Regolamento eIDAS e Identity Proofing

25 Maggio 2026

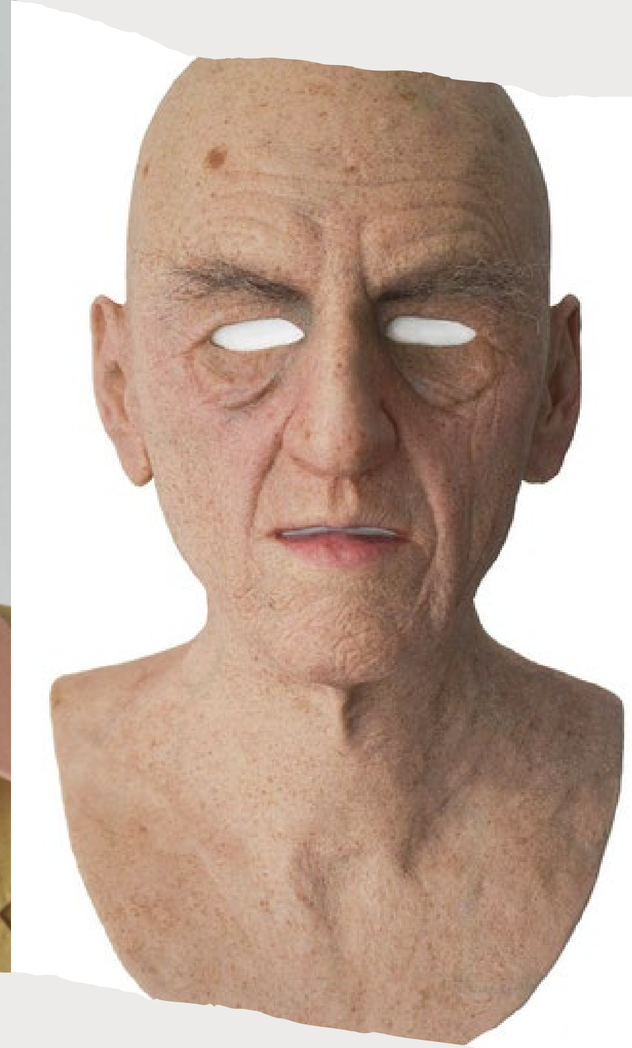
AgID Academy

Gianni Amato
CERT-AGID
Funzionario Area Vigilanza e Sicurezza, AGID

Agency for Digital Italy
Presidency of the Council of Ministers

Deepfake injection
Identity fraud

Verificare un'identità a distanza non è un problema tecnologico, ma di fiducia!



Maschera di silicone

Funziona?

La superficie d'attacco digitale

L'Evoluzione dei Servizi

La spinta verso l'EUDI Wallet e il remote onboarding ha rimosso la barriera della presenza fisica.

- → Transizione completa verso il Fintech
- → Onboarding 100% asincrono
- → Digitalizzazione dei documenti primari

⚠ Rischi Critici

Niente presenza fisica = Segnali manipolabili

Ambiente non controllato = Device compromesso

Dispositivo non affidabile = Bypass della camera

Il regolamento **eIDAS-2.0** (che istituisce *EUDI Wallet*) è entrato in vigore nel maggio 2024
UE prevede che **ogni Stato membro renda disponibile il proprio wallet entro dicembre 2026**.

- Provider di identità per il Wallet nazionale: **SPID** e **CIE**
- **IT-Wallet** sarà il portafoglio nazionale

Ruolo	Livello	Funzione rispetto a EUDI
SPID / CIE	Identità nazionale “tradizionale”	Fornitori di identità che alimentano il wallet nazionale. Ereditano il ruolo di "Identity Provider fondamentali" con livello di garanzia Elevato (LoA High).
IT-Wallet (su App IO)	Wallet nazionale	Portafoglio dichiaratamente conforme a EUDI, che include credenziali PA e può integrare SPID/CIE.
EUDI Wallet (standard UE)	Ecosistema UE	Quadro normativo e tecnologico che regola interoperabilità, sicurezza, trust e portabilità dei wallet nazionali.

Meccanismi di remote proofing

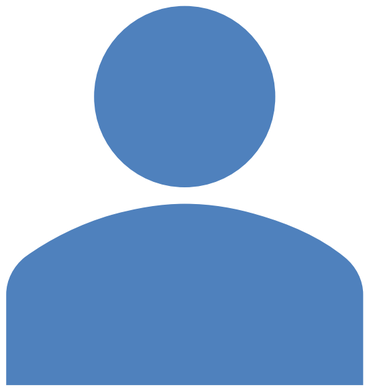
*L'identità **non** viene verificata da una persona fisica ma da un **sistema** > **algoritmo***

Acquisizione

Raccolta di documenti (ID/ Passaporto) e biometria (foto/ video) tramite app.

Verifica

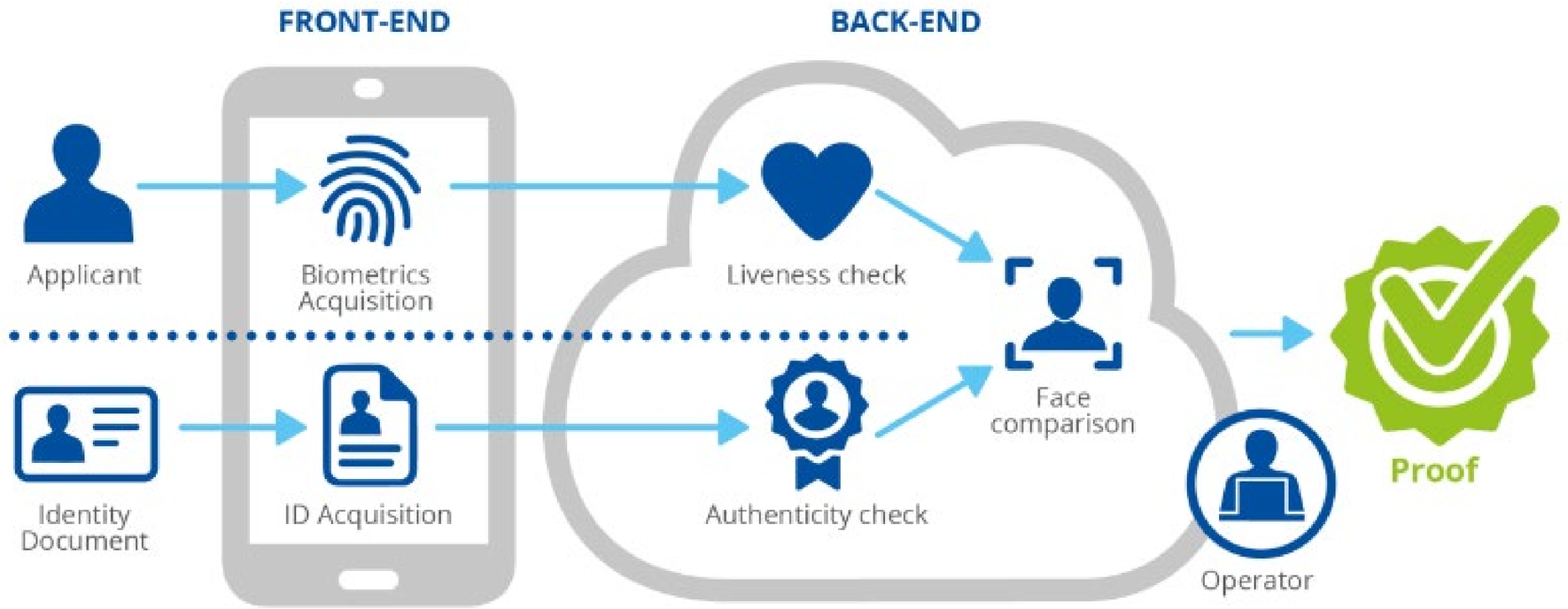
Matching biometrico e controlli automatici (OCR, Liveness) via Back-end.



