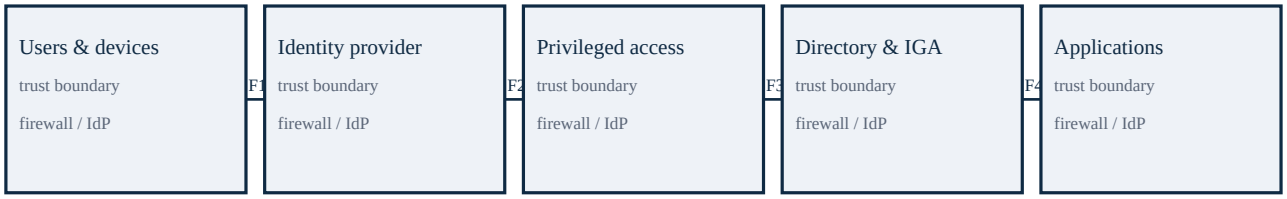
Southern Mutual Bank

Identity & Access Architecture Diagram — Payments Switch

Architecture diagram · data flow diagram · synthetic assessor-grade test document

Diagram ID	SOU-DGM-0212
System	Payments Switch
Owner	James O'Connor (Head of Operational Risk)
Version	3.2
Last reviewed	25 Sep 2026
Status	Current — reflects production topology

1. Diagram



Arrows are data flows (see section 3); every boundary crossing is a firewall or identity control point.

2. Zones and trust boundaries

Zone	Contents and boundary control
Users & devices	Managed devices, conditional access, MFA
Identity provider	Entra ID / SSO, authentication, MFA policies
Privileged access	PAM vault, just-in-time elevation, session recording
Directory & IGA	Active Directory, role-based access, recertification
Applications	Payments Switch and federated SaaS

3. Data flows

Flow	Source -> destination	Data	Protocol / encryption	Controls at the boundary
F1	User -> Identity provider	Authentication (SAML/OIDC), MFA challenge	TLS 1.2+	Conditional access, phishing-resistant MFA for admins
F2	Identity provider -> Application	SSO assertion, role claims	TLS 1.2+ signed assertion	Least privilege via role-based access profiles
F3	Administrator -> PAM	Privileged access request, credential check-out	TLS 1.2+ mTLS	Just-in-time elevation, session recording, approval
F4	PAM -> Target system	Brokered privileged session	SSH / RDP over TLS	Vaulted credentials rotated after use

Flow	Source -> destination	Data	Protocol / encryption	Controls at the boundary
F5	HR system -> IGA	Joiner / mover / leaver events	TLS 1.2+ API	Automated provisioning and de-provisioning of user accounts
F6	IGA -> Directory	Entitlement provisioning, access rights	LDAPS	Quarterly access review and recertification
F7	Identity provider -> SIEM	Sign-in and audit logs	TLS 1.2+	Logging of authentication events, alerting on anomalies

4. Security controls shown

Control area	Implementation
Authentication	Multi-factor authentication enforced for all users; phishing-resistant for privileged users
Privileged access	All privileged accounts brokered through PAM; no standing administrator access
Account management	User accounts uniquely attributable; service accounts vaulted and non-interactive
Access rights	Role-based access, least privilege, recertified quarterly (privileged) and semi-annually
Federation	SSO for all SaaS; local accounts prohibited except approved break-glass

5. Control framework mapping

Framework	Indicative mapped controls
ASD ISM	Guidelines: Access, System hardening, Monitoring
Essential Eight	ML2 target
ISO/IEC 27001:2022	A.5.15, A.5.18, A.8.2, A.8.16, A.5.23
SOC 2 (TSC)	CC6.1, CC6.2, CC6.3, CC7.2
APRA CPS 234	Information security capability, Control testing, Incident notification

Maintained under change control; reviewed after every material network or identity change and at least annually. Source: enterprise architecture repository (system context and network topology views).