# «Public Sandbox Trust Infrastructure» Factsheet

## Deutsch

*Bitte lesen Sie dieses Dokument sorgfältig durch, bevor Sie das «Anmeldeformular für Interessierte zur Teilnahme an der «Public Sandbox Trust Infrastructure» ausfüllen und zurücksenden.*

### 1. Was ist die «Public Sandbox Trust Infrastructure»?

Im Allgemeinen ist eine Sandbox ein isolierter Testbereich/Pilotbetrieb, in dem neue Applikationen und technologische Ansätze erprobt werden können. Bei der «Public Sandbox Trust Infrastructure» geht es darum, technische Komponenten und Prozesse nicht nur innerhalb der Bundesverwaltung, sondern auch mit zukünftigen Ökosystem-Teilnehmerinnen aus öffentlicher Hand und der Wirtschaft zu testen. Die Partizipationsmöglichkeit mittels Sandbox ist ein grosses Bedürfnis der Fach-Öffentlichkeit, welche den Prozess rund um die E-ID und die darunterliegende Vertrauensinfrastruktur verfolgt.

### 2. Welche Ziele werden mit der «Public Sandbox Trust Infrastructure» verfolgt?

- Technische Erfahrungen sammeln (Funktionalitäten, Skalierung, Sicherheit, Betrieb etc.)
- Organisatorische Erfahrungen sammeln (Onboarding, Support etc.)
- Fachliche Erfahrungen sammeln (Erprobung von Anwendungsfällen, organisationsübergreifende Interoperabilität, Usability etc.).
- Weitere Akteure für Ökosystem gewinnen

### 3. Welche Rollen werden in der «Public Sandbox Trust Infrastructure» von wem wahrgenommen?

| Rolle | Beschreibung | Wer kann Rolle ausfüllen? |
|---|---|---|
| Ausstellerin | Eine Ausstellerin stellt elektronische Nachweise aus.<br><br>Eine Ausstellerin kann die von ihr ausgestellten elektronischen Nachweise revozieren. | Vom BIT zugelassene Akteure. |
| Inhaberin | Eine Inhaberin beantragt und erhält einen elektronischen Nachweis von einer Ausstellerin. Sie weist einen elektronischen Nachweis der Verifikatorin vor. | Keine technische Restriktion. Wer eine Wallet besitzt und eine Verbindung zu einer Ausstellerin herstellen kann. Mit anderen Worten: alle, die von einer Ausstellerin eingeladen werden. |
| Verifikatorin | Eine Verifikatorin kann sich von einer Inhaberin einen elektronischen Nachweis vorweisen lassen und diesen kryptographisch überprüfen. | Keine technische Restriktion. Eine Inhaberin kann entscheiden, wem sie ein Nachweis zur Verifikation übermittelt.<br>Das BIT kann Verifikatorinnen auf dem Basisregister zulassen. |
| Basisregister | Zentrales Verzeichnis öffentlicher Schlüssel und Identifikatoren der zugelassenen Akteure.<br><br>**Wichtig: Auf dem Basisregister werden keine digitalen Nachweise und auch keine Informationen zu deren Ausstellung gespeichert.** | Wird vom BIT betrieben.<br><br>Auf dem Register abgebildete Daten sind öffentlich abrufbar. Ausstellerinnen werden eingeschränkte Schreiberechte gewährt. |
| Vertrauensregister | In der «Public Sandbox Trust Infrastructure» wird kein Vertrauensregister zur Verfügung gestellt. | |