Validation

Binding

Associazione definitiva tra l'identità verificata e l'utente digitale.



Dove nasce la fiducia nel remote onboarding

Il processo è diviso tra acquisizione e decisione

- Front-end → raccolta dati (non affidabile)
- Back-end → analisi automatica
- Output → identità verificata

Acquisition: La raccolta dell'Identità digitale

- Dati testuali: Estrazione automatica delle informazioni tramite OCR dal documento d'identità:

- Nome e Cognome
- Data di nascita
- MRZ della tessera

- **Dati biometrici:** Acquisizione dello scatto della foto del documento e di un selfie in tempo reale dell'utente tramite la fotocamera dello smartphone.

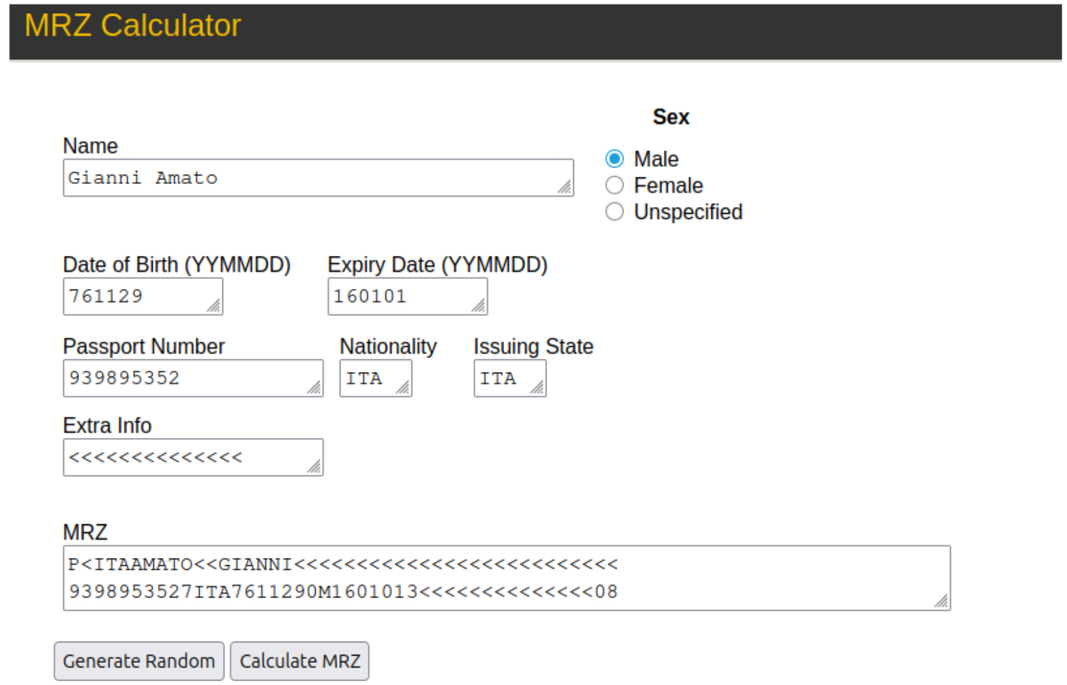
- **Sorgente non affidabile:** L'utente potrebbe inquadrare lo schermo di un computer che mostra il documento di un'altra persona.

- **Flusso video / Camera Injection:** Un attaccante avanzato non usa la fotocamera fisica, ma emula il dispositivo software iniettando un flusso video preregistrato o modificato direttamente nell'applicazione di onboarding.

Presentation vs Injection attacks

Categoria	Metodo	Meccanismo d'Attacco	Livello
Presentation	Replay Video	Video riprodotto su display esterno davanti alla camera	Fisico
Presentation	Maschere 3D	Artefatti fisici per imitare i tratti del volto	Fisico
Injection	Virtual Camera	Software che simula una webcam iniettando video manipolati	Digitale
Injection	Deepfake Bypass	Contenuto sintetico che scavalca l'intera pipeline hardware	Digitale

Validation: Il controllo documentale



- **Controlli di coerenza logica:** Verifica algoritmica dei checksum presenti nella banda MRZ (Machine Readable Zone) sul retro del documento.
- **Analisi degli elementi di sicurezza:** Algoritmi di visione artificiale controllano la presenza di ologrammi, filigrane, i font ufficiali dello Stato e la corretta formattazione dei bordi.

- **Falsificazioni:** Al falsario basta saper fare un calcolo matematico elementare per generare i numeri giusti e ingannare i software di validazione.
- **Mancanza di verifica hardware:** Nei flussi commerciali asincroni non viene letto il chip NFC del documento elettronico (CIE o passaporto), limitandosi all'analisi della foto, che è facilmente manipolabile tramite software di fotoritocco.

