023. Customer Security Controls Framework (CSCF). Brussels: SWIFT.  
SWIFT, 2025. BIC Directory. [online] Available at: <https://www.swift.com/standards/data-standards/bic> [Accessed 14 September 2025].  
World Wide Web Consortium (W3C), 2016. Subresource Integrity (SRI) Recommendation. Geneva: W3C.  
World Wide Web Consortium (W3C), 2021. Content Security Policy Level 3. Geneva: W3C.

Annexure: Disclosure of AI Usage in my Assessment

1. Section(s) within the assessment in which generative AI was used

• Section(s) within the assessment in which generative AI was used, Poe Part 1 Application Development Security.

2. Name of AI tool(s) used

• QuillBot Paraphrasing Tool

3. Purpose/intention behind use

• Paraphrasing, correcting grammar and spelling.

4. Date(s) in which generative AI was used

• From 1 September 2025 – 12 September 2025.

5. Link QuilBot paraphrasing tool

• <https://quillbot.com/paraphrasing-tool>