Identità digitale

Identificazione remota, autenticazione sicura e gestione degli attributi

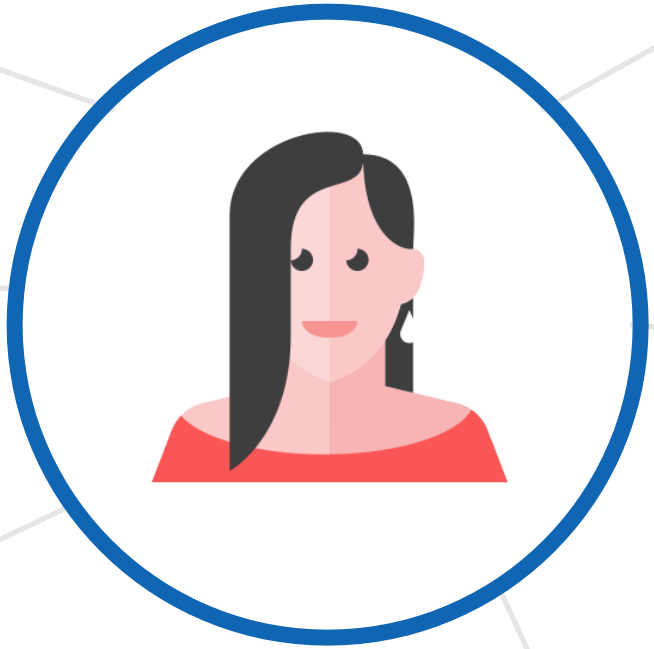
Marco Pernpruner, Giada Sciarretta, Alessandro Tomasi
Security & Trust Research Unit
Fondazione Bruno Kessler, Trento, Italy

PMI Academy, Accademia d'Impresa
5 maggio 2021

Identità digitale
è parte della nostra vita quotidiana...

Dipendente

Account bancario



Account su social network

Cittadino

spid

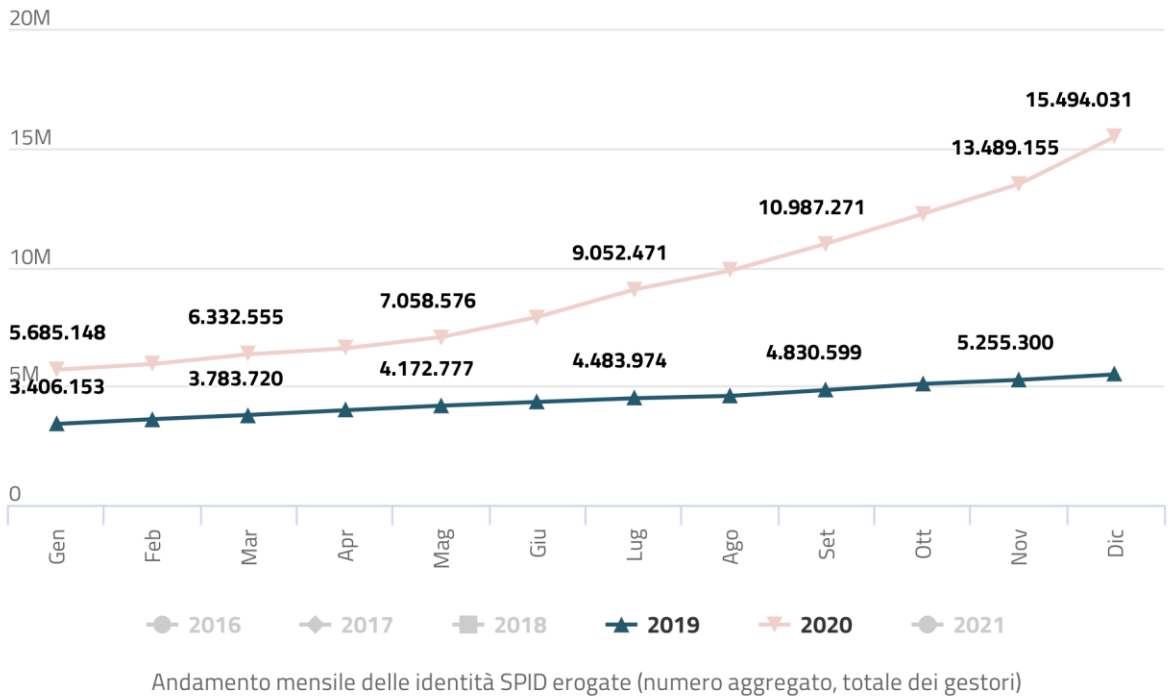
Siti di e-commerce

...

Incremento tecnologico - Italia 2020
...soprattutto ora

spid

20.269.399
05/05/2021



Andamento mensile delle identità SPID erogate (numero aggregato, totale dei gestori)

Digital Report 2021

Piattaforme social

Oltre **2 milioni di nuovi utenti**

Internet

Siamo connessi per **oltre 6 ore al giorno**
Oltre **1 milione di nuovi utenti**

E-commerce

Speso il **24% in più rispetto al 2019**

Identità digitale
Rapporto Clusit 2021

Il **10%** degli attacchi gravi nel 2021 sono direttamente riferibili al tema **Covid-19**

Aumento casi di phishing, siti clonati, malware ...

INTESA SANPAOLO

La password de la sua carta Flash e stata inserita piu
Per proteggere la sua carta abbiamo sospenso il acceso.

Per recuperare il acceso clicca su :

https://www.monetaonline.it/layout/03069/pop/code-ident
31357819513/

li cart

False e-mail dall'Organizzazione Mondiale della Sanità per il Coronavirus, occhio alla truffa

Nel testo della e-mail viene annunciato un documento con tutte le precauzioni per evitare il contagio da Coronavirus e si invita ad aprire il documento allegato

Da Dr. Penelope Marchetti <peder@kennel-lope.dk>
Oggetto **Coronavirus: Informazioni importanti su precauzioni**
A Me

Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus,
della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie con
coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggi

Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

1 allegato: f211298392683.doc 387 k

FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

Security & Trust – Centro FBK CyberSecurity
Identità digitale

! Necessità di **soluzioni sicure** e **tool di analisi** per la protezione dell'identità digitale

Security-by-design

Design di soluzioni di on-boarding, autenticazione e controllo degli accessi

Valutazione automatica di sicurezza e rischio

Di soluzioni di on-boarding e autenticazione

POLIGRAFICO E ZECCA DELLO STATO ITALIANO
security and innovation in our history

Servizi PA

TRENTINOSALUTE 4.0

Servizi sanitari

CherryChain

Servizi FinTech

...

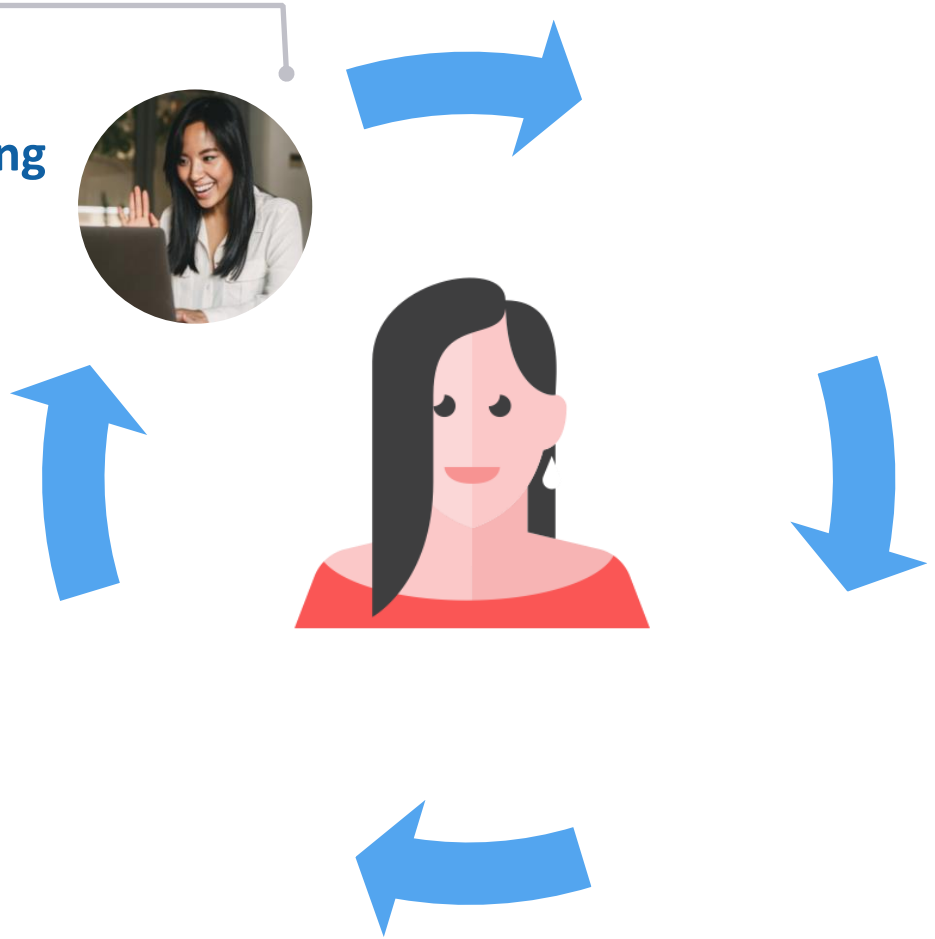
Ciclo di vita dell'identità
...in sicurezza

National Institute of Standards and Technology
U.S. Department of Commerce

Ciclo di vita dell'identità ...in sicurezza

National Institute of Standards and Technology
U.S. Department of Commerce

Inizia il rapporto



Identificazione/on-boarding

Processo tramite il quale un richiedente fa domanda di diventare un utente di un servizio e il servizio valida l'identità del richiedente

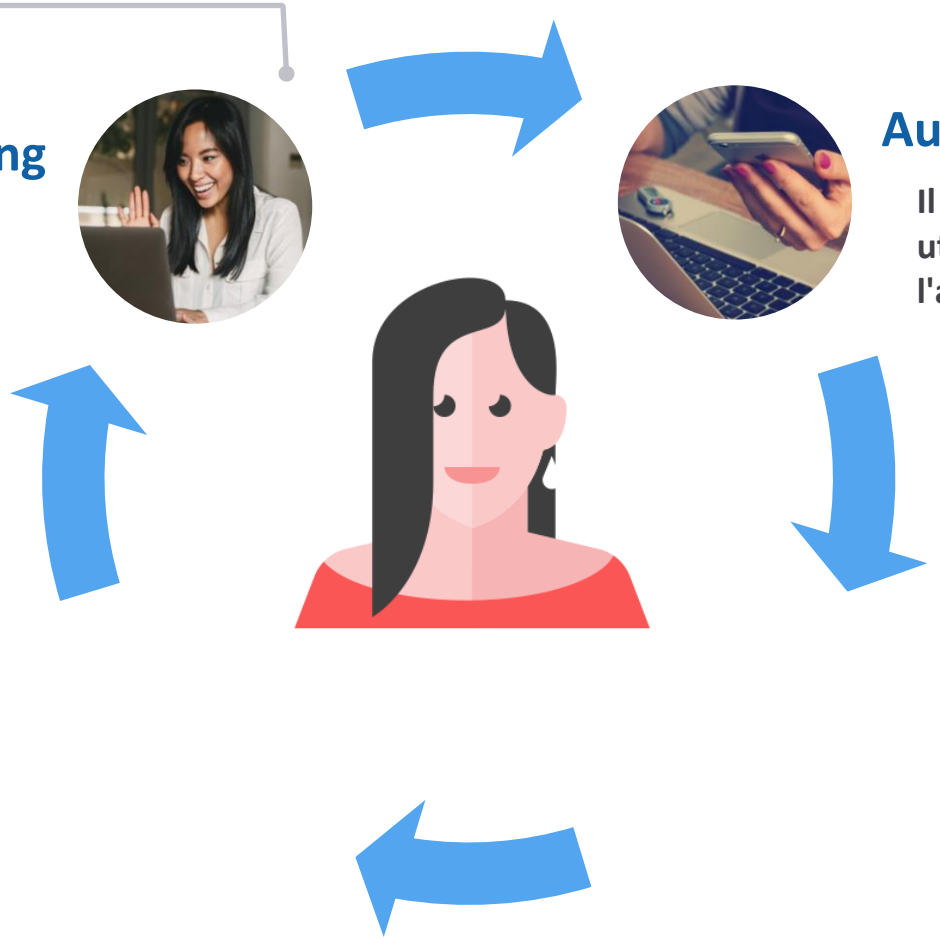
FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