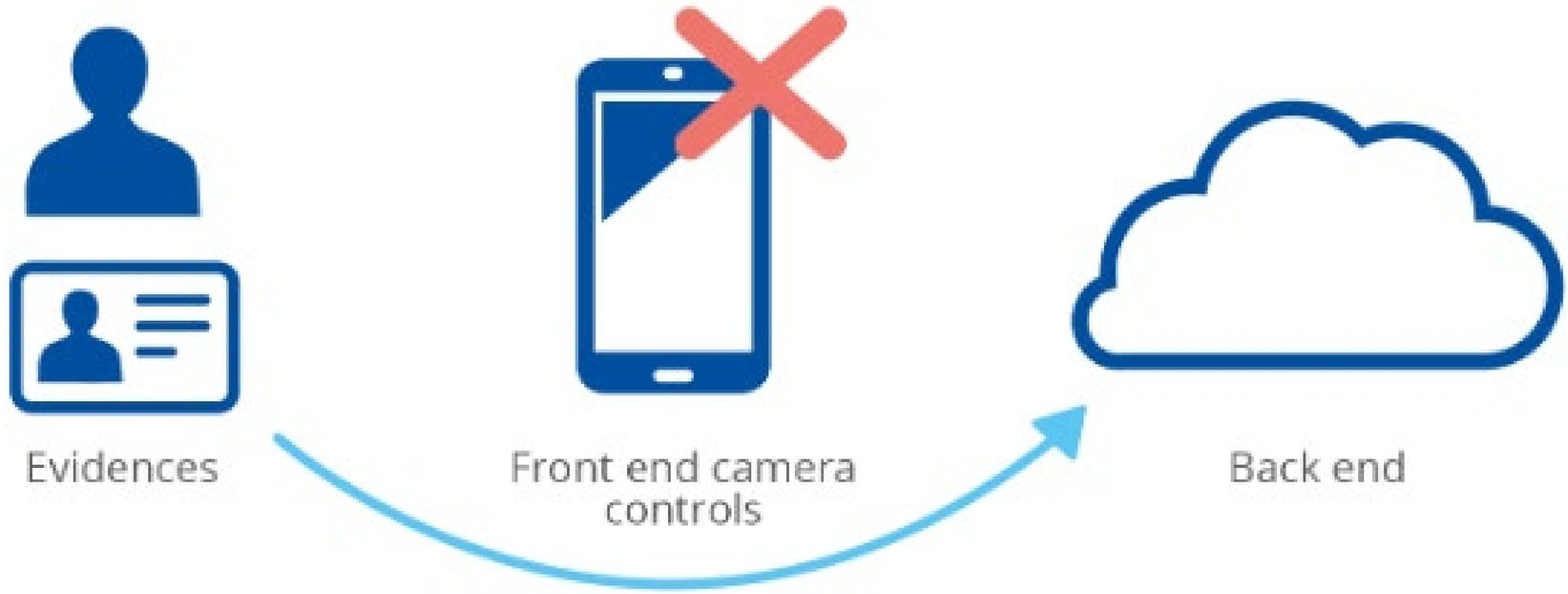
Verification: Biometria e liveness

- **Face Matching:** L'algoritmo confronta i vettori biometrici estratti dalla foto del documento con quelli del selfie scattato sul momento, calcolando un punteggio di somiglianza probabilistica.

- **Liveness Detection:** *Attiva,* può chiedere di fare azioni imprevedibili come ruotare la testa o sbattere le palpebre o *Passiva,* analisi della texture della pelle, della profondità e della luce riflessa dallo schermo.

- **Software injection (camera bypass):** L'attaccante non si presenta davanti alla telecamera con una maschera. Usa emulatori o strumenti di *hooking* software per intercettare il flusso della fotocamera fisica del telefono e sostituirlo con un file video sintetico (Deepfake) generato al computer.

- **Il software ingannato alla radice:** Poiché il video iniettato è programmato al computer per muovere gli occhi o girarsi esattamente quando l'app lo richiede, i controlli di *liveness attiva* falliscono strutturalmente. Inoltre, l'algoritmo analizza pixel perfetti convinto che arrivino dal sensore fisico della fotocamera, mentre sta analizzando un flusso artificiale.



Injection attack. L'IA rende tutto più reale

Se l’attaccante controlla l’input, può simulare:

- **movimento**
- **espressioni**
- **comportamento**

Binding: legame crittografico

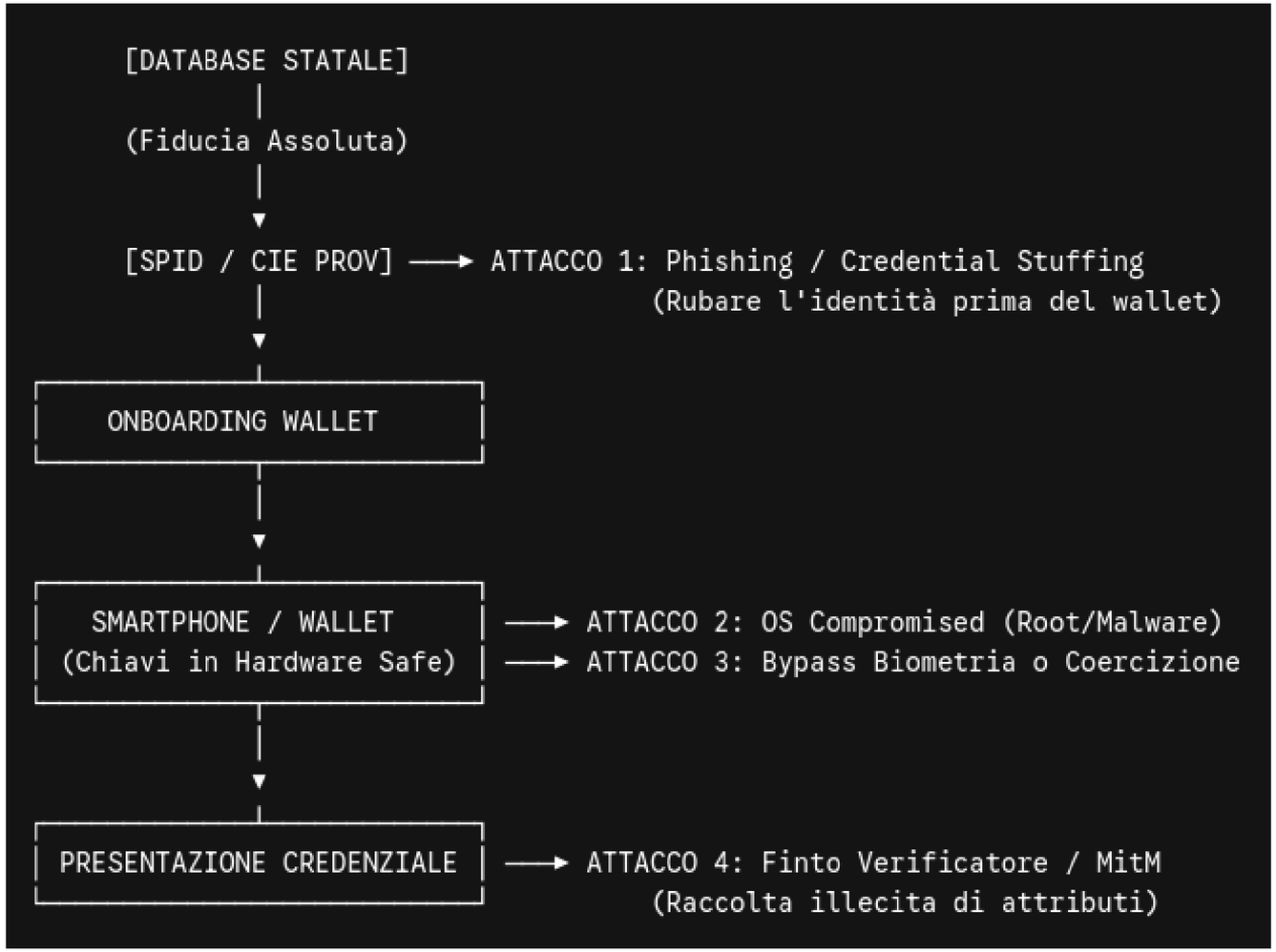
*Una volta accertata l'identità (tramite i controlli precedenti o ereditandola da un sistema certo come SPID/CIE), il sistema deve "**legare**" (binding) in modo indissolubile l'**identità digitale** al **dispositivo fisico** dell'utente.*

- **Generazione key:** Il telefono genera una coppia di chiavi asimmetriche (pubblica e privata).
- **Isolamento HW:** La chiave privata viene sigillata all'interno del chip di sicurezza dedicato dello smartphone *(Secure Enclave su iOS, StrongBox su Android)*. Questa chiave non può essere letta o esportata da nessun software, nemmeno dal sistema operativo.
- **Sblocco locale:** L'uso della chiave privata viene subordinato alla biometria locale: il FaceID/TouchID del telefono che sblocca il chip hardware, non l'app.

- **Bypass logico su OS compromessi:** Smartphone infettato da un malware con privilegi di Root o Jailbreak, l'attaccante non può estrarre la chiave privata, ma può manipolare l'applicazione che la usa. L'app chiede al chip "*la biometria è corretta?*", il malware altera la risposta software convertendola in un "SÌ" artificiale, firmando operazioni all'insaputa dell'utente e bypassando il FaceID fisico.
- **Phishing dell'onboarding:** Senza un secondo controllo basta un phishing delle credenziali SPID della vittima e avvia l'onboarding sul *proprio* smartphone modificato. Il sistema genererà le chiavi hardware sul telefono dell'attaccante, legando legalmente l'identità della vittima al dispositivo del criminale.

Vettori di attacco

Dove può attaccare un adversary



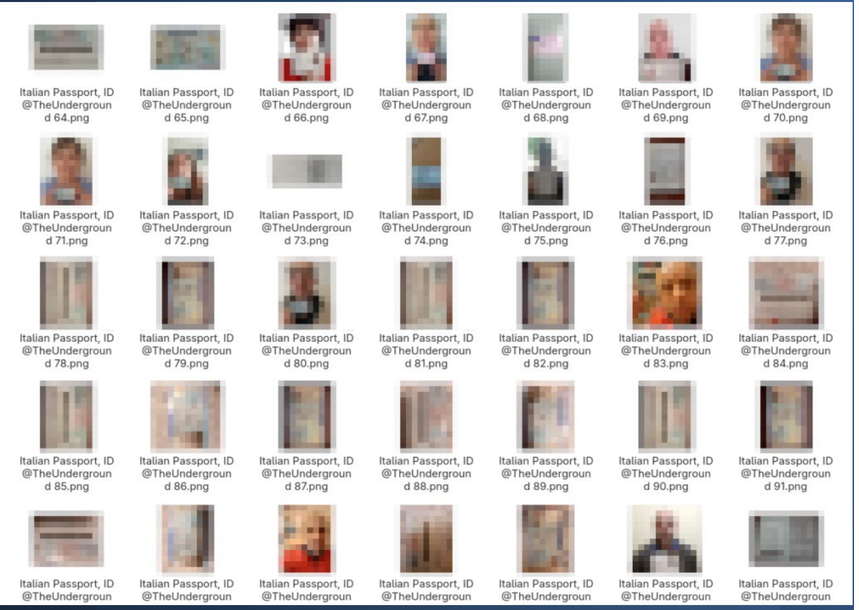
Il limite del remote identity proofing

Dipendenza dal segnale

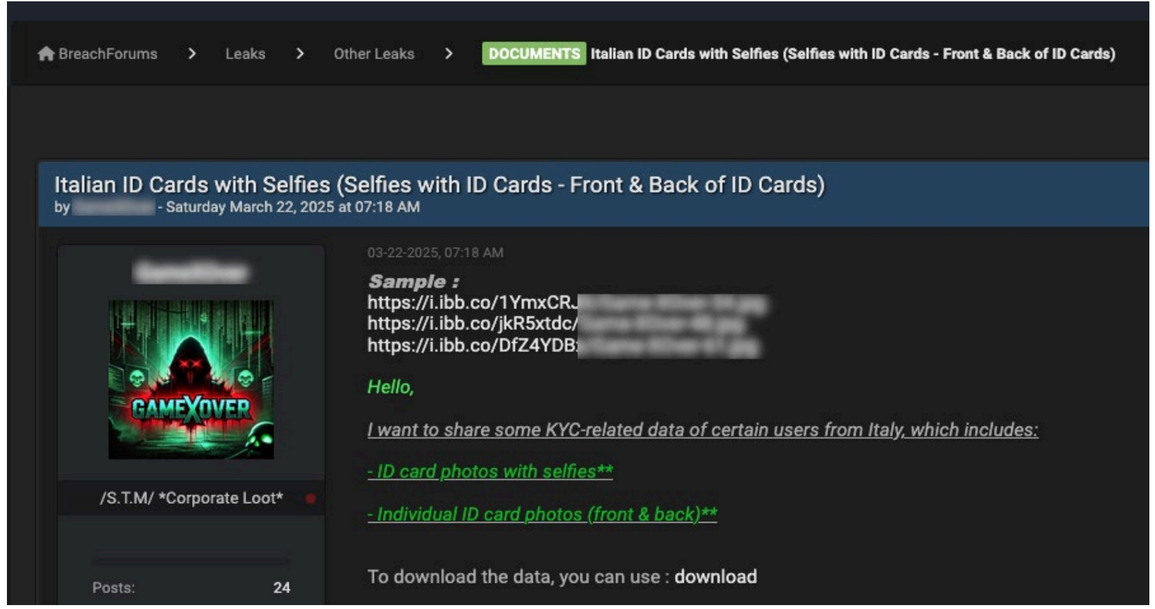
Non stiamo verificando una persona, stiamo verificando **dati digitali** su quella persona.

