## 4 FORME DI AUTENTICAZIONE

### 1. “qualcosa che si sa”


È un’informazione che solo la persona che si vuole autenticare conosce: dimostrando di conoscere questa informazione, si dimostra di essere effettivamente chi si dichiara di essere. **Password** e **PIN** sono il caso più noto.

### 2. “qualcosa che si ha”


È un oggetto fisico in possesso di chi si vuole autenticare.
L’ipotesi è che questo oggetto sia unico e non duplicabile, che il proprietario non lo ceda e si accorga se gli viene sottratto.
Una **smart card** è tra gli esempi più noti.

### 3. “qualcosa che si è”

**Biometria statica.**
Si tratta di misurare alcune caratteristiche del nostro corpo (impronte digitali, iride o altro) che presumibilmente sono uniche da individuo a individuo e immutabili nel tempo.

### 4. “qualcosa che si fa”

**Biometria dinamica.**
Esempi includono il riconoscimento in base alla voce, caratteristiche della calligrafia, ritmo di battitura sulla tastiera, osservazione della camminata, etc. .

## PROBLEMI

Ogni forma di autenticazione, se implementata e utilizzata correttamente, permette l’accesso in sicurezza ai sistemi.
Tuttavia, ci sono dei problemi.

### “Qualcosa che si sa / ha“

Si può avere un notevole “sovraccarico amministrativo”, ovvero, la gestione delle informazioni (per quanto riguarda le **password**) e la protezione di tali informazioni sui dispositivi (per quanto riguarda le **smart card**).
Nel caso di password, ad esempio, l’informazione viene fornita direttamente, esponendola all’intercettazione, al **phishing** e ad altri attacchi, con il grosso problema che non è detto che chi subisce il furto se ne possa accorgere.
Nel caso della smart card, questa può essere smarrita, cedendone il possesso ad un potenziale malintenzionato.

### “Qualcosa che si è / fa“

Ci sono una serie di problemi legate alla gestione di falsi positivi e falsi negativi (vedi brochure “*Autenticazione basata su biometria*”), l’accettazione del sistema da parte degli utenti “poco pratici”, i costi e la convenienza.

## RIFERIMENTI


- http://www.c3t.it/projects/awareness/articoli&brochure/autenticazione/



*POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)*



# L’AUTENTICAZIONE

Scopri cosa vuol dire autenticarsi in un contesto digitale.

## PERCHÉ AUTENTICARE ?

L'**autenticazione** è alla base di qualsiasi meccanismo di sicurezza.

*"Prima dimmi chi sei ... "*

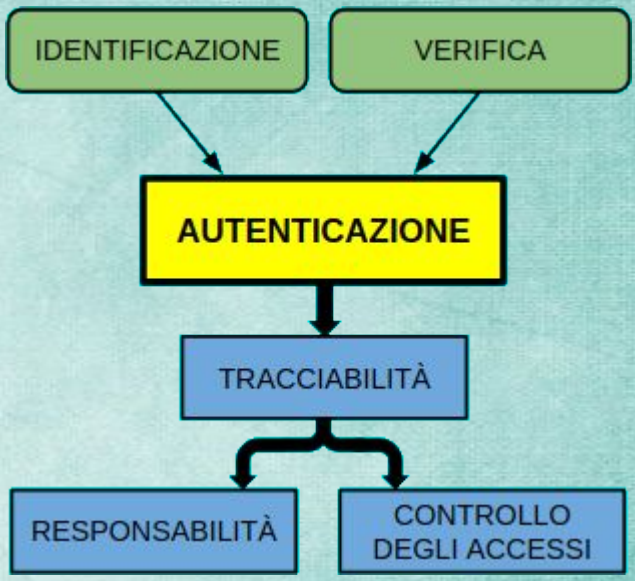
Il concetto è che, generalmente, ogni individuo preferirebbe sapere con chi ha a che fare, prima di avere un qualsiasi tipo di interazione con una controparte.

In particolare, l'autenticazione fornisce le basi per (ma è distinta da):

1. tracciabilità delle azioni;
2. attribuzione di responsabilità;
3. controllo degli accessi.

Si può pensare all'autenticazione come una composizione di due funzioni:

- funzione di **identificazione**: come l'utente viene autenticato all'interno del sistema (es. ID, username, ...);
- funzione di **verifica**: effettivo riconoscimento della persona fisica a quella digitale che sta richiedendo l'accesso.




## MECCANISMO GENERALE

Secondo il modello del **NIST** (National Institute of Standards and Technology), per un utente che vuole prendere parte ad un sistema digitale, si distinguono la fase preliminare di registrazione nel sistema e la consuetudinaria sessione di accesso al sistema (in breve **Enrollment & Verify**).