Ciclo di vita dell'identità
...in sicurezza

National Institute of Standards and Technology
U.S. Department of Commerce

L'utente riceve una credenziale

Inizia il rapporto



Identificazione/on-boarding

Processo tramite il quale un richiedente fa domanda di diventare un utente di un servizio e il servizio valida l'identità del richiedente

Autenticazione

Il processo di verifica dell'identità di un utente come prerequisito per consentire l'accesso alle risorse di un sistema

FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

Ciclo di vita dell'identità
...in sicurezza

National Institute of Standards and Technology
U.S. Department of Commerce

L'utente riceve una credenziale

Inizia il rapporto

Identificazione/on-boarding

Processo tramite il quale un richiedente fa domanda di diventare un utente di un servizio e il servizio valida l'identità del richiedente

Autenticazione

Il processo di verifica dell'identità di un utente come prerequisito per consentire l'accesso alle risorse di un sistema

Autorizzazione e **gestione attributi**

Il processo di verifica dei permessi di accesso di un utente, in genere automatizzato valutando gli attributi di un soggetto

FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

Ciclo di vita dell'identità ...in sicurezza

National Institute of Standards and Technology
U.S. Department of Commerce

L'utente riceve una credenziale

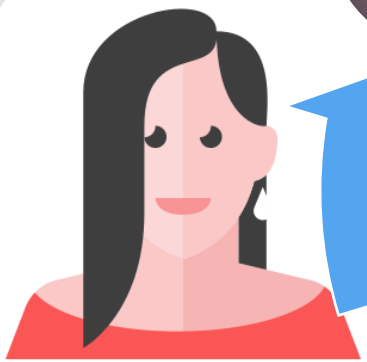
Inizia il rapporto

Identificazione/on-boarding

Processo tramite il quale un richiedente fa domanda di diventare un utente di un servizio e il servizio valida l'identità del richiedente

Autenticazione

Il processo di verifica dell'identità di un utente come prerequisito per consentire l'accesso alle risorse di un sistema



Autorizzazione e **gestione attributi**

Il processo di verifica dei permessi di accesso di un utente, in genere automatizzato valutando gli attributi di un soggetto

Fine rapporto

Annullamento della registrazione

FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

Identificazione

Identificazione (Enrollment/On-boarding)
Identity Assurance Level (IAL)

National Institute of Standards and Technology
U.S. Department of Commerce

Livello che indica il grado di certezza che l'identità rivendicata dal richiedente sia la sua vera identità.

"On the Internet, nobody knows you're a dog."

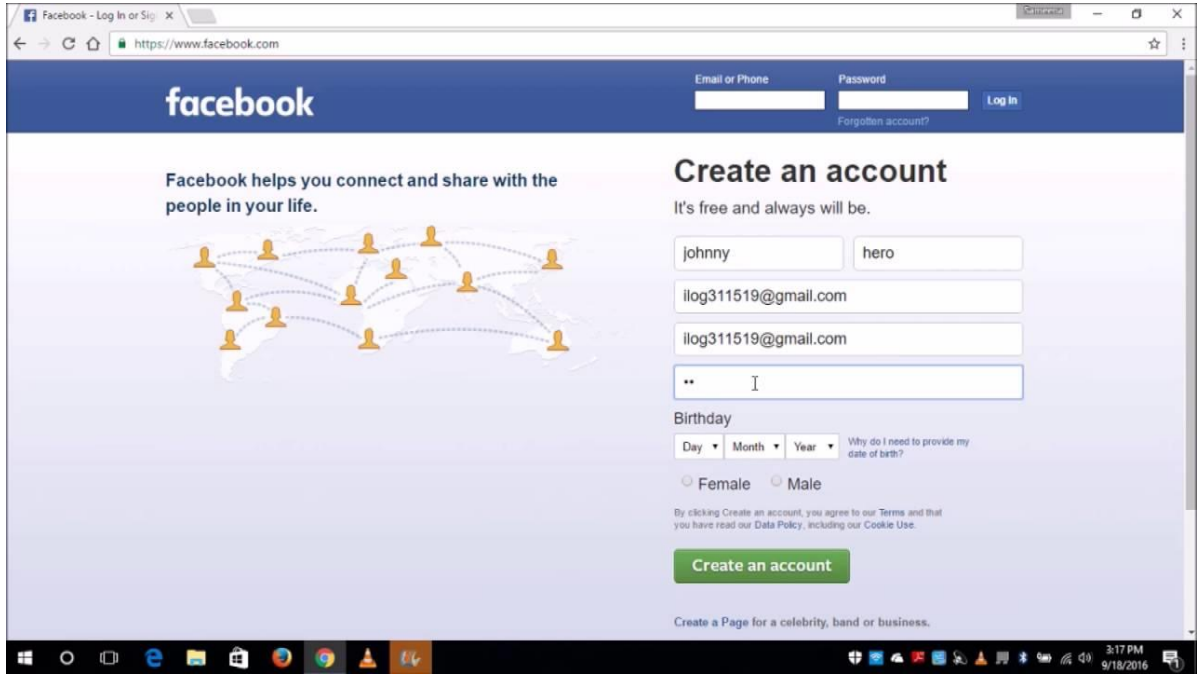
FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

Identificazione (Enrollment/On-boarding)
Identity Assurance Level (IAL)

National Institute of Standards and Technology
U.S. Department of Commerce

Livello che indica il grado di certezza che l'identità rivendicata dal richiedente sia la sua vera identità.

IAL1	Gli attributi sono dichiarati dal richiedente stesso (self-asserted)



FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

Identificazione (Enrollment/On-boarding)
Identity Assurance Level (IAL)

National Institute of Standards and Technology
U.S. Department of Commerce

Livello che indica il grado di certezza che l'identità rivendicata dal richiedente sia la sua vera identità.

IAL1	Gli attributi sono dichiarati dal richiedente stesso (self-asserted)
IAL2	È richiesta un'identificazione remota o di persona

- Identificazione remota tramite webcam
- Identificazione remota tramite documento elettronico
- Identificazione remota tramite firma elettronica

FONDAZIONE BRUNO KESSLER
ST SECURITY & TRUST
PMI ACADEMY

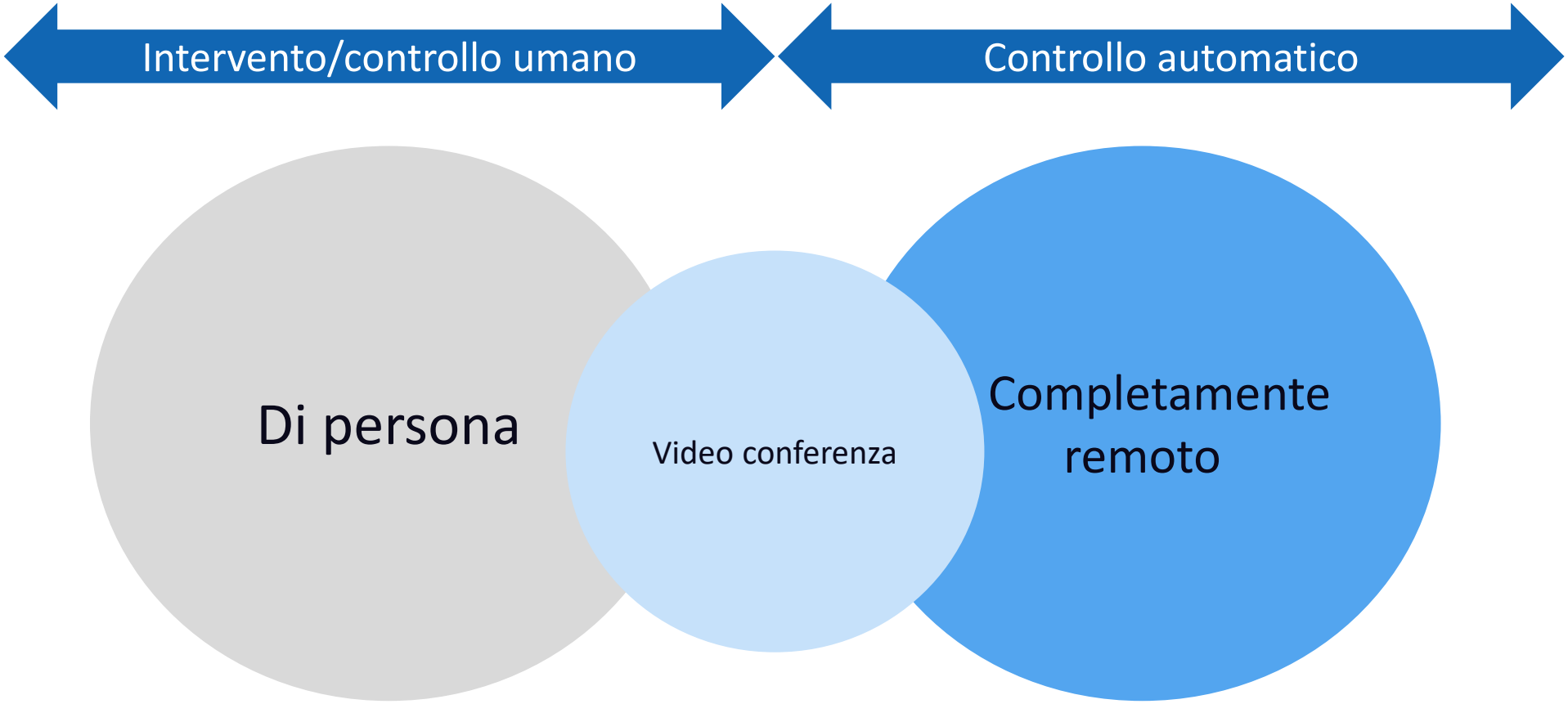
Identificazione (Enrollment/On-boarding)
Identity Assurance Level (IAL)

National Institute of Standards and Technology
U.S. Department of Commerce

Livello che indica il grado di certezza che l'identità rivendicata dal richiedente sia la sua vera identità.

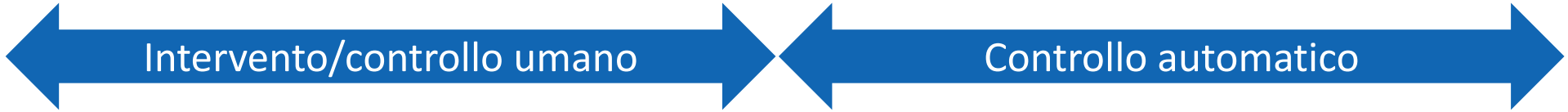
IAL1	Gli attributi sono dichiarati dal richiedente stesso (self-asserted)
IAL2	È richiesta un’identificazione remota o di persona
IAL3	È richiesta un’identificazione di persona. Gli attributi identificativi devono essere verificati da un’entità autorizzata attraverso l’esaminazione del documento fisico.

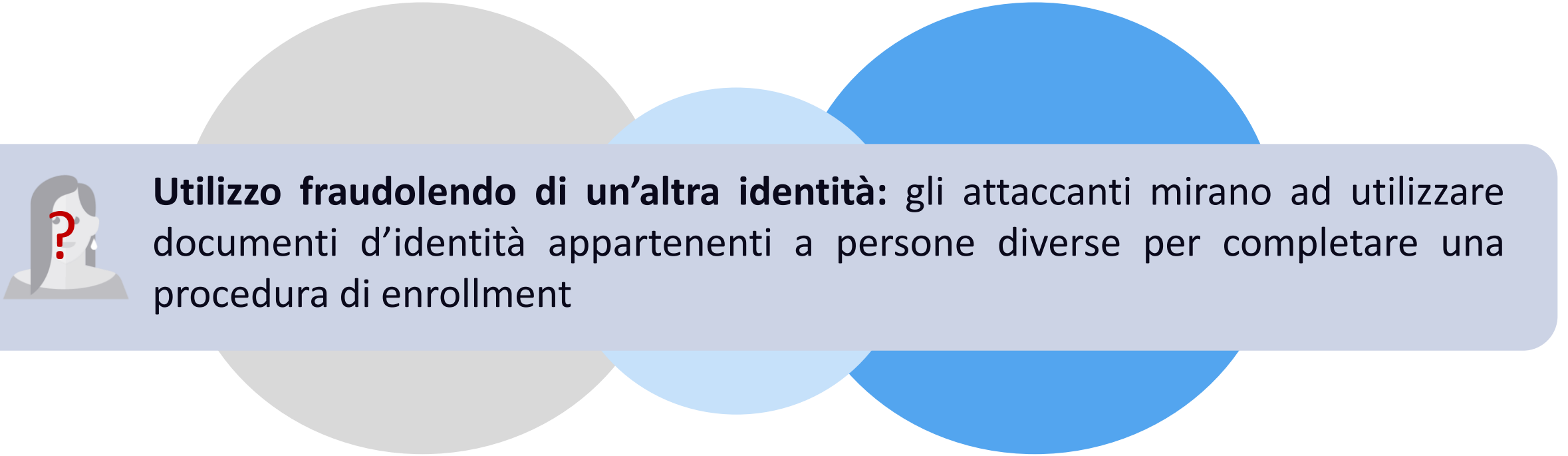
Bilanciare sicurezza e usabilità
Diverse procedure di enrollment



Sicurezza?

