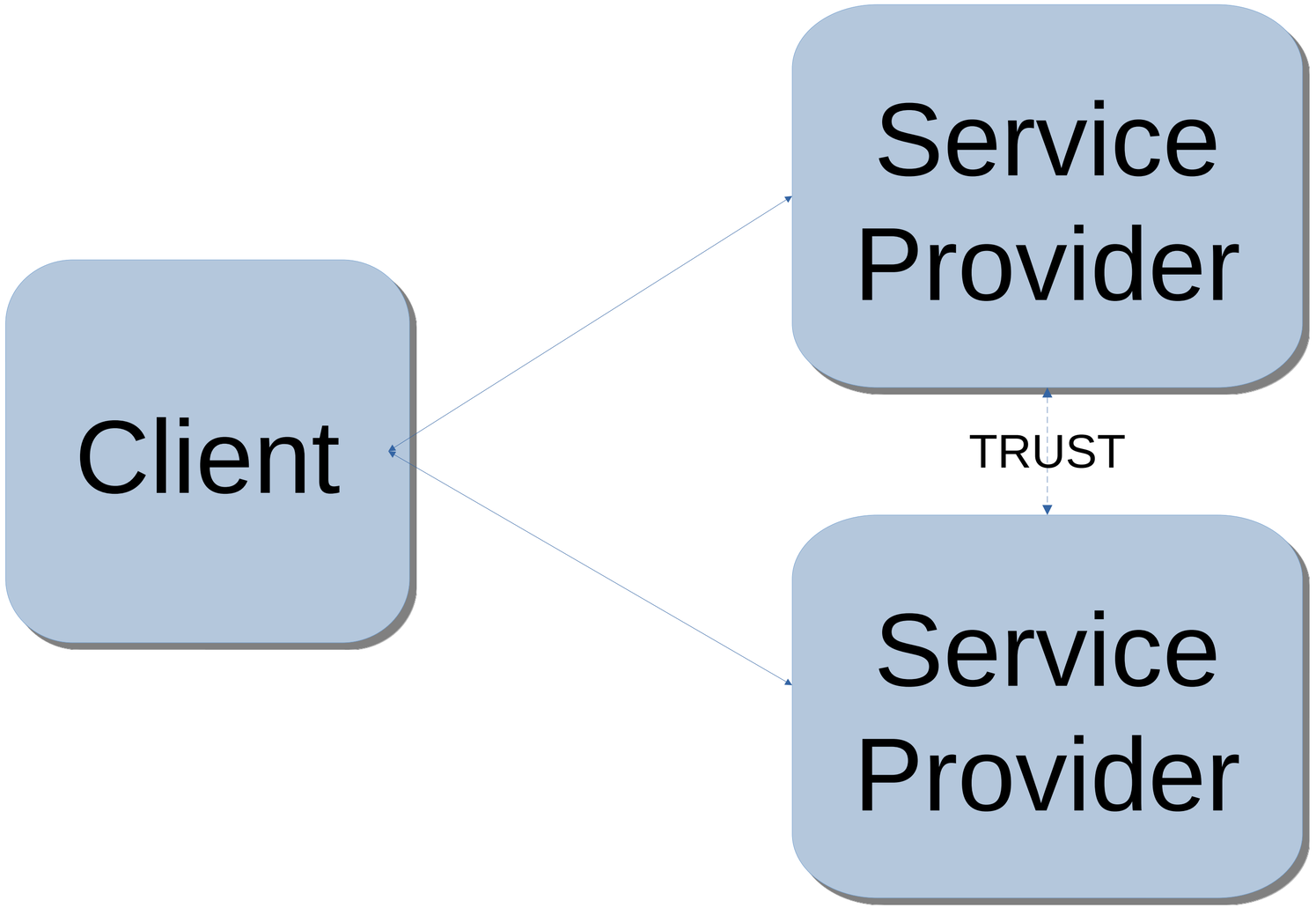
Sviluppo prototipale di una soluzione survivable per autenticatori hardware FIDO