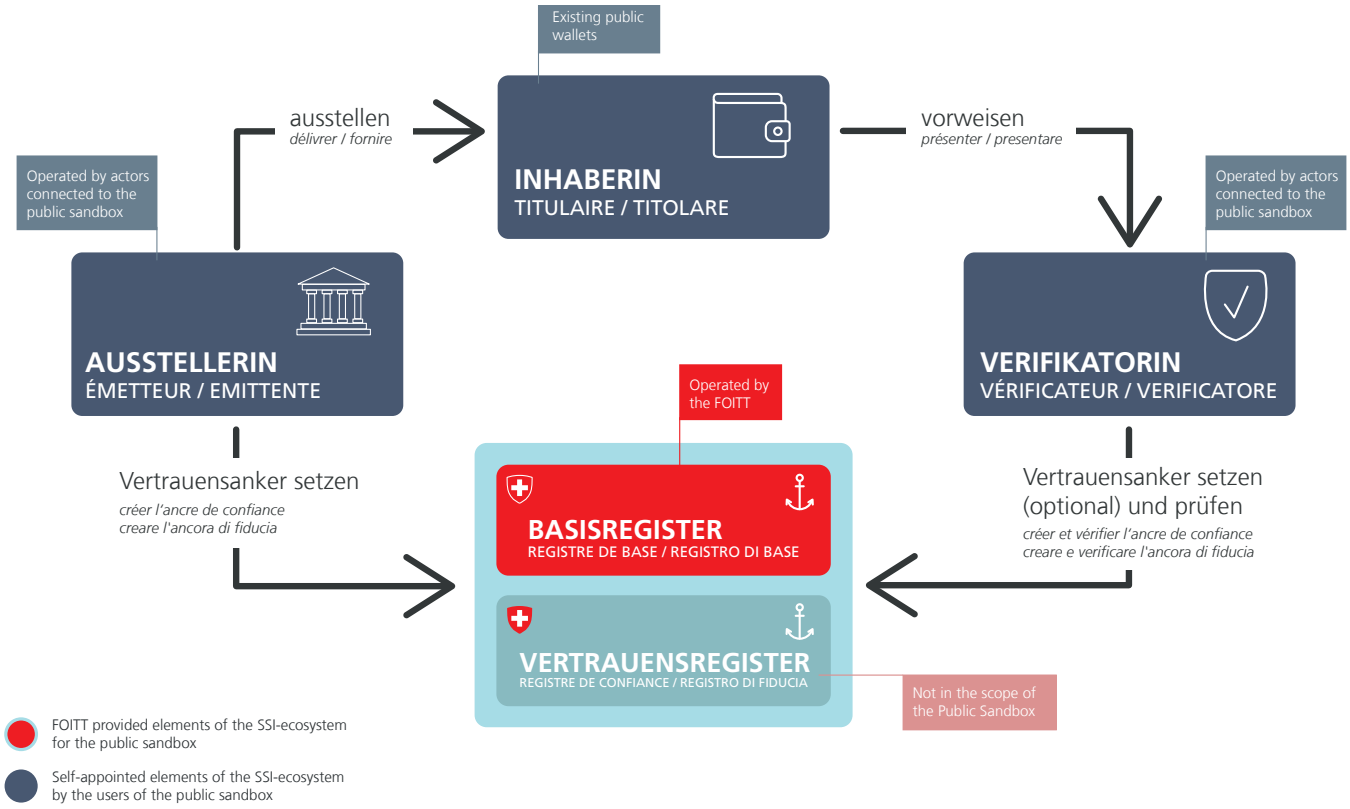


*Abbildung Umfang «Public Sandbox Trust Infrastructure»*

## 4. Von wem werden welche Daten innerhalb der «Public Sandbox Trust Infrastructure» bearbeitet?

| Rolle | Datenbearbeitung |
|---|---|
| **Ausstellerin** | Auf dem Basisregister abgebildet<br>• Eigener Identifikator<br>• Eigener öffentlicher Schlüssel<br>• Schema-Definition der ausgestellten Nachweise (Beschreibung, aus welchen Datenfeldern ein digitaler Nachweise besteht).<br><br>Gegenüber Inhaberin<br>• Sämtliche Attribute, die Inhalt des elektronischen Nachweises sind. Diese Daten sind in vielen Fällen personenbezogen; sie werden direkt zwischen Ausstellerin und Inhaberin übertragen.<br><br>Auf einer Lösung zur Revokation (Betrieben durch die Ausstellerin)<br>• Information, ob ein Nachweis revoziert wurde. |
| **Inhaberin** | Von der Ausstellerin<br>• Sämtliche Attribute, die Inhalt des elektronischen Nachweises sind. Diese Daten sind in vielen Fällen personenbezogen; sie werden end-zu-end-verschlüsselt und direkt zwischen Ausstellerin und Inhaberin übertragen.<br><br>Gegenüber Verifikatorin<br>• Sämtliche übermittelten Attribute, die Inhalt des elektronischen Nachweises sind. Diese Daten sind in vielen Fällen personenbezogen; sie werden end-zu-end-verschlüsselt und direkt zwischen Inhaberin und Verifikatorin übertragen. |

| | |
|---|---|
| **Verifikatorin** | Auf dem Basisregister (optional)<br>• Eigener Identifikator<br>• Eigener öffentlicher Schlüssel<br><br>Gegenüber Inhaberin<br>• Von der Inhaberin übermittelte Attribute, die Inhalt des elektronischen Nachweises sind. Diese Daten sind in vielen Fällen personenbezogen; sie werden end-zu-end-verschlüsselt und direkt von der Inhaberin an die Verifikatorin übertragen. |
| **Basisregister** | Technische Komponente (durch das BIT betrieben)<br>• Identifikatoren von angeschlossenen Ausstellerinnen (muss) und Verifikatorinnen (optional)<br>• Öffentliche Schlüssel von angeschlossenