# Secure authentication

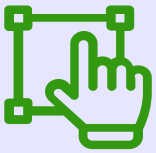
ISO 27002 Control 8.5

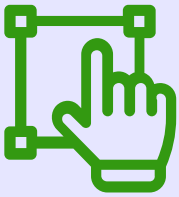
## Control

Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control

## Purpose

To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted





## Why is it important?

- Secure authentication is foundational for controlling access to systems and information
- Multi-factor authentication reduces possibilities for unauthorized access to critical systems
- Log-on procedures must be designed to prevent unauthorized assistance and minimize the risk of password capture

## Examples of sub-controls

- Using multi-factor authentication for accessing critical information systems
- Implementing log-on procedures that do not display sensitive system information until successful log-on
- Protecting against brute force log-on attempts (e.g., CAPTCHA, blocking after failed attempts)
- Terminating inactive sessions after a defined period of inactivity
- Validating log-on information only upon completion of all input data

## Which concepts are related ?

- Multi-factor authentication (MFA)
- Log-on procedures
- Brute force attempts
- Biometric authentication
- CAPTCHA

## Link with other frameworks

- NIST 800-53 rev5 : AC-7, AC-8, AC-9, IA-6
- NIST CSF 2.0 : PR.AA-01, PR.AA-05

Renaud Dardenne
Asphalia Consulting