Relatore: Luca Ferretti
Correlatore: Federico Magnanini
Tesista: Giulio Barabino

Ingegneria Informatica - sede di Mantova, Unimore

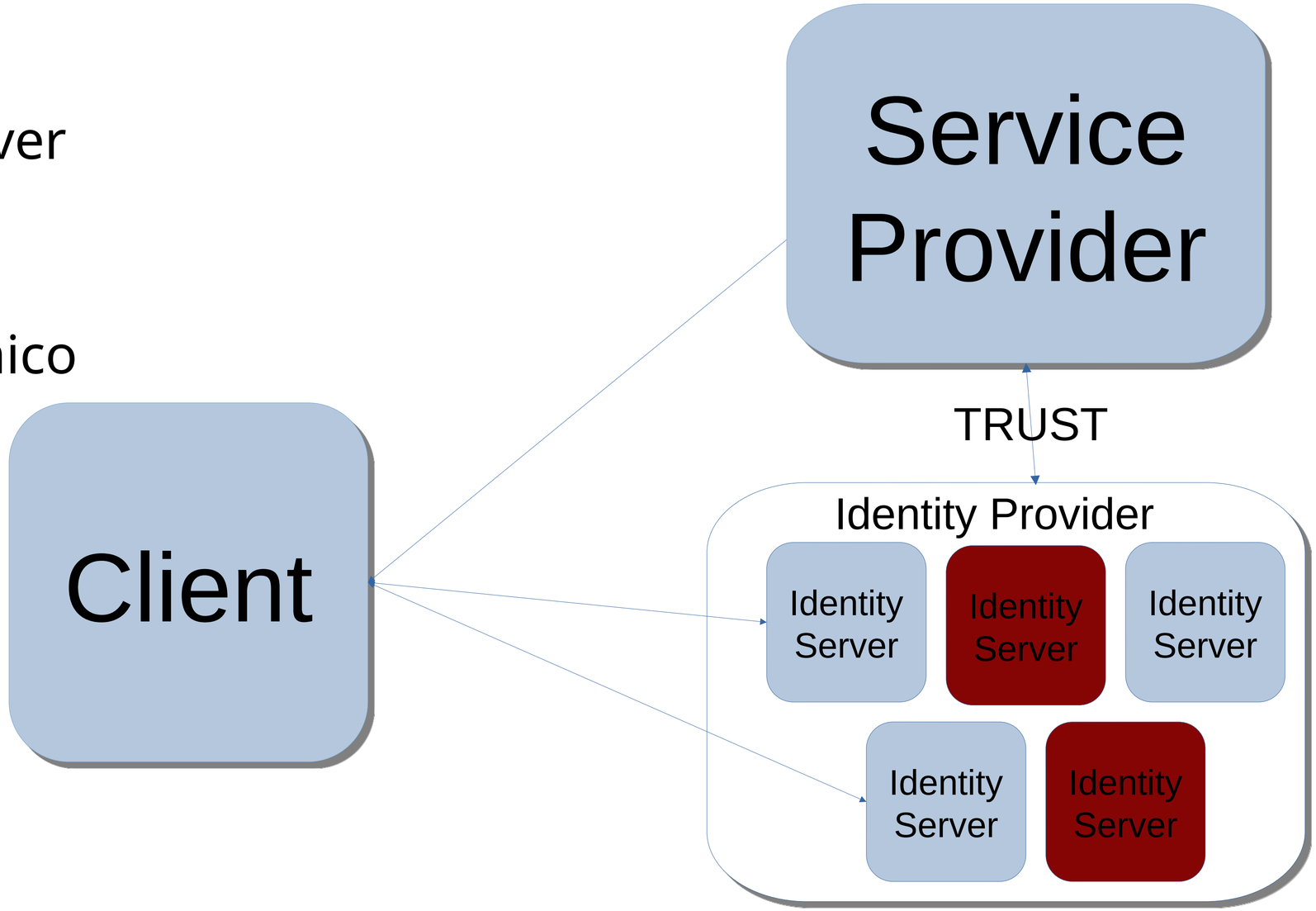
Scenario di riferimento

- Protocollo SSO
- Autenticazione delegata
- Principio di “trust”



Survivability

- Replicazione Identity Server
- Tolleranza alle intrusioni
- Livello di sicurezza dinamico



