«Public Sandbox Trust Infrastructure» Factsheet

Italiano

Vi preghiamo di leggere attentamente il presente documento prima di compilare e inviare il modulo di iscrizione per la partecipazione alla «Public Sandbox Trust Infrastructure».

1. Cos'è la «Public Sandbox Trust Infrastructure»?

Generalmente il termine «sandbox» descrive un ambiente di prova di un progetto pilota, in cui si possono testare applicazioni e metodi tecnologici nuovi. Lo scopo della «Public Sandbox Trust Infrastructure» è sperimentare componenti e processi tecnici non soltanto all'interno dell'Amministrazione federale, ma anche nella collaborazione con i futuri partecipanti a questo ecosistema, appartenenti al settore pubblico o a quello economico. L'opportunità partecipativa offerta dall'allestimento di una sandbox risponde a un grande bisogno del pubblico specializzato, che segue gli sviluppi relativi ai mezzi d'identificazione elettronici (Id-e) e all'infrastruttura di fiducia su cui si fondano.

2. Quali obiettivi persegue la «Public Sandbox Trust Infrastructure»?

- Raccogliere esperienze sotto il profilo tecnico (funzionalità, scalabilità, sicurezza, esercizio ecc.)
- Raccogliere esperienze sotto il profilo organizzativo (onboarding, supporto ecc.)
- Raccogliere esperienze sotto il profilo specialistico (testare casi di applicazione, garantire l'interoperabilità tra le varie organizzazioni, l'usabilità ecc.)
- Acquisire nuovi attori che partecipino all'ecosistema

3. Quali sono i ruoli all'interno della «Public Sandbox Trust Infrastructure» e chi li svolge?

Ruolo	Descrizione	Chi può svolgere il ruolo?
Emittente	Emette mezzi di autenticazione elettronici. Può revocare i mezzi di autenticazione elettronici che ha emesso.	Attori autorizzati dall'UFIT.
Titolare	Richiede un mezzo di autenticazione elettronico e lo ottiene da un emittente. Presenta il mezzo di autenticazione elettronico al verificatore.	Nessuna restrizione tecnica. Chiunque possieda un wallet e sia in grado di creare una connessione con un emittente, ovvero tutti coloro che ricevono un invito da un emittente.
Verifikatorin	Può richiedere la presentazione di un mezzo di autenticazione elettronico al suo titolare e verificarlo sul piano crittografico.	Nessuna restrizione tecnica. Il titolare può decidere a chi trasmettere il mezzo di autenticazione elettronica per sottoporlo a verifica. L'UFIT è autorizzato a inserire i verificatori nel registro di base.
Basisregister	Registro centrale di chiavi pubbliche e identificativi appartenenti agli attori ammessi. **Importante: sul registro di base non vengono salvati mezzi di autenticazione elettronici né informazioni sulla loro emissione.**	È gestito dall'UFIT. I dati figuranti nel registro di base sono accessibili al pubblico. Agli emittenti sono concessi diritti di scrittura limitati.
Vertrauensregister	Nella «Public Sandbox Trust Infrastructure» non si mette a disposizione alcun registro di fiducia.	