Bilanciare sicurezza e usabilità
Diverse procedure di enrollment





Sicurezza?

Nostro contributo
Analisi sicurezza e rischio

Tool automatico per l'analisi di sicurezza e rischio di procedure di enrollment

Proteggere dispositivi e app

Tecniche di anti-spoofing

- Non è possibile caricare foto
- Selfie solo dalla fotocamera anteriore
- Liveness detection
- ….

M. Pernpruner, G. Sciarretta, S. Ranise. "A Framework for Security and Risk Analysis of Enrollment Procedures: Application to Fully-Remote Solutions Based on eDocuments". SECRYPT 2021.

Autenticazione sicura

Ciclo di vita dell'identità
...in sicurezza

National Institute of Standards and Technology
U.S. Department of Commerce

L'utente riceve una credenziale

Inizia il rapporto

Identificazione/on-boarding

Processo tramite il quale un richiedente fa domanda di diventare un utente di un servizio e il servizio valida l'identità del richiedente

Autenticazione

Il processo di verifica dell'identità di un utente come prerequisito per consentire l'accesso alle risorse di un sistema

Autorizzazione e gestione attributi

Il processo di verifica dei permessi di accesso di un utente, in genere automatizzato valutando gli attributi di un soggetto

Fine rapporto

Annullamento della registrazione

FONDAZIONE BRUNO KESSLER

SECURITY & TRUST

PMI ACADEMY

Autenticazione sicura
Fattori di autenticazione

L’autenticazione può fare affidamento su determinati *fattori di autenticazione*:

Images source: https://appspicket.com/the-next-generation-in-2fa-technology/

Sicurezza dei protocolli
Metodologia di analisi

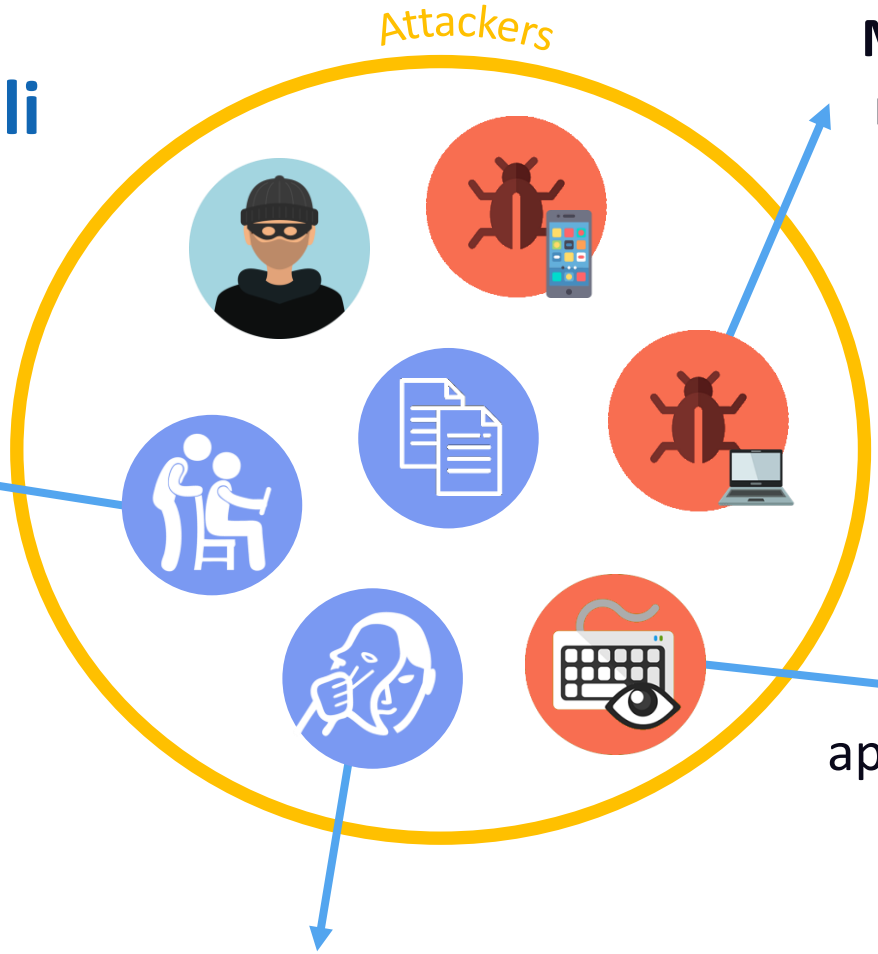
1

Analisi di sicurezza
Permette di rilevare quali attaccanti sono in grado di compromettere il protocollo

2

Analisi del rischio
Permette di valutare i rischi connessi agli attaccanti, prioritizzando le mitigazioni

Sicurezza dei protocolli
Analisi di sicurezza



Man in the Browser: applicazione malevola nel browser dell'utente

Shoulder Surfer: compromette informazioni segrete spiando la vittima

Eavesdropping Software: applicazione malevola che intercetta quando digitato sulla tastiera

Social Engineer: convince la vittima con l'inganno a rivelare segreti o effettuare operazioni

Sicurezza di protocolli
Analisi del rischio

Probabilità

Impatto

Rischio = Probabilità × Impatto

Probabilità che un attacco si verifichi

Conseguenze nel caso in cui l'attacco abbia successo

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

PMI ACADEMY

Sicurezza di protocolli
Analisi del rischio con OWASP Risk Rating Methodology

		Probabilità		
		Bassa	*Media*	*Alta*
Impatto	*Basso*	Trascur.	Basso	Medio
	Medio	Basso	Medio	Alto
	Alto	Medio	Alto	Critico

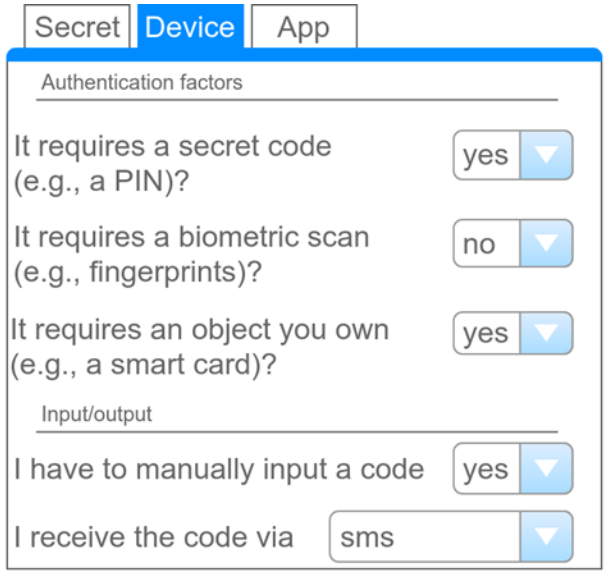
Rischio = Probabilità × Impatto

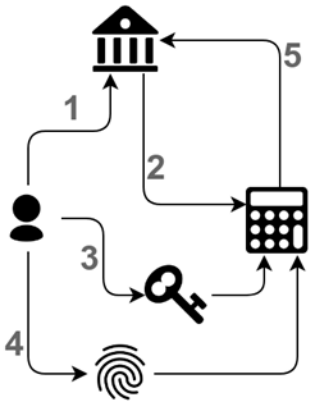
Probabilità che un attacco si verifichi

Conseguenze nel caso in cui l'attacco abbia successo

Sicurezza di protocolli
MuFASA

MuFASA





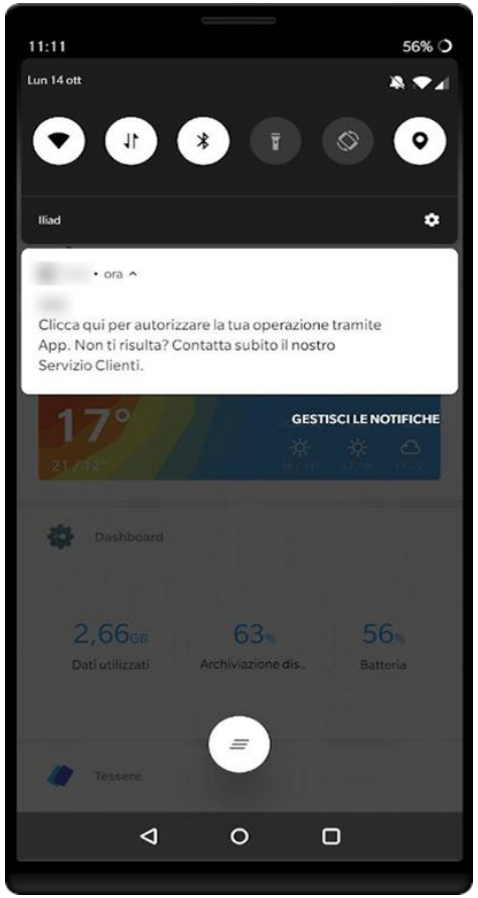
Utilizzo	Traduzione	Modellazione	Analisi	Resoconto
L'utente utilizza il protocollo e acquisisce esperienza	L'utente descrive il protocollo da analizzare rispondendo alle domande di un questionario	Il protocollo descritto viene modellato in un linguaggio di specifica interno	Il protocollo descritto viene analizzato per valutarne la resistenza	I risultati dell'analisi vengono mostrati all'interno di un resoconto in PDF

Sicurezza di protocolli
MuFASA – Utilizzo

MuFASA

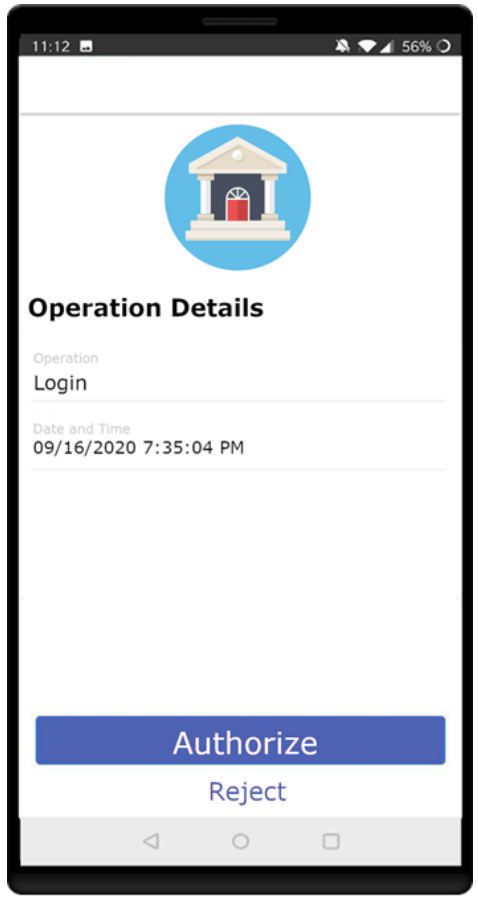
Sicurezza di protocolli
MuFASA – Utilizzo

MuFASA



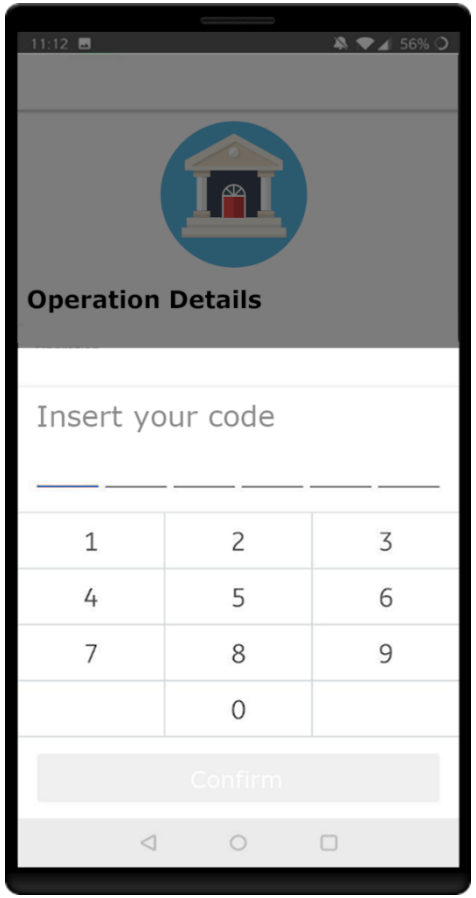
Sicurezza di protocolli
MuFASA – Utilizzo