- Il sistema assume che i dati siano autentici alla fonte
- Viene verificata la **coerenza**, non la realtà fisica
- Tutto ciò che passa per il device può essere alterato

In presenza	Da remoto
○ documento fisico ○ persona reale ○ controllo diretto	○ immagini ○ stream video ○ segnali digitali



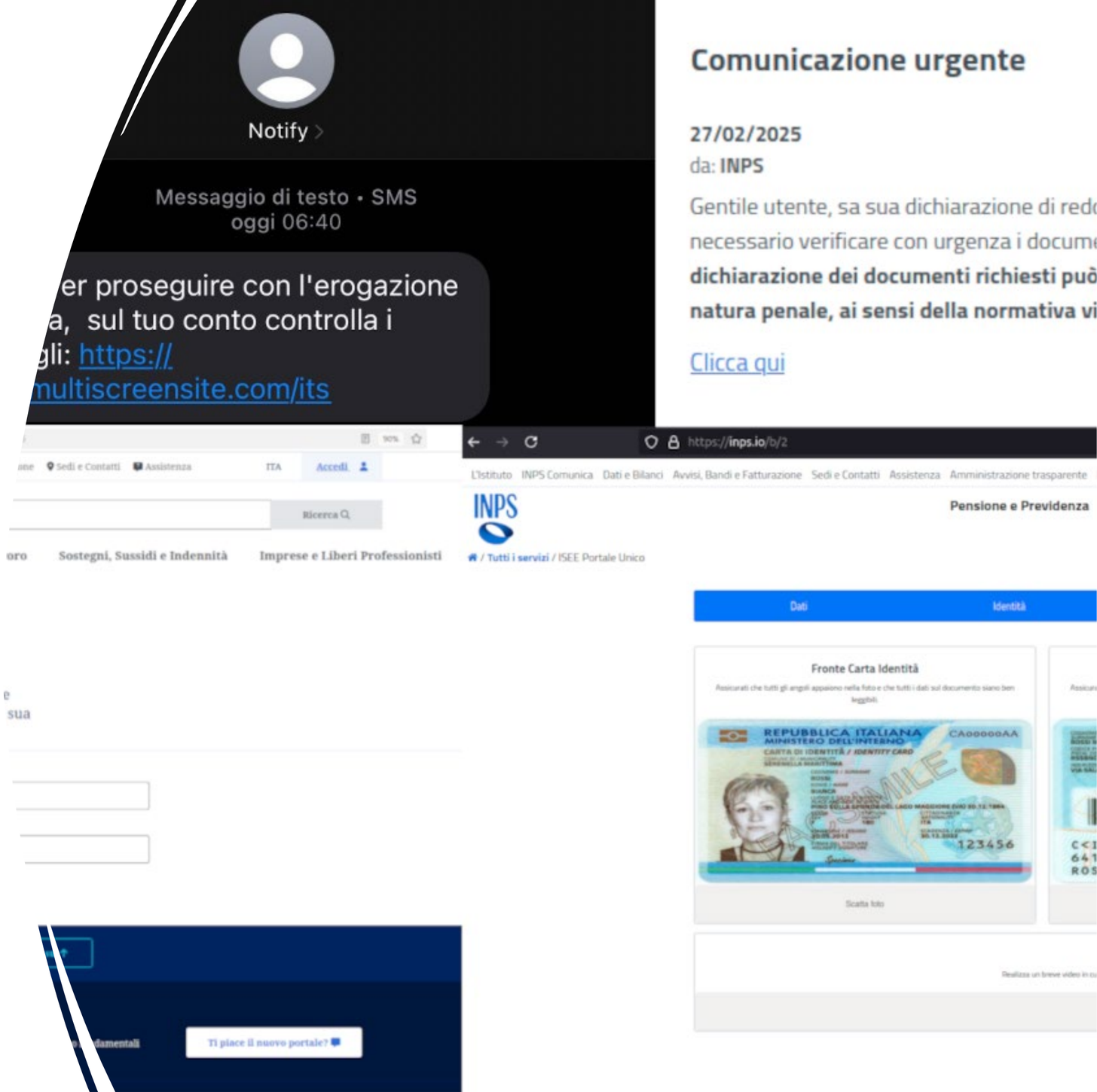
Il furto di identita'



