SIT314/SIT729 – Week 11 Group Activity  
Security, interoperability and legal issues with IoT Applications

short line

# Overview

# This activity is to think about security, interoperability and legal issues for a case study.

# Tasks

Consider a new Australian Banking service which allows the use of retina eye-identification to withdraw money from any ATM at any bank. Answer the following:

1. What potential security issues does that application have?

**Biometric template compromise (irrevocable):** If a retina template is stolen, users can’t “reset” their retina like a password. Use encrypted storage (HSM), template-protection (cancelable biometrics), tight access control, and minimal retention.

**Presentation attacks (spoofing & liveness):** High-res images/printed contacts/replayed video could fool sensors. Deploy robust PAD/liveness (pupil response, micro-saccades, active challenge-response) and secure sensor attestation.

**Sensor tampering & overlays:** Malicious camera overlays at ATMs could capture eye images or inject frames. Use tamper-evident hardware, secure boot, remote attestation and inspections.

**Transmission & replay/MITM:** Features sent to matchers could be intercepted or replayed. Protect with TLS 1.3 + mTLS, nonces/timestamps, signed payloads, and network segmentation.

**Central matcher DoS / availability:** Attacks on a central matcher could block withdrawals network-wide. Add autoscaling, rate-limits, edge/ATM fallback, and BCP/DR.

**Enrollment fraud & coercion:** Fake identities or forced withdrawals. Require in-branch KYC, document/face cross-checks, duress signals (PIN/gesture) and risk-based monitoring.

**Privacy leakage & function creep:** Using retina data beyond withdrawals undermines trust. Enforce purpose limitation, data minimisation, and explicit consent.

**Bias & performance variance:** Error rates vary with lighting, eye conditions, and demographics. Use capture-quality thresholds, assisted UX, and periodic re-evaluation on real cohorts.

1. What potential interoperability issues does the application have?

**Template/algorithm portability:** Vendor-specific retina/iris templates may not interoperate. Prefer open standards (e.g., ISO/IEC 19794-6 for iris image data), plus conformance testing and certification profiles.

**Cross-bank identity federation:** “Any-bank ATM” needs a trust framework, routing and clear SLAs/liability. Consider federation (e.g., OIDC/FIDO-style), shared PKI, audit, and dispute processes.

**Hardware & calibration differences:** Different ATM cameras/IR illuminators lead to variable capture quality. Standardise calibration and require device quality signals in the protocol.

**Legacy ATM support:** Older machines may lack cameras/compute or secure OS baselines. Use upgrade kits/external capture modules or phase deployment.

**Online vs edge matching & latency:** Cloud matching adds latency and needs resilient networking. Use edge inference, encrypted local template caches, and bandwidth-aware fallbacks.

**Fallback & accessibility:** Provide equitable alternatives (card+PIN or app) when biometrics fail or users can’t enrol (eye conditions).

1. What legal, regularity and rights issues does the application have?

* **Privacy Act 1988 & APPs (sensitive information):** Biometric data is sensitive—needs express consent, notice, purpose limitation, minimisation, PIA, strict retention/deletion policies.
* **Notifiable Data Breaches (NDB) scheme:** If templates/identifiers are breached, assess and notify OAIC and affected individuals.
* **APRA prudential standards (e.g., CPS 234; outsourcing CPS 231):** Strong information-security controls, third-party risk management and incident response for banks.
* **AML/CTF obligations:** Align biometric KYC with AUSTRAC requirements (risk-based controls, record-keeping).
* **ePayments Code & liability clarity:** Define liability/apportionment for unauthorised withdrawals via biometrics and ensure transparent dispute resolution.
* **Cross-border data transfer (APP 8):** If any biometric processing/storage is offshore, implement comparable protections and contractual safeguards.
* **Disability Discrimination Act 1992 & accessibility:** Provide reasonable alternatives for users unable to use retina scanning.
* **Children/minors & vulnerable users:** Extra consent/guardrails; opt-out paths where appropriate.
* **Law-enforcement access & warrants:** Clear policy for lawful access, audit trails, proportional retention.