MuFASA



Sicurezza di protocolli
MuFASA – Utilizzo

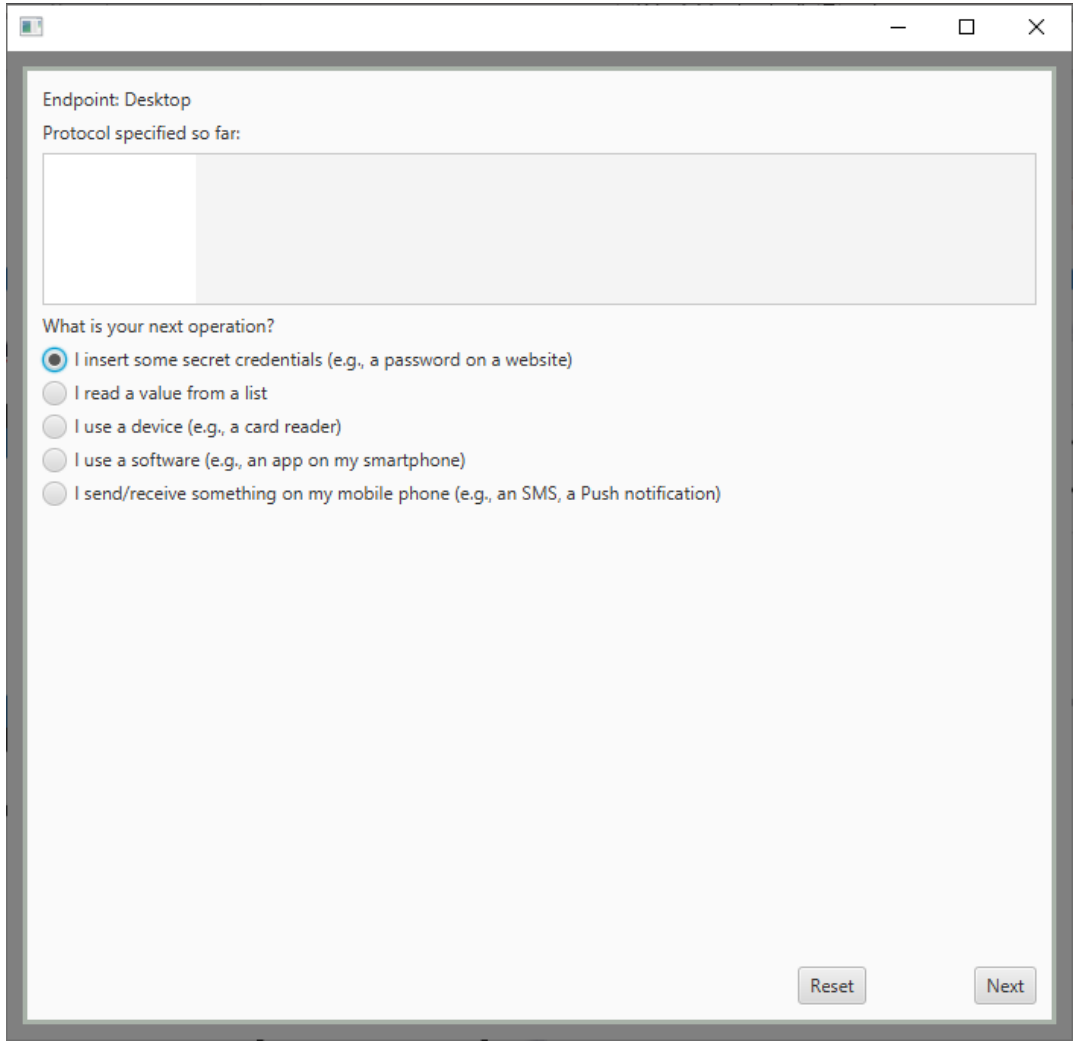
MuFASA



Sicurezza di protocolli

MuFASA – Traduzione

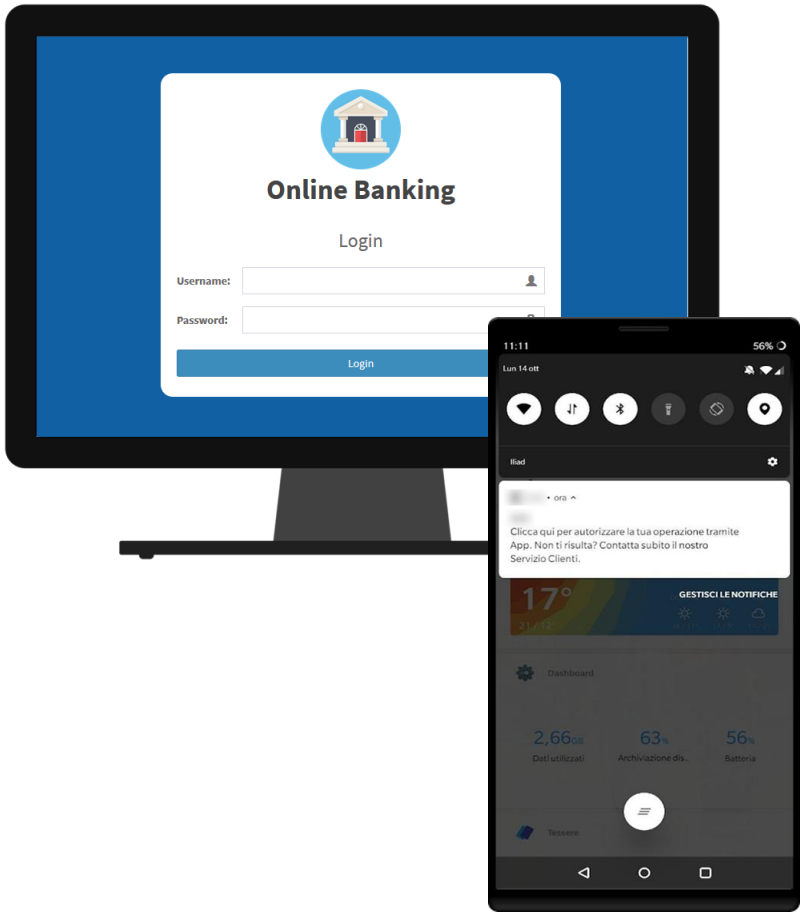
MuFASA

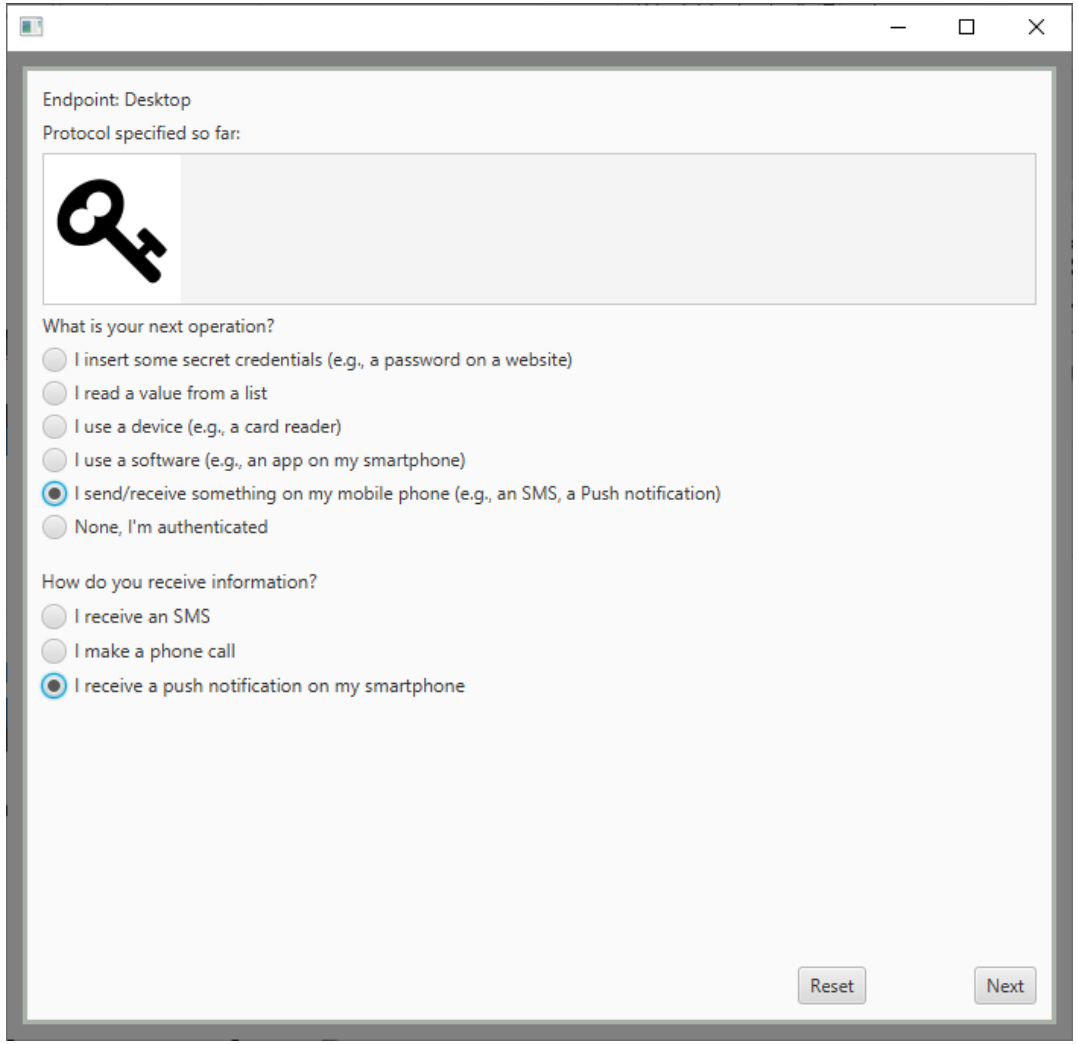


Sicurezza di protocolli

MuFASA – Traduzione

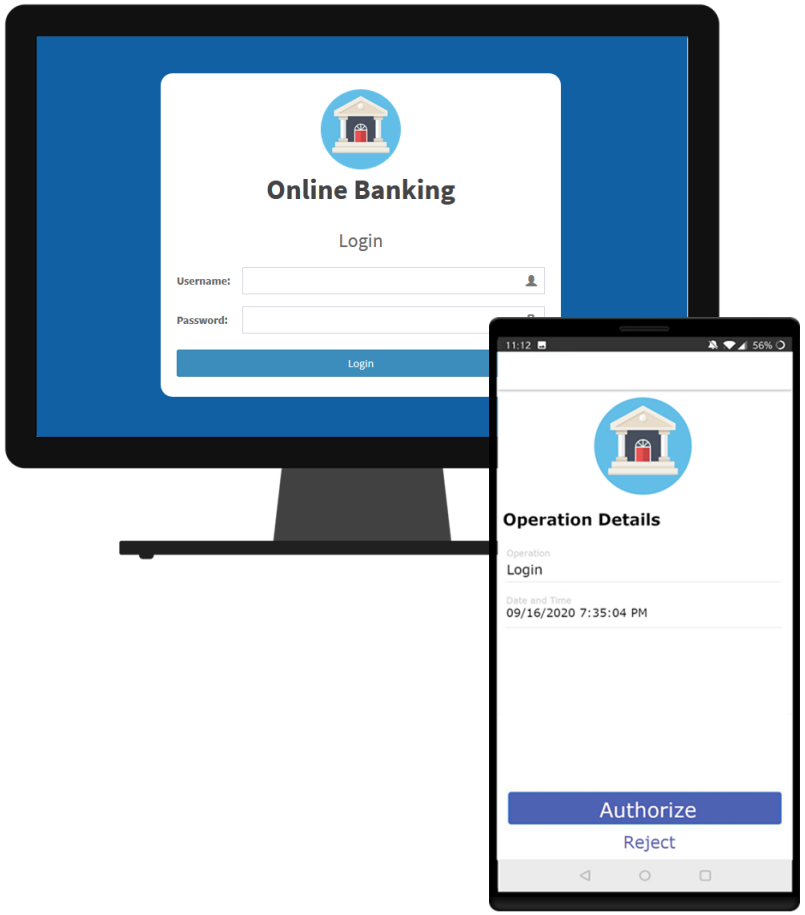
MuFASA

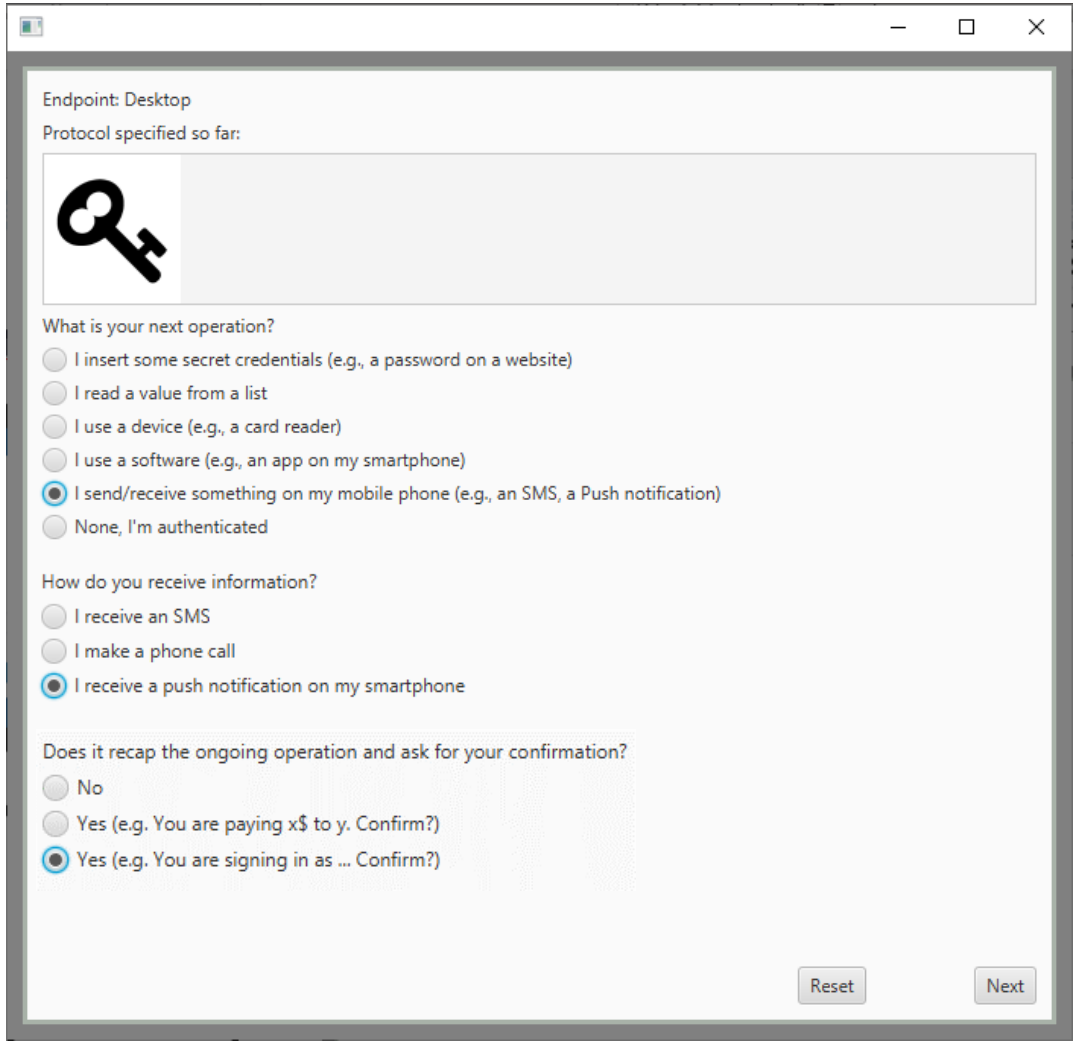




Sicurezza di protocolli
MuFASA – Traduzione

MuFASA

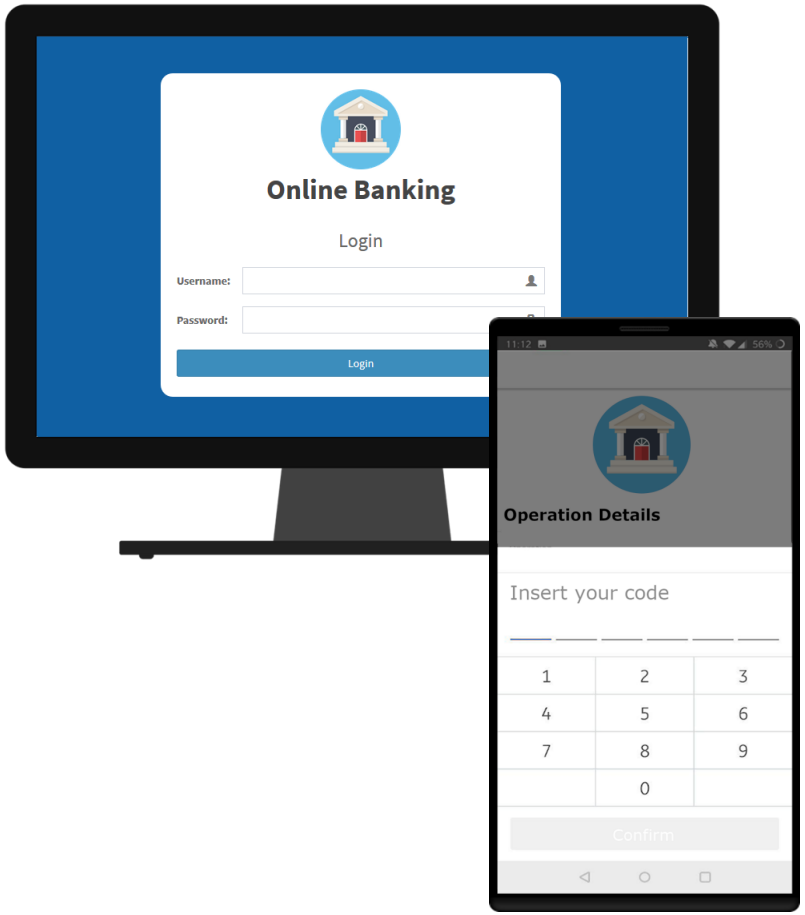


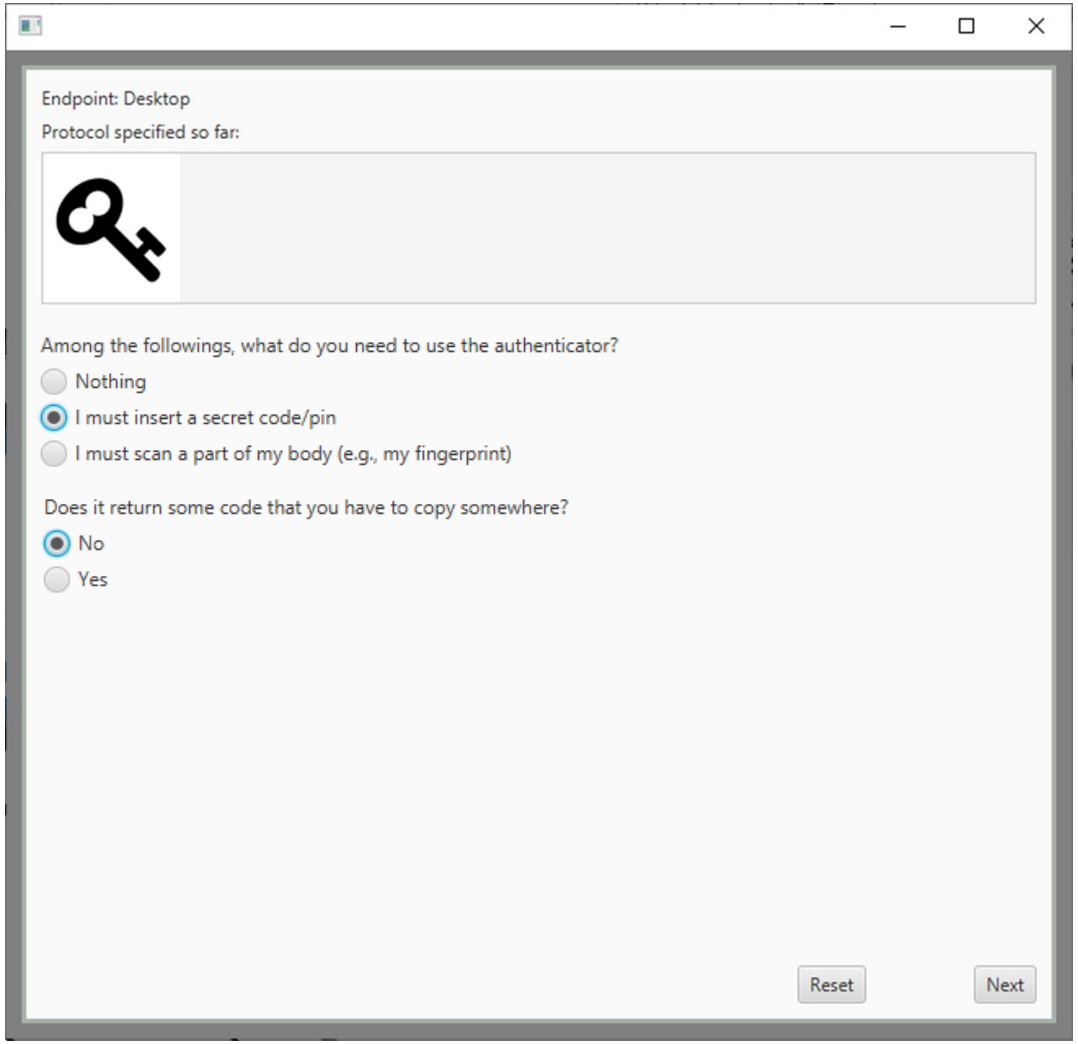


Sicurezza di protocolli

MuFASA – Traduzione

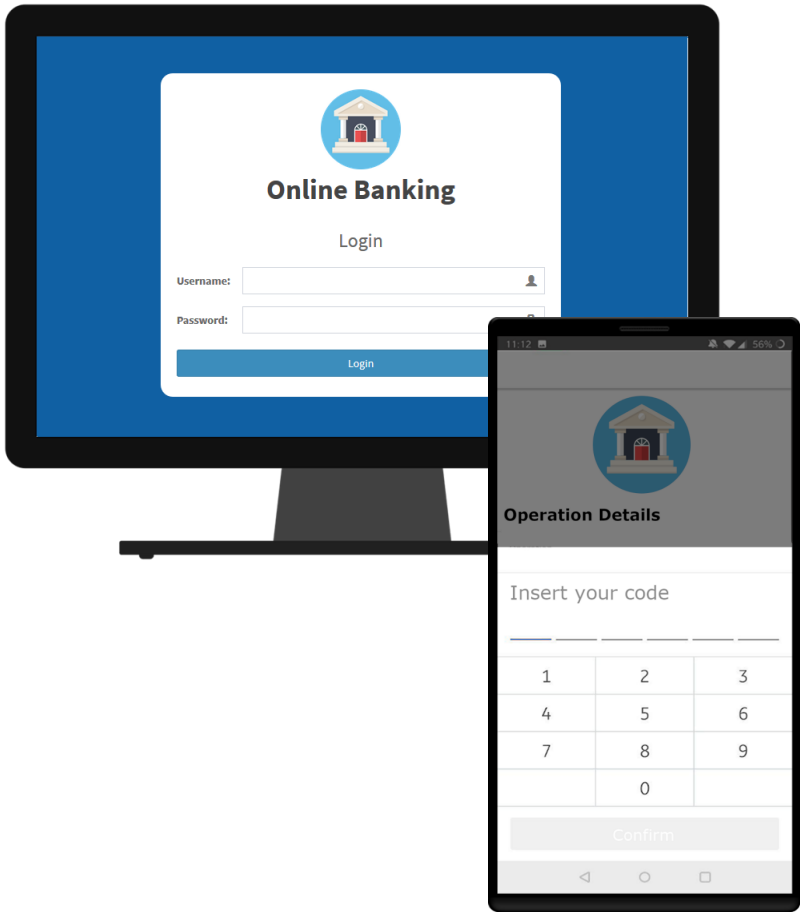
MuFASA

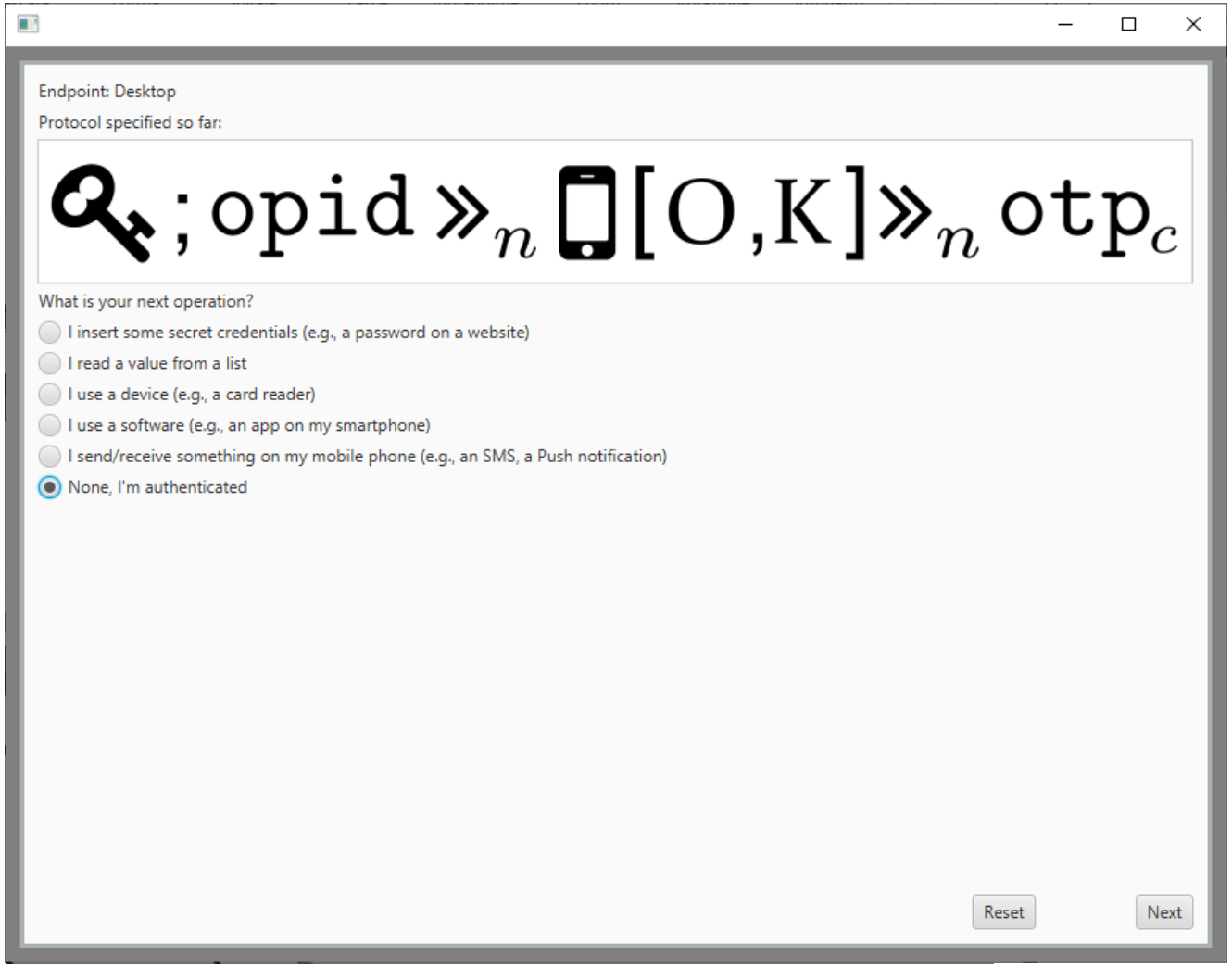