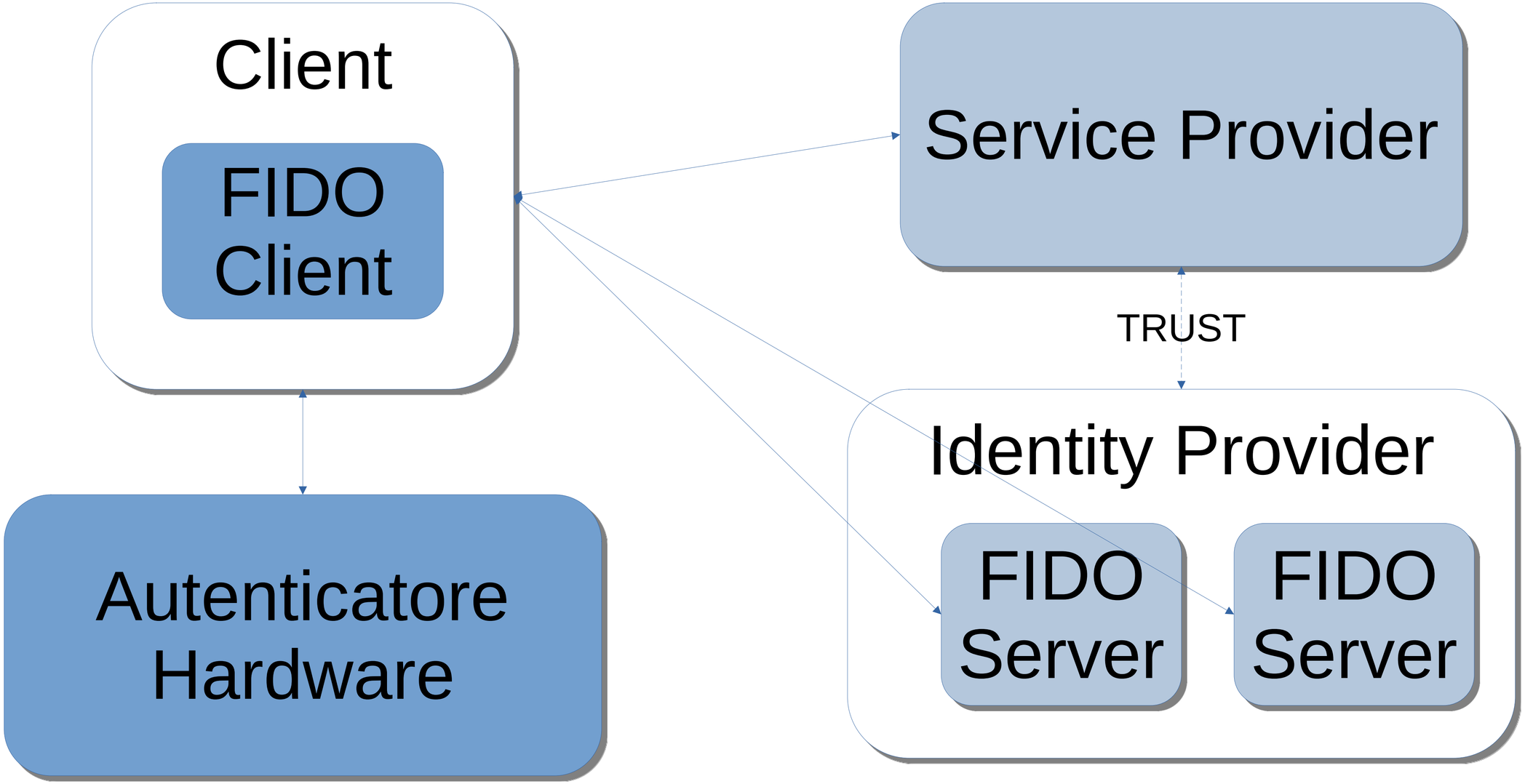
Passwordless

- Autenticazione 'robusta'
- Diversi fattori di autenticazione
- Autenticazione entropicamente forte