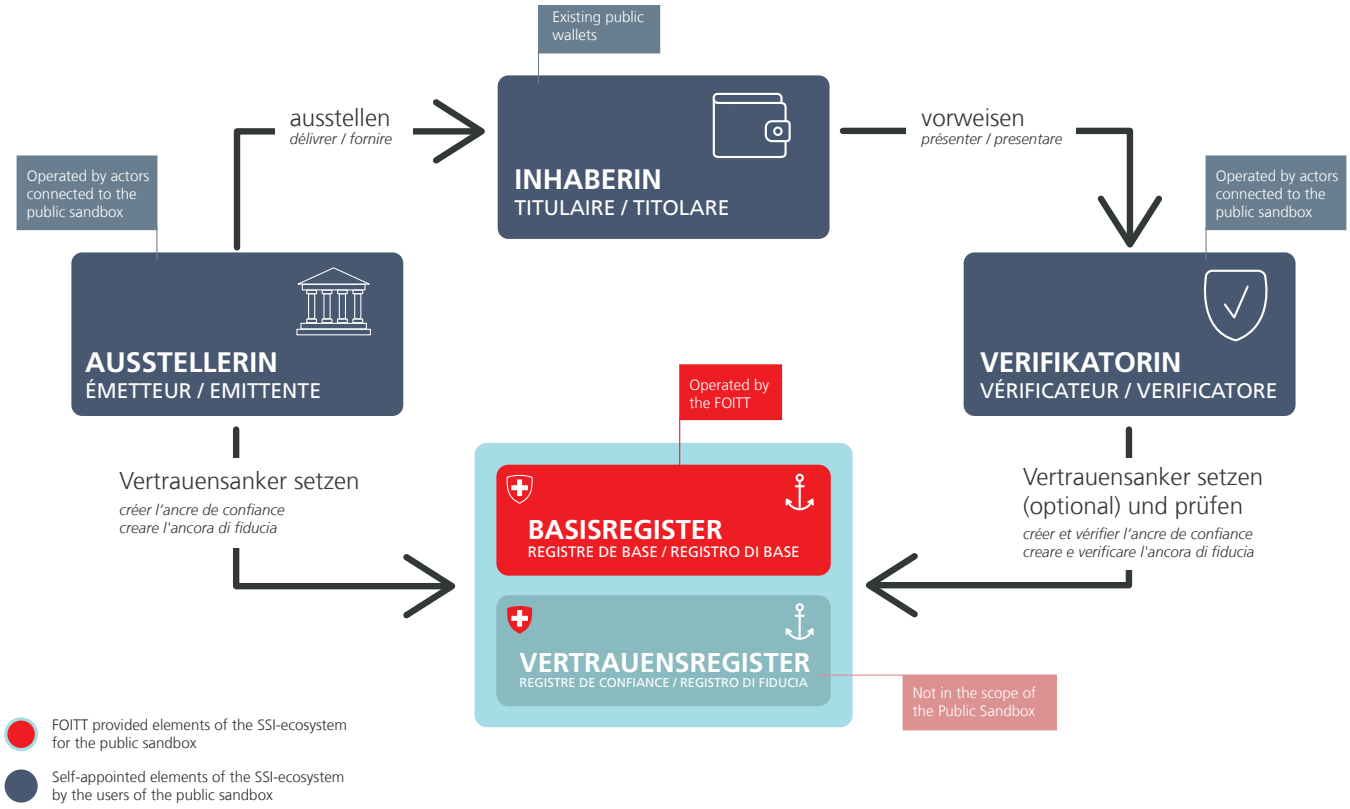

Figura relativa al funzionamento della sandbox

4. Chi elabora i dati all'interno della «Public Sandbox Trust Infrastructure» e di quali dati si tratta?

Ruolo	**Trattametno dei dati**
Emittente	Dati figuranti nel registro di base: • il proprio identificativo; • la propria chiave pubblica; • lo schema di definizione/il tipo del mezzo di autenticazione elettronico emesso (descrizione dei campi di dati che compongono un mezzo di autenticazione elettronico). Dati in relazione al titolare: • l'insieme degli attributi che costituiscono il contenuto del mezzo di autenticazione elettronico. In molti casi si tratta di dati personali che vengono trasferiti direttamente tra emittente e titolare. Dati relativi a una soluzione di revoca (gestita dall'emittente): • informazioni concernenti la revoca di un mezzo di autenticazione elettronico.
Titolare	Dati in relazione all'emittente: • l'insieme degli attributi che costituiscono il contenuto del mezzo di autenticazione elettronico. In molti casi si tratta di dati personali che vengono protetti da una crittografia end-to-end e trasferiti direttamente tra emittente e titolare. Dati in relazione al verificatore: • l'insieme degli attributi trasmessi che costituiscono il contenuto del mezzo di autenticazione elettronico. In molti casi si tratta di dati personali che vengono protetti da una crittografia end-to-end e trasferiti direttamente tra titolare e verificatore.

Verificatore	Dati figuranti nel registro di base (facoltativo): • il proprio identificativo; • la propria chiave pubblica. Dati in relazione al titolare: • gli attributi trasmessi dal titolare che costituiscono il contenuto del mezzo di autenticazione. In molti casi si tratta di dati personali che vengono protetti da una crittografia end-to-end e trasferiti direttamente dal titolare al verificatore.
Registro di base	Dati relativi alla componente tecnica (gestita dall'UFIT): • gli identificativi degli emittenti connessi (requisito obbligatorio) e dei verificatori connessi (requisito facoltativo); • le chiavi pubbliche degli emittenti connessi (requisito obbligatorio) e dei verificatori connessi (requisito facoltativo); • le comunicazioni che spiegano come reperire le informazioni relative alla revoca di un mezzo di autenticazione elettronico (rimando al sistema dell'emittente); • lo schema delle credenziali impiegato dall'emittente e integrato nel registro di base; • la definizione del mezzo di autenticazione elettronico, ovvero l'autorizzazione secondo cui emettere mezzi di autenticazione conformemente a uno schema prestabilito attribuita a ciascun emittente.
Collezione di dati dell'UFIT (gestione dei partecipanti connessi al sistema)	Quale amministratore della sandbox, competono esclusivamente all'UFIT la registrazione manuale e il trattamento dei dati indicati nel modulo di iscrizione. Informazioni estrapolate dal modulo di iscrizione: • informazioni relative all'organizzazione; • persone di contatto; • informazioni sul business case; • integratori tecnici; • informazioni tecniche (identificativi e chiavi pubbliche); • dichiarazione di consenso in merito alle condizioni di utilizzo della sandbox. L'archiviazione avviene in ambiente protetto. L'accesso all'infrastruttura di fiducia Id-e è consentito soltanto alle persone autorizzate del team DevOps.