Sicurezza di protocolli
MuFASA – Traduzione

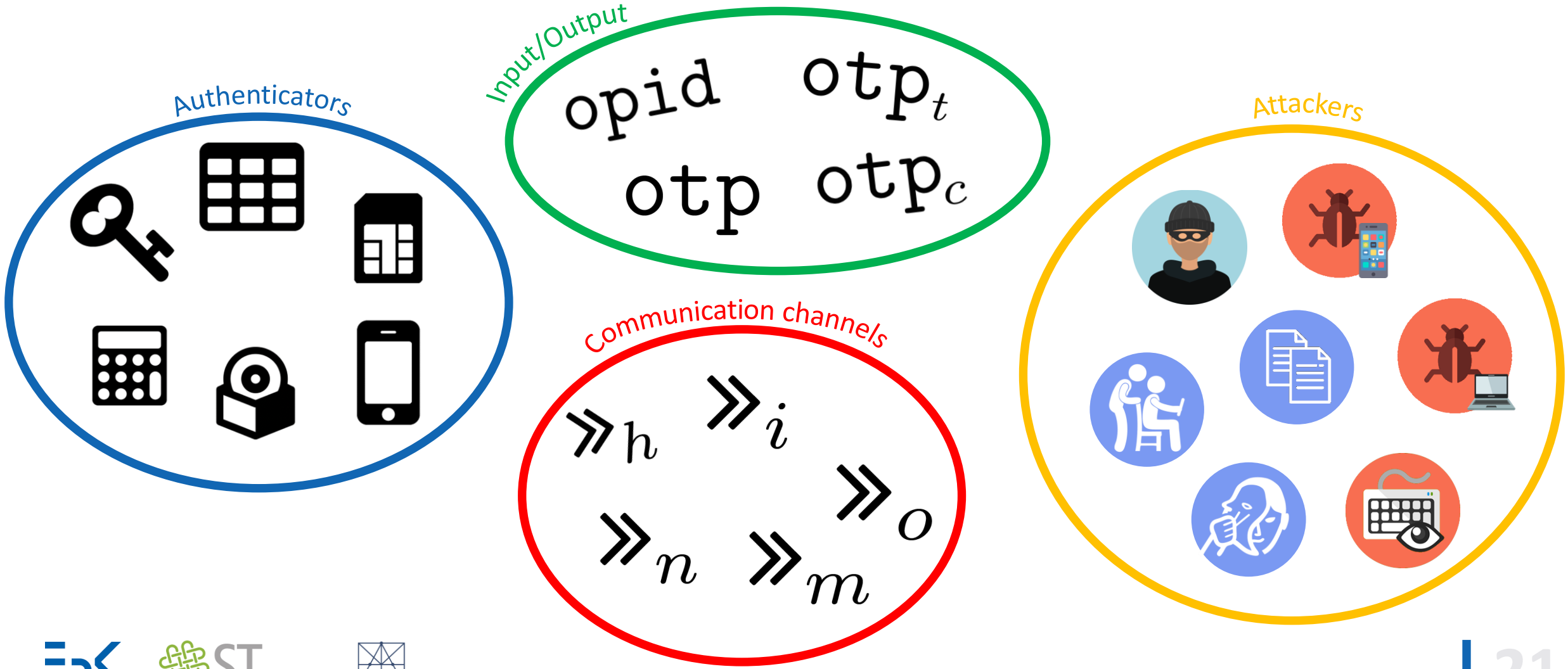
MuFASA





Sicurezza di protocolli
MuFASA – Modellazione

MuFASA



Sicurezza di protocolli
MuFASA – Resoconto

MuFASA

Analysis of MFA Protocol

Info on the Analyzed Protocol:
- *Starting Endpoint:* Desktop
- *Number of authenticators:* 2
- *Employed authentication factors:* [K, K, O]

Protocol Complexity
- *Memory:* 2
- *Manual Operations:* 0
- *Extra Devices:* 0
- ***Complexity Score: 2***

Compliance with security requirements
- *Requirement 1:* true
- *Requirement 2:* true
- *Requirement 3:* true
- *Requirement 4:* false

Result of the resistance analysis