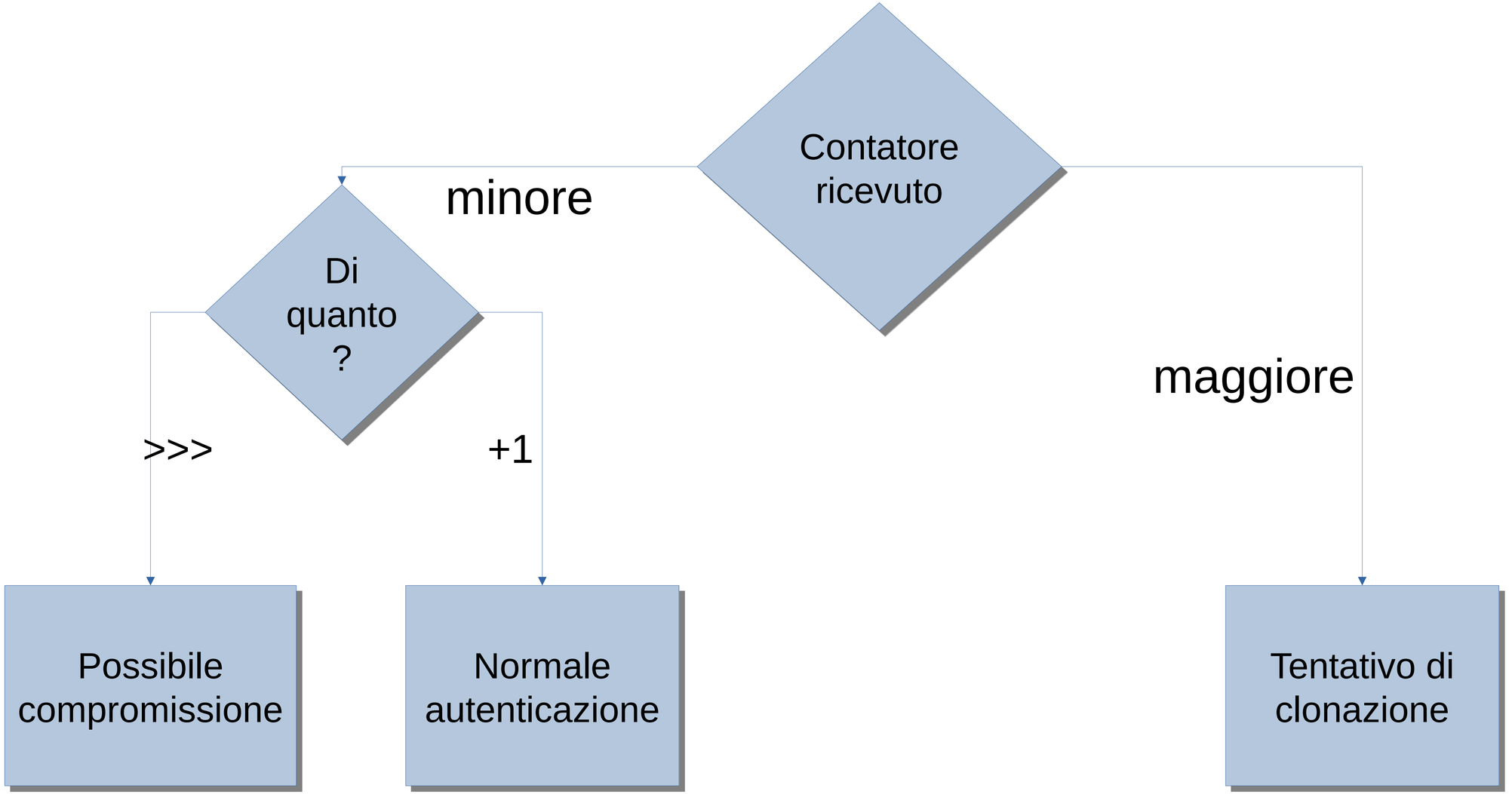
FIDO

- Associazione nata nel 2013
- Due standard: CTAP e WebAuthn
- Obiettivo: autenticazione più sicura

