EASA Information & Cyber Security - Are You Employing Multi-Factor Authentication (MFA)

Sofema Online (SOL) considers alternative solutions for MFA as part of the EASA Compliant ISMS

Introduction

The requirement for Multi-Factor Authentication (MFA) in your EASA-compliant organisation stems from the need to establish robust access controls as part of your Information Security Management System (ISMS), mandated by EASA Part-IS (Regulations (EU) 2023/203 and 2022/1645).

- While EASA Part-IS mandates the need for strong access controls (including MFA) based on your risk assessment, it typically does not prescribe specific technologies.
- Your choice should align with the risk profile of the systems (especially those impacting aviation safety), usability, and the general best practices often aligned with ISO/IEC 27001 standards.

The available options for Multi-Factor Authentication generally fall into the following categories, based on the three factors of authentication: something you know, something you have, and something you are.

1. Knowledge Factor (Something You Know)

This is combined with another factor, as a password alone is a single factor.

- **Password/PIN:** This is the base factor that is combined with one of the options below to achieve MFA.

2. Possession Factor (Something You Have)

This factor is generally considered more secure than the knowledge factor alone and is a core part of most MFA implementations.

Option	Description	Security & Usability Considerations
Software Tokens / Authenticator Apps	A mobile application (e.g., Microsoft Authenticator, Google Authenticator, Duo) generates a **Time-based One-**	**High Security:** Codes are offline-generated. **Good Usability:** Easy for users who carry a smartphone. **Vendor**

Option	Description	Security & Usability Considerations
	Time Password (TOTP) code every 30-60 seconds.	**Independence:** Often works with any system supporting TOTP.
Push Notifications	The user receives a notification on a registered device (usually a smartphone) and approves the login attempt with a single tap.	**Very High Usability:** Extremely simple and fast. **Medium Security:** Still vulnerable to *MFA fatigue/spamming* attacks unless combined with a number-matching prompt.
SMS One-Time Passcodes (OTP)	A code is sent to a registered mobile number via SMS.	**Medium Usability:** Requires mobile network signal. **Lower Security:** Vulnerable to **SIM-swapping** and interception, often discouraged for high-risk access.
Hardware Security Keys	A physical device (e.g., YubiKey) that plugs into a USB port or uses NFC. Often leverages **FIDO2/WebAuthn** standards.	**Highest Security: Phishing-resistant**, as the key verifies the site's domain. **Medium Usability:** Requires the user to carry a physical token. **Strong Compliance:** Highly recommended for administrators and users with access to safety-critical systems.
Hardware Tokens (Proprietary)	Small devices that display a rotating OTP code (e.g., RSA SecurID).	**High Security:** Dedicated, air-gapped security device. **Lower Usability:** Costly to procure and manage, and users must carry an extra device.
Digital Certificates (PKI)	Authentication via a smart card or software certificate installed on the device.	**Very High Security:** Strong assurance of identity and device. Often integrated with **Public Key Infrastructure (PKI)** solutions used in aviation. **Medium Usability:** Requires specialized

Option	Description	Security & Usability Considerations
		infrastructure, smart card readers, or secured devices.

3. Inherence Factor (Something You Are)

This relies on unique biological characteristics of the user.

Option	Description	Security & Usability Considerations
Biometric Authentication	Uses physical traits like fingerprint, facial scan, or iris scan.	High Security: Unique to the user. High Usability: Fast and seamless, often built into modern devices (phones, laptops). Implementation Note: Biometrics should ideally only unlock a key stored on the device, rather than being transmitted, to maintain security.

Recommendations for EASA ISMS Compliance

To ensure compliance with EASA Part-IS (which is highly aligned with **ISO 27001** and principles of **Zero Trust**), your risk assessment should guide the selection of MFA methods based on the criticality of the information/system:

1. **Prioritise Phishing-Resistant MFA:** For highly privileged accounts (IT/ISMS Administrators) and accounts accessing **safety-critical systems** (e.g., maintenance data, flight planning, or airworthiness systems), implement **Hardware Security Keys (FIDO2)** or **Digital Certificates (PKI)**. These are the gold standard for high-security environments as they prevent phishing attacks.
2. **Standardise on Authenticator Apps:** For the majority of your user base accessing less critical, but still sensitive, ISMS-scoped systems, **Authenticator Apps (TOTP)** and **Push Notifications** are a balance of security and usability. If using push notifications, ensure they include a **number-matching** feature.
3. **Avoid SMS OTPs** for all but the lowest-risk or temporary access scenarios due to their inherent security vulnerabilities.

By adopting a **risk-based approach**, you can choose the right MFA option for each user group and system, effectively mitigating the risk of unauthorized access which is a core requirement of EASA Part-IS.