Base attackers: DT, AD, SS, ES, SE, MB, MM

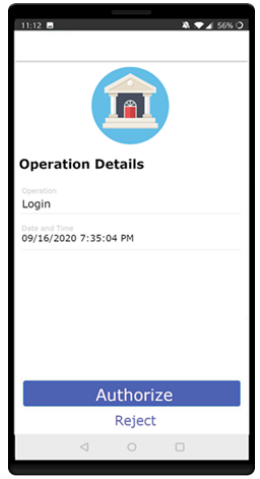
Max number of attackers in combination: 3

Considered attackers: 63

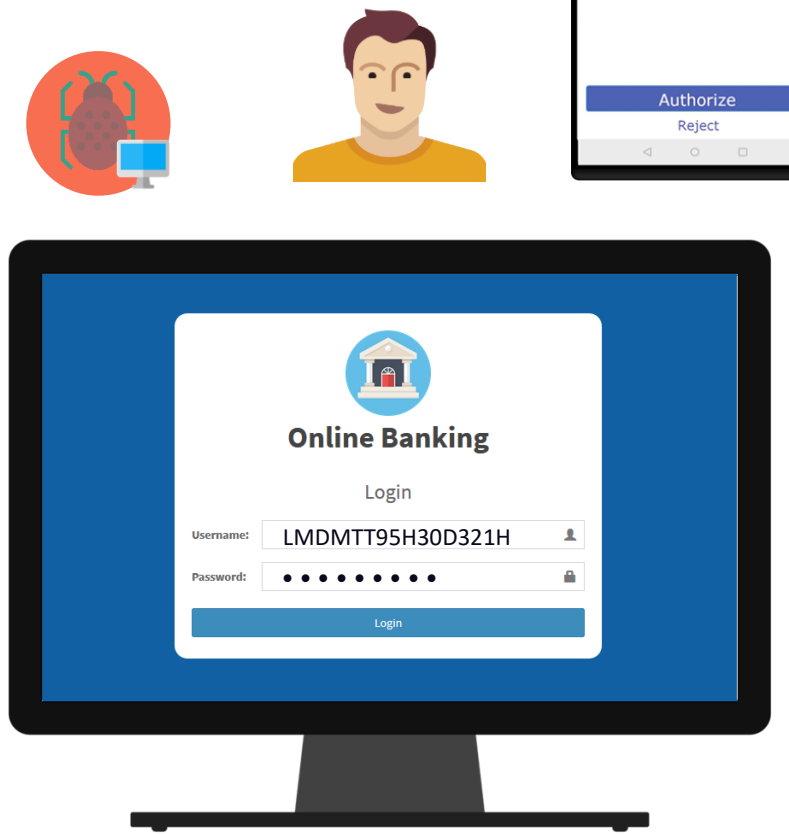
Risk Evaluation

Combinations of attackers	Likelihood	Impact	Risk
MB	MEDIUM	HIGH	HIGH
SE	MEDIUM	MEDIUM	MEDIUM
DT SS	MEDIUM	MEDIUM	MEDIUM
ES MM	LOW	HIGH	MEDIUM
ES DT	LOW	MEDIUM	LOW
SS AD	LOW	MEDIUM	LOW
ES AD	LOW	MEDIUM	LOW
SS MM	LOW	MEDIUM	LOW

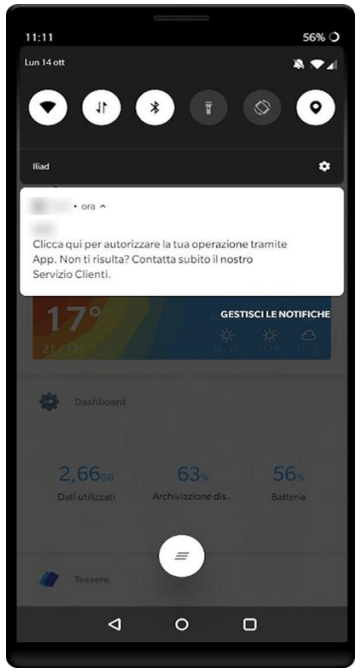
Sicurezza di protocolli
Esempio di attacco

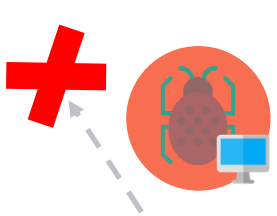


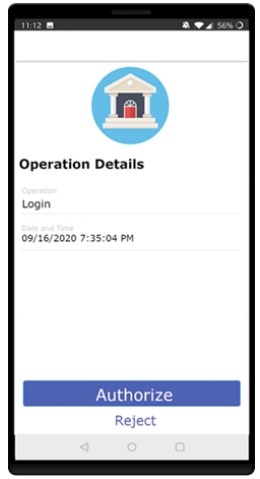
Sicurezza di protocolli
Esempio di attacco



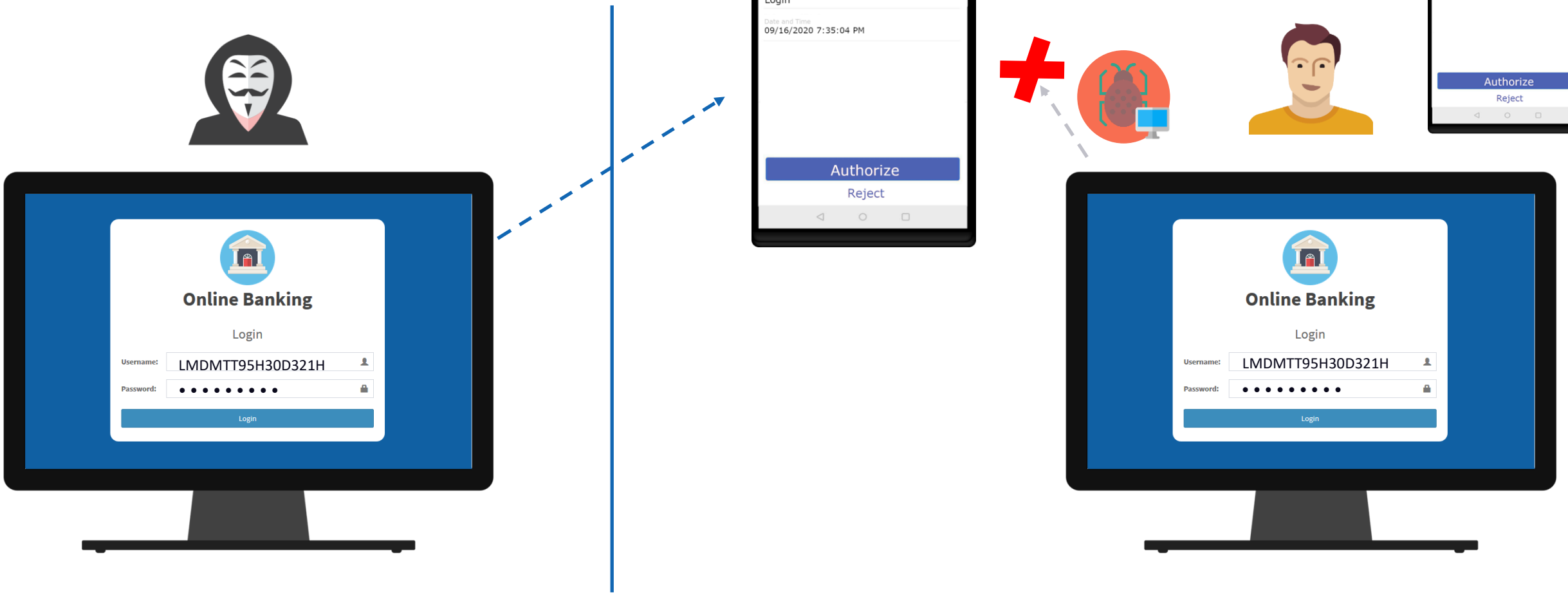
Sicurezza di protocolli
Esempio di attacco



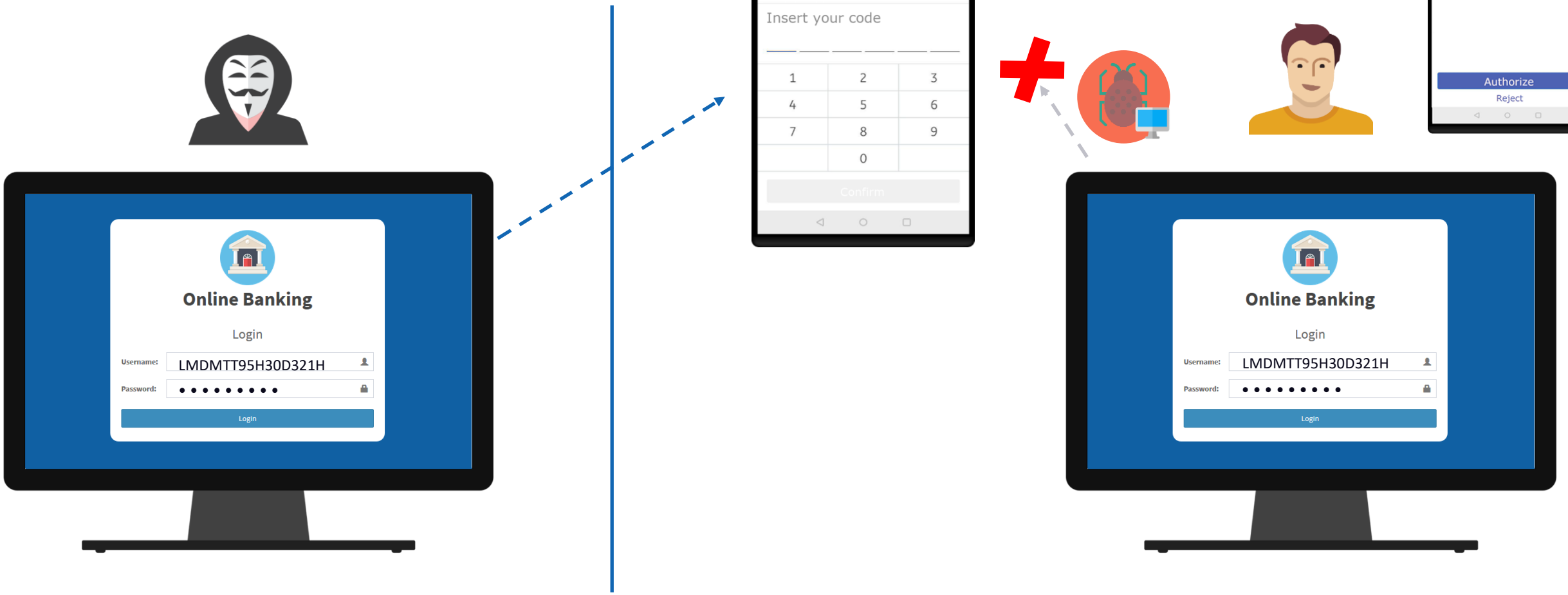




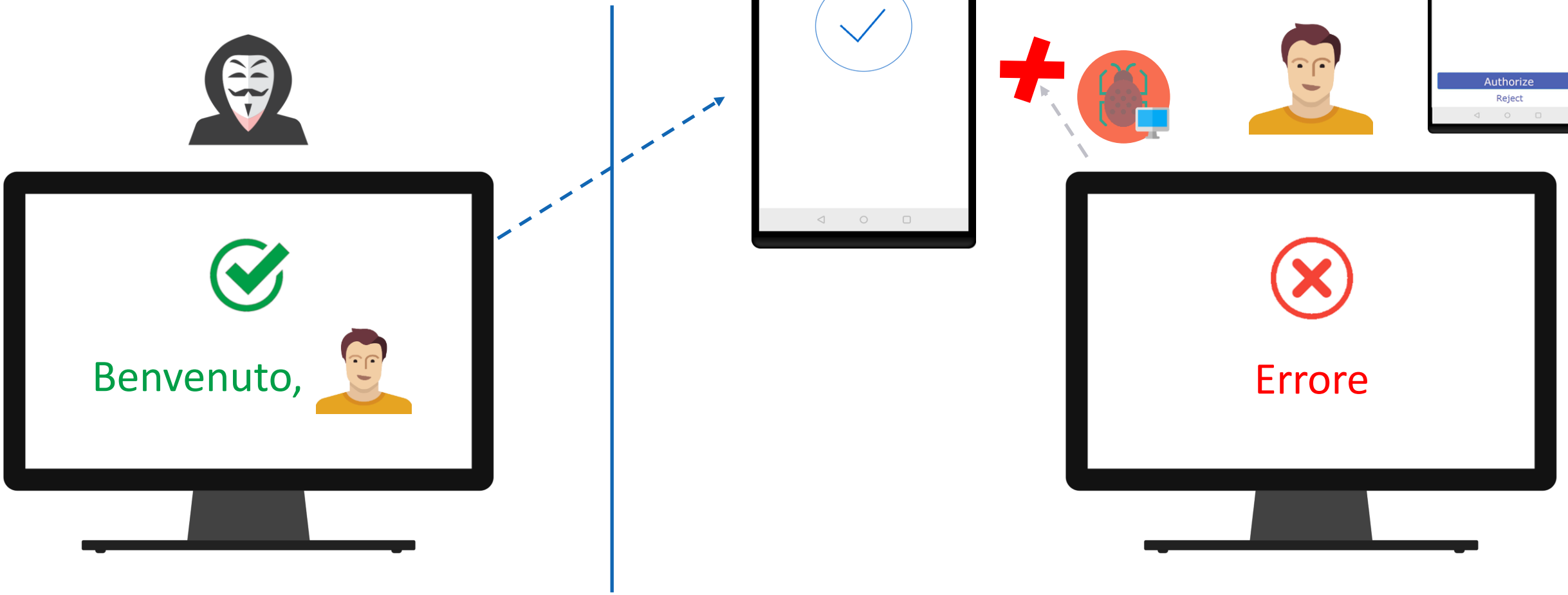
Sicurezza di protocolli
Esempio di attacco



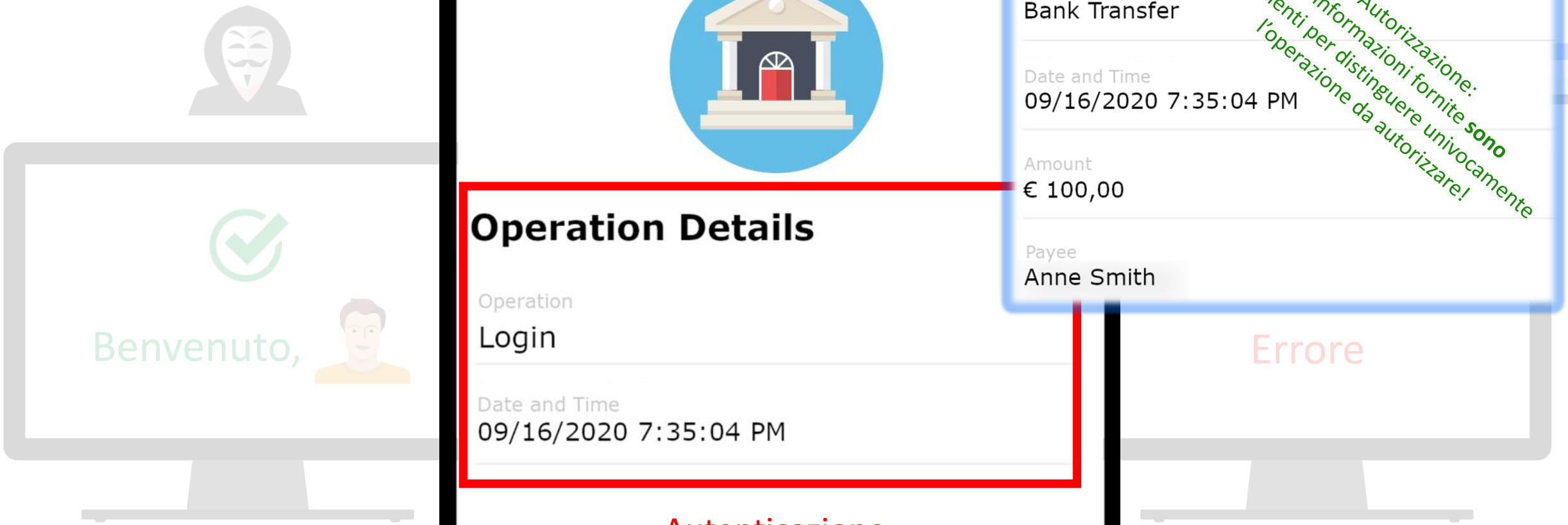
Sicurezza di protocolli
Esempio di attacco



Sicurezza di protocolli
Esempio di attacco



Sicurezza di protoc
Esempio di attacco



Autenticazione:
Le informazioni fornite **non sono**
sufficienti per distinguere univocamente
il tentativo di autenticazione!

Sicurezza di protocolli
Benefici nell'utilizzo di MuFASA

MuFASA

Facilità, tracciabilità e riproducibilità

L'utente descrive il protocollo MFA desiderato rispondendo alle domande poste all'interno di un questionario in linguaggio naturale. Il tool permette l'esplorazione di diverse soluzioni alternative (what-if analysis) garantendo la riproducibilità e la tracciabilità del processo.