Smishing

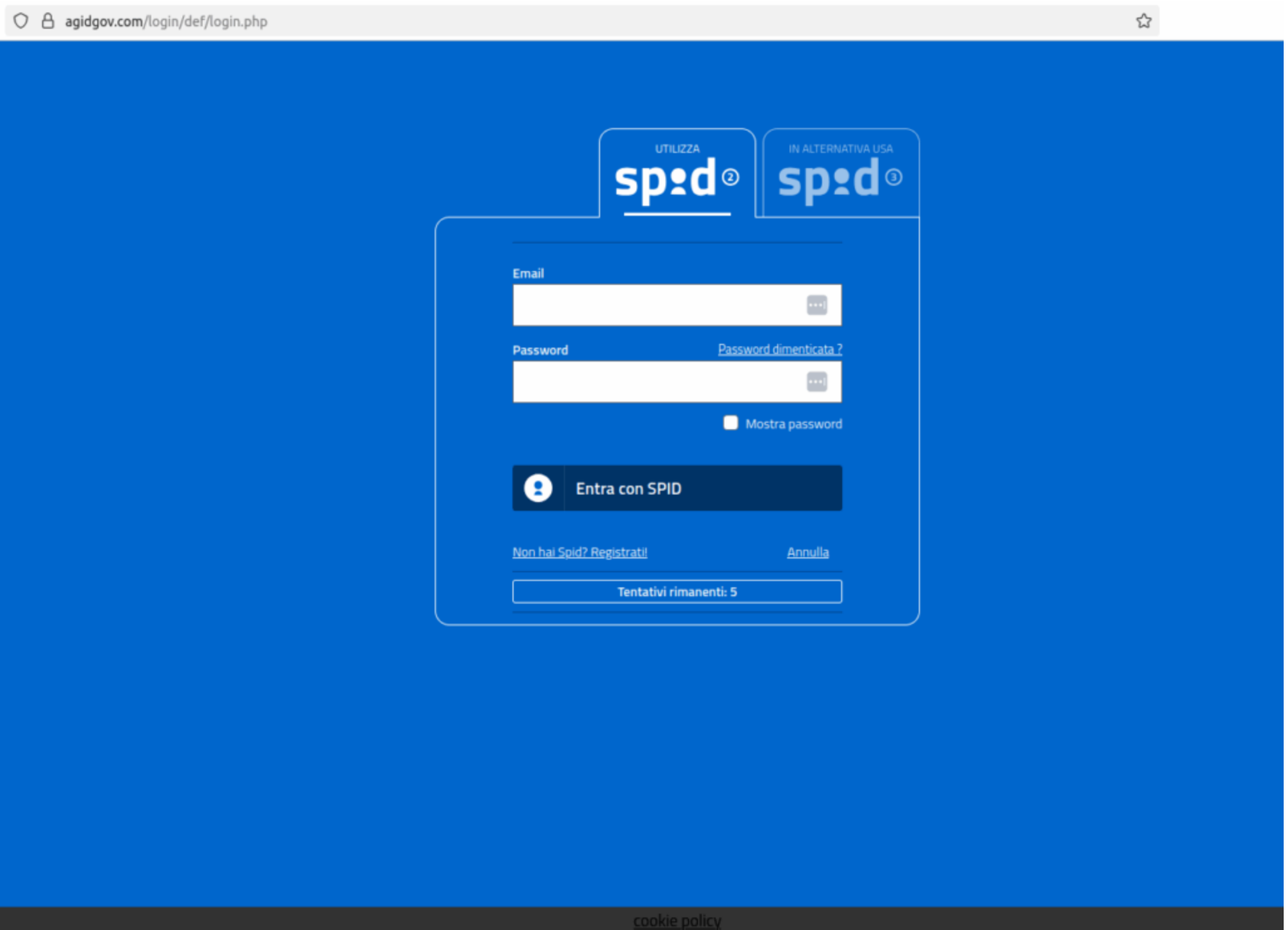
File rubati
- Carta identita'
- Patente guida
- Tessera sanitaria
- Buste paga
- Selfie

Obiettivo
- Creare false identità digitali
- Impossessarsi degli emolumenti statali



Non solo INPS, anche AgID

Dominio creato ad-hoc



Gentile Sig. [redacted],

La informiamo che, per garantire la continuità dei servizi a lei dedicati, è necessario effettuare l'aggiornamento della documentazione richiesta tramite il nostro portale.

La invitiamo cortesemente a completare la procedura entro il **07/05/2025**

In caso di mancato aggiornamento, i servizi potranno essere temporaneamente sospesi fino alla regolarizzazione.

Aggiorna la Documentazione

Per eventuali chiarimenti o assistenza, restiamo a sua disposizione.

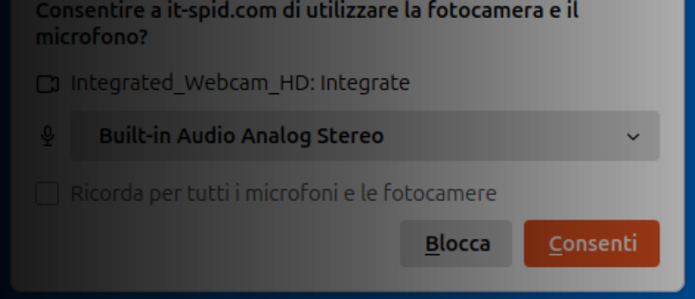
Cordiali saluti,

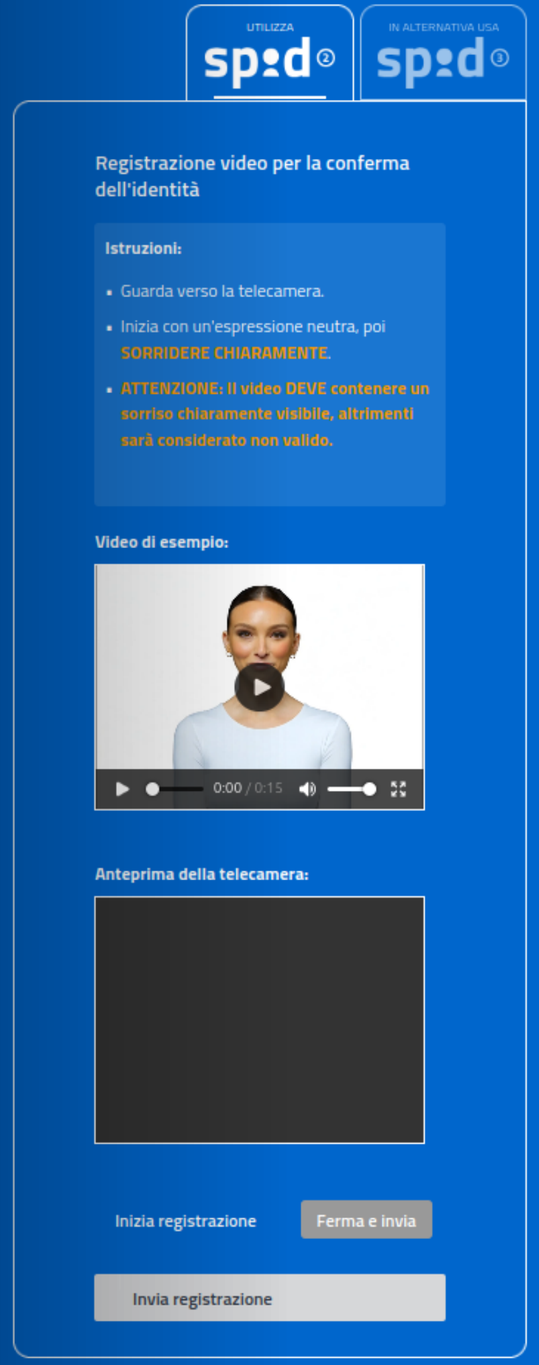
spid
Sistema Pubblico di Identità Digitale

Riceve questa email in quanto cliente registrato presso il Sistema Pubblico di Identità Digitale. Se ha già completato l'aggiornamento, può ignorare questo messaggio.

