Q25: Two-Factor Authentication (2FA) Documentation

Our organization enforces strong Two-Factor Authentication (2FA) on all client-facing mobile and web applications. Implementation details: - We enforce 2FA using multiple secure methods, including Security Keys, Biometrics, Push Notifications, Time-based One-Time Passwords (TOTP, e.g., Google Authenticator), and SMS/Email-based One-Time Passcodes (OTP). - Users are required to enable 2FA during account registration and cannot access critical services without it. - Knowledge-based MFA (e.g., MFA security questions) is also available as a fallback mechanism where necessary. - Our policy mandates periodic reviews and enforcement to ensure compliance with security best practices. This layered approach ensures account protection against unauthorized access, credential theft, and phishing attacks, thereby providing robust authentication for all end users.