Autenticazione passwordless FIDO



Sistema di rilevamento clonazioni



Testbed Sperimentale

Autenticatore: Solokeys

- Progetto Open Source
- Autenticatore fisico
- Codice in C

Server FIDO: Yubico

- Sviluppatori libreria FIDO
- Lato server
- Codice in Python

Modifiche operate

Autenticatore

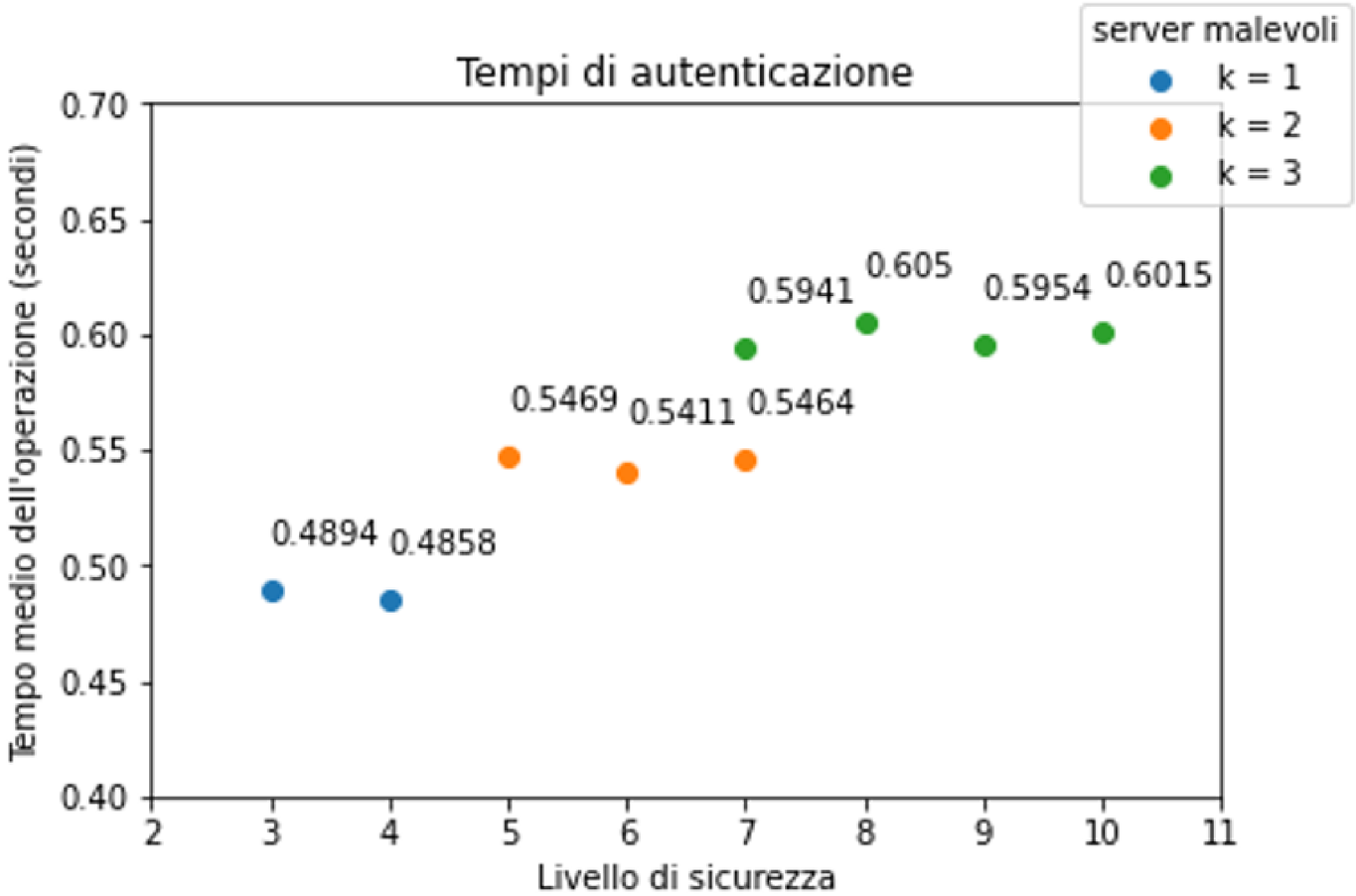
- Introduzione livello di sicurezza nelle strutture dati già presenti
- Incremento contatore in funzione del livello di sicurezza
- Creazione struttura per la memorizzazione di contatori per credenziale

Libreria FIDO

- Invio del livello di sicurezza
- Memorizzazione del contatore ricevuto
- Implementazione logica di controllo sul contatore

Prestazioni

- Prestazioni coerenti con quanto già dimostrato
- Multipli Security Level
- Trade-off prestazioni – sicurezza accettabile



$$|Q| \in [(2k + 1), (3k + 1)]$$

Conclusioni

- Ulteriori analisi con hardware fisico necessarie
- Analisi costi-benefici per implementazione lato produttore
- Prestazioni adatte a scenari reali di autenticazione

Grazie per l’attenzione