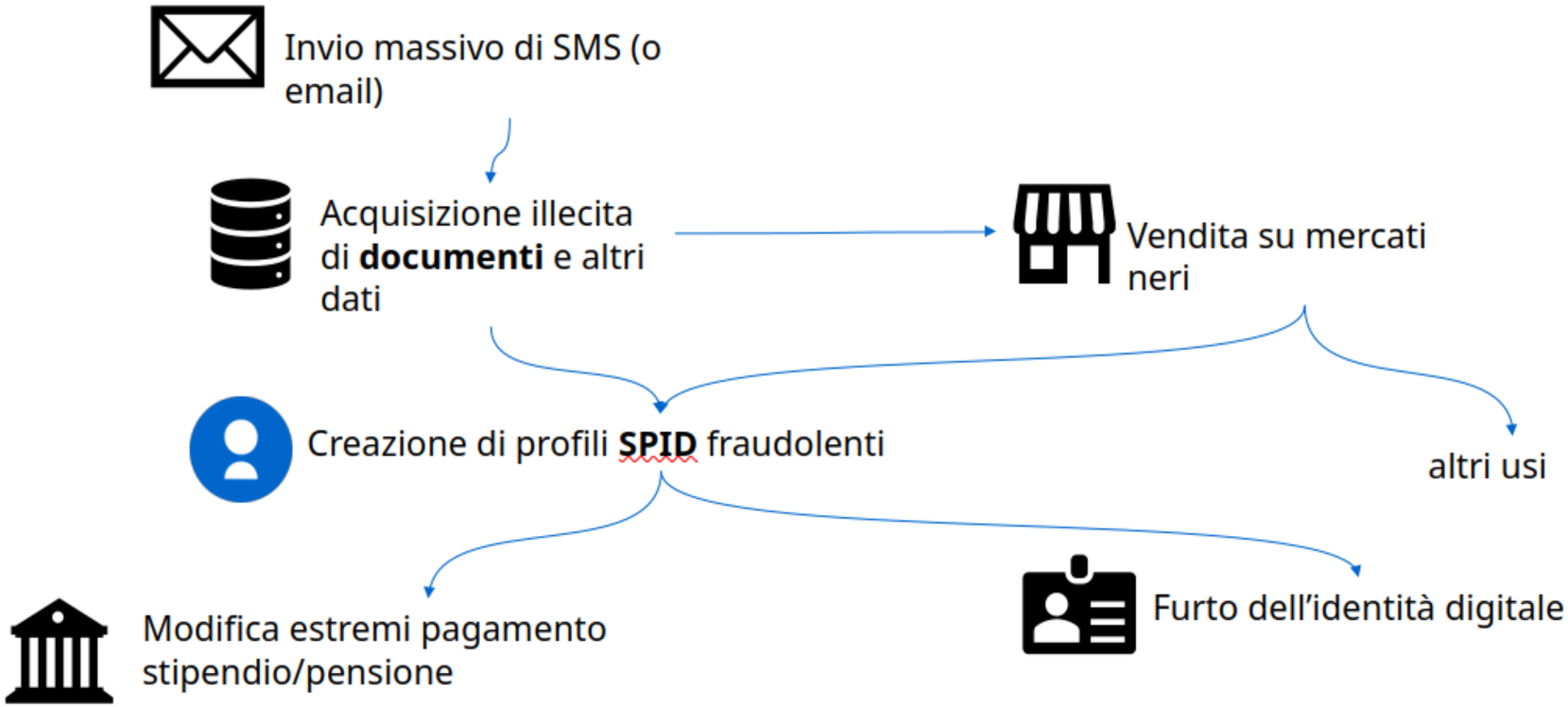
Registra un video sul momento

Guarda verso la telecamera
Sorridi chiaramente





Monetizzare dai documenti



Il ciclo di vita della frode

IT-Wallet. Identità digitale nel mondo reale

Partirà a breve

- documenti e attributi su smartphone
- integrazione con app IO uso pubblico e privato
- interoperabilità UE

identità digitale diventa

- riutilizzabile
- condivisibile
- centrale

Cambio di paradigma con EUDI Wallet e il modello eIDAS 2.0

EUDI Wallet risolve le minacce descritte ***eliminando il remote onboarding asincrono basato su selfie****.*

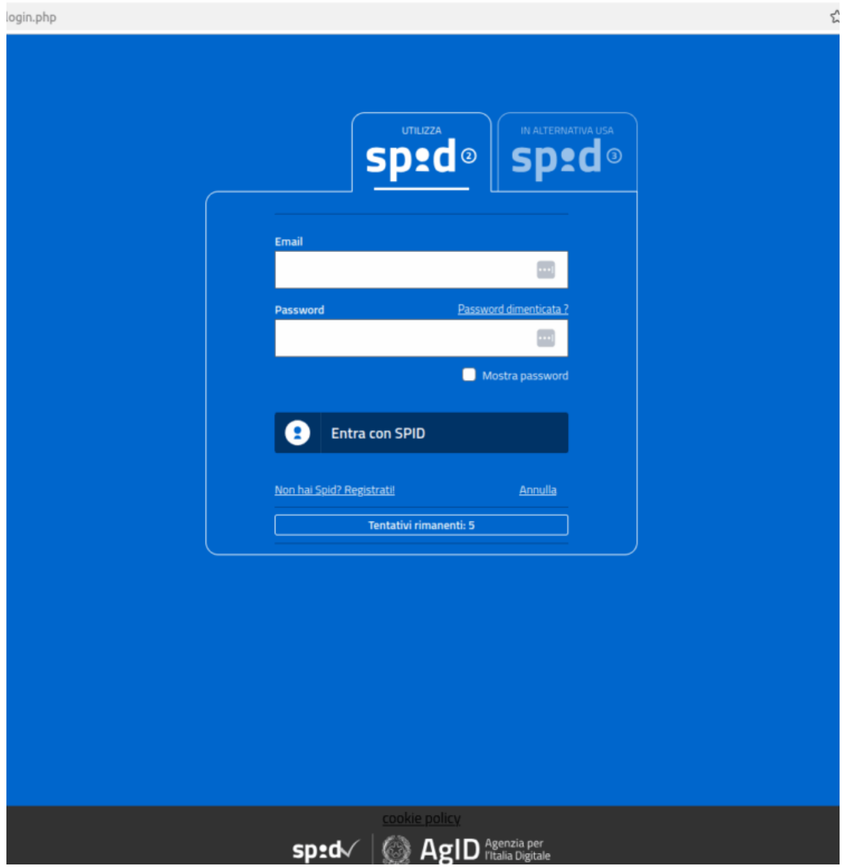
- IT-Wallet applica l'**Identity Binding crittografico**
- Non chiede una foto -> si fida di SPID/CIE
- I dati (Patente, Tessera Sanitaria) vengono recuperati direttamente dalle basi dati dello Stato (Motorizzazione, ANPR) tramite API sicure e firmati digitalmente

Se il sistema è protetto, dove attaccheranno?

- ***Phishing**:* Rubare le credenziali SPID/CIE prima che l'utente attivi il wallet sul proprio telefono.
- ***Malware On-Device**:* Compromissione OS dello smartphone (Root/Jailbreak) per intercettare i dati quando vengono mostrati a schermo.
- ***Verificatori malevoli**:* Finti lettori QR che chiedono più dati del dovuto.

Sito fake / clone

- L'attaccante crea un finto sito di login che copia l'interfaccia dell'Identity Provider.
- L'utente inserisce credenziali sul finto sito. Il server dell'attaccante li prende e li gira *immediatamente* al sito vero del Provider.
- Il sito vero del Provider genera la richiesta di 2nd livello: invia l'SMS o notifica push sul telefono dell'utente.
- L'utente, convinto di stare facendo il login legittimo, approva la notifica o inserisce OTP sul finto sito dell'attaccante.
- L'attaccante intercetta l'OTP, lo gira al sito vero e **ruba il cookie di sessione autenticata**.



Verificatori malevoli

- Un finto addetto alla sicurezza all'ingresso di un locale o un finto sito web per sbloccare un servizio online, mostra un QR Code da inquadrare con il Wallet.
- Il QR Code contiene una richiesta di dati. Invece di chiedere solo l'attributo "*Maggiore di 18 anni*", il verificatore malevolo richiede surrettiziamente **tutti i dati del PID** (*Nome, Cognome, Codice Fiscale, Data di nascita, Luogo di nascita*).
- Sullo schermo del telefono apparirà una richiesta di autorizzazione. Se l'utente è abituato a cliccare "*Accetta*" velocemente senza leggere attentamente l'elenco dei dati richiesti, autorizza il trasferimento.
- L'attaccante riceve così un pacchetto di dati certificati dallo Stato, perfetti per essere riutilizzati per creare truffe finanziarie, aprire conti correnti a nome della vittima o fare furti d'identità mirati.

Controlli Tecnici

PAD (Anti-spoofing) e IAD (Anti-injection) combinati con verifica NFC.

Controlli Ambientali

Monitoraggio della sessione e sicurezza del device per prevenire root/emulazione.

Processi & Org

Fallback manuale per casi sospetti e formazione continua degli operatori.

Come mitigare il rischio nel remote identity proofing

ENISA propone un approccio **multi-layer**

Ma nessun controllo da solo è sufficiente.

Controlli tecnici

Servono a verificare che la persona e il documento siano veri, e presenti sul momento.

• **PAD (anti-spoofing):** Verifica delle azioni: fare un occhiolino, sorridere o girare la testa per dimostrare che sei una persona in carne e ossa davanti alla telecamera, e non una foto stampata.

• **IAD (anti-injection):** Impedire di aggirare la webcam inserendo un flusso video falso direttamente nel codice del dispositivo.

• **Verifica documento (OCR, NFC):** Controlla l'autenticità del documento d'identità.

- L'OCR legge il testo della tua carta d'identità per compilarla automaticamente,
- L'NFC funziona come i pagamenti contactless del telefono, legge il chip invisibile dentro il passaporto o la carta d'identità elettronica per verificare i dati originali firmati dallo Stato.

Controlli ambientali

Servono a garantire che l'ambiente digitale e il canale di comunicazione siano sicuri.

- **Sicurezza del device:** Controlla che il telefono o il computer usato non siano infetti.
- **Protezione della sessione:** Garantisce che nessuno si inserisca nella comunicazione tra te e il server.
- **Controllo canale video:** Verifica la qualità e l'integrità del video. Se la connessione salta continuamente o l'immagine è troppo sgranata, il sistema blocca la procedura perché la scarsa qualità potrebbe nascondere un tentativo di truffa.

Controlli procedurali

Riguardano le regole e i passaggi da seguire durante la verifica.

- **Step aggiuntivi per casi sospetti:** Misure extra se qualcosa non quadra. Se il sistema nota che la faccia somiglia a quella sul documento ma ci sono piccoli dubbi, chiede un secondo documento o di fare un'azione imprevista.
- **Fallback manuale:** L'intervento umano quando l'algoritmo fallisce.
- **Gestione del rischio:** Decidere il livello di controllo in base a cosa si sta proteggendo. Per aprire un conto corrente con un saldo da milioni di euro si useranno controlli molto più severi e rigidi rispetto a quelli richiesti per attivare una tessera punti del supermercato.

Controlli organizzativi

Riguardano la gestione interna dell'azienda che effettua la verifica.

- **Audit:** Controlli periodici sul funzionamento del sistema.
- **Logging:** Registrazione di tutto ciò che accade. Il sistema tiene una scatola nera che registra l'ora esatta di ogni tentativo di accesso, quale operatore ha approvato la pratica e quali controlli automatici sono passati, utile in caso di future indagini per frode.
- **Formazione operatori:** Addestrare il personale umano.Gli operatori fanno corsi regolari per imparare a riconoscere i nuovi tipi di documenti falsi o le tecniche di truffa create con l'intelligenza artificiale.

AGID | Agenzia per l'Italia Digitale

Grazie per l'attenzione

Gianni Amato
CERT-AGID

Funzionario Area Vigilanza e Sicurezza, AGID