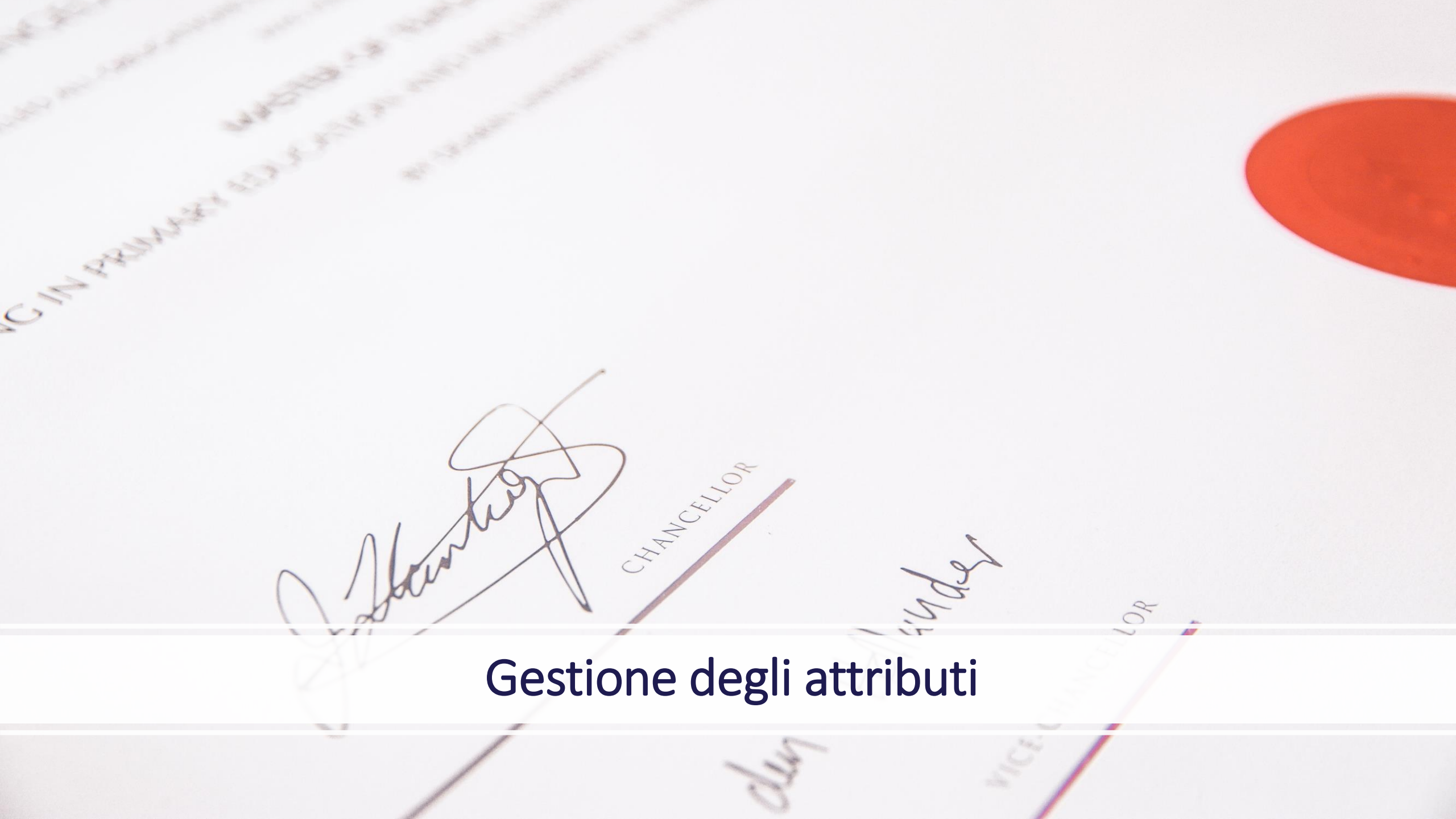
Analisi di sicurezza

Il protocollo descritto viene analizzato al fine di identificare l'impatto di diversi tipi di attaccanti che possono colludere quali:

- Eavesdropping Software
- Man in the Browser
- Shoulder Surfer
- Social Engineering

Mitigazione dei rischi

Il tool restituisce un report con l'indicazione delle misure di mitigazione più appropriate per ciascun tipo di attacco

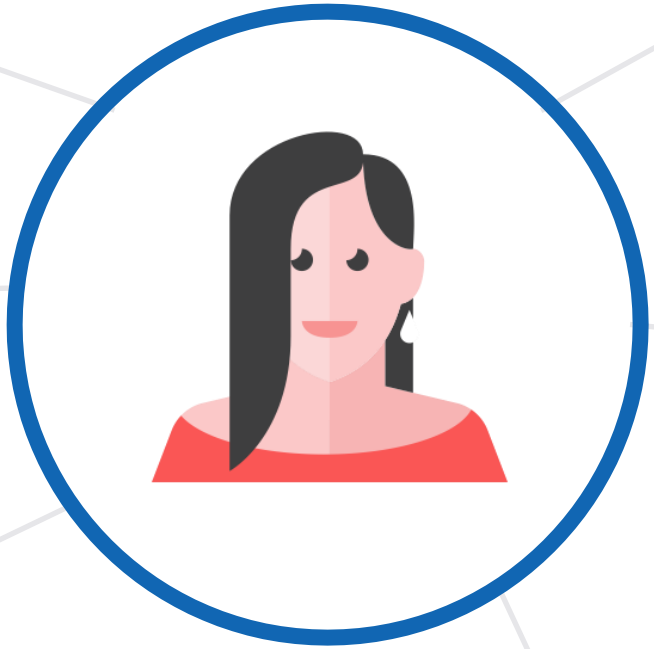


Gestione degli attributi

Identità digitale
...insieme di attributi

Dipendente

Account bancario



Account su social network

email

Informazioni personali

Cittadino

spid

email

Informazioni personali

Siti di e-commerce

email

Indirizzo di spedizione

Numero della carta di credito

...

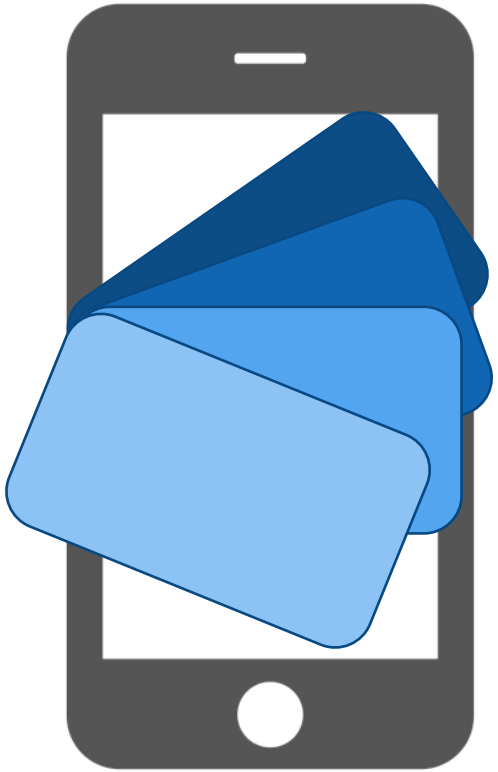
Carte

- Rilasciate da un’autorità
- Attestano proprietà di un soggetto
- Verificabili alla presentazione

Autorità	Attributi	Documento	Verifica
Stato	anagrafica	CIE	chip & PIN
Banca	IBAN	bancomat	chip & PIN
Motorizzazione	# patente	patente	de visu
Telecom	# cellulare	SIM	chip & PIN
GDO	# carta fedeltà	carta fedeltà	-

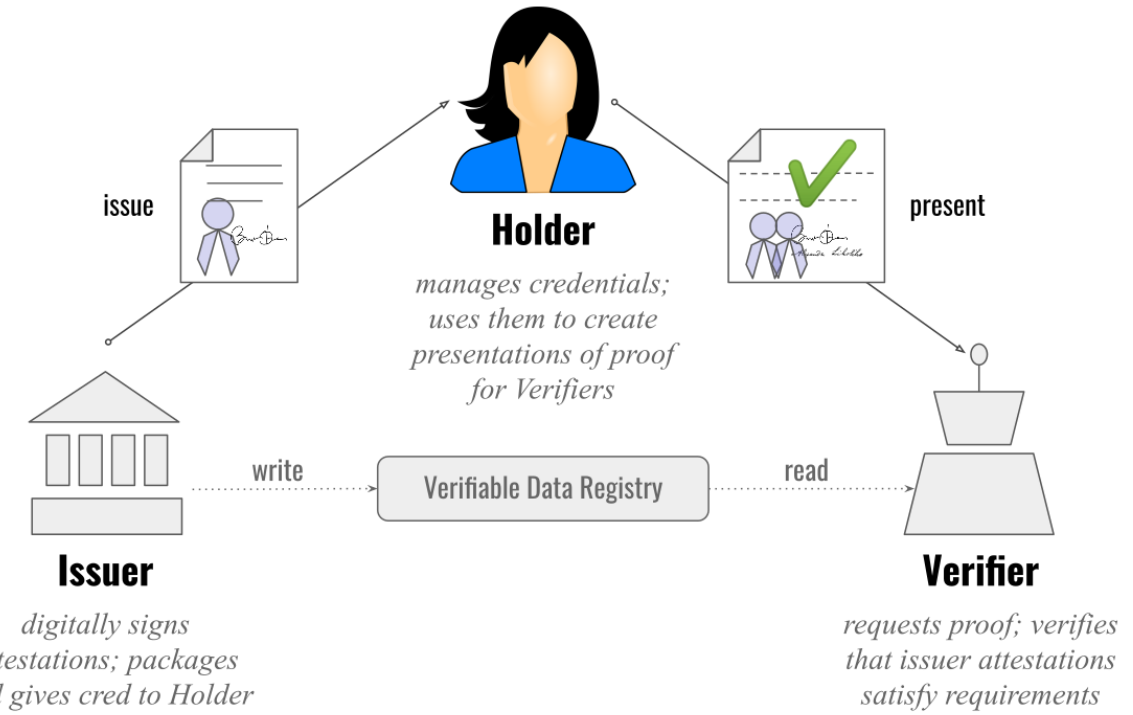
Potenziale digitale

- **Verifica** attestazioni immediata e **remota**
- Nuove attestazioni:
  - Istituto di formazione: diploma
  - Ordine professionale: iscrizione all'albo
  - Datore di lavoro: aziendale
- Nuovi servizi:
  - Firma contratti
  - Sottoscrizione abbonamenti
  - Apertura conti
  - …



Credenziali Verificabili

- W3C recommendation
  - https://www.w3.org/TR/vc-data-model/



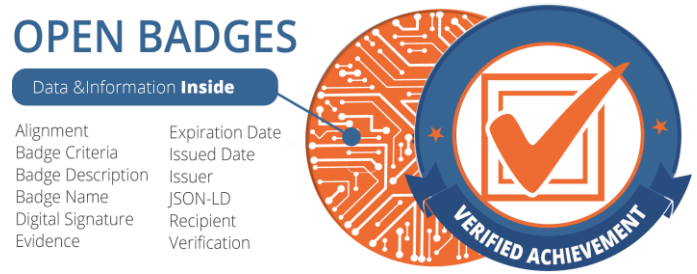
https://commons.wikimedia.org/wiki/File:VC_triangle_of_Trust.svg

Credenziali Verificabili (VC) e Identificativi Decentralizzati (DID)

- Critico il **legame credenziali – identità**: personali, legali, professionali.
- VC: rilascio e verifica attestazioni secondo standard.
- DID: identità non legate a un singolo ente – telecom, email, o specifica app
- Innovazione richiede infrastruttura, gestione informatica, e uno o più servizi; migliora compliance e log; riduce frizione e costi dovuti a errori e ritardi.

Progetti all'orizzonte

- Open Badges
  - https://openbadges.org/
- ID Union
  - https://idunion.org/
  - Bosch, Siemens, Commerzbank, DB, T-mobile…
- Covid Credentials
  - https://www.covidcreds.org/
  - Linux Foundation Public Health (LFPH)
- KYC
  - https://www.cherrychain.it/



https://openbadges.org/
Creative Commons Attribution 4.0 International License

CherryChain®

Security & Trust e identità digitale
Soluzioni e strumenti (selezione)

Analisi automatica di sicurezza dei protocolli di autenticazione multi-fattore
https://dl.acm.org/doi/10.1145/3386685

mIDAssistant
https://github.com/stfbk/mIDAssistant

Pullprinting
https://st.fbk.eu/complementary/CODASPY2021

MuFASA (Multi-Factor Security Analysis)
https://st.fbk.eu/tools/MuFASA

TLSAssistant
https://st.fbk.eu/tools/TLSAssistant

Micro-ID-Gym
A framework that increases awareness for Single Sign-On deployment.
https://st.fbk.eu/tools/Micro-Id-Gym

FONDAZIONE BRUNO KESSLER

ST SECURITY & TRUST

Grazie per l'attenzione!

Marco Pernpruner
mpernpruner@fbk.eu

Giada Sciarretta
giada.sciarretta@fbk.eu

Alessandro Tomasi
altomasi@fbk.eu

https://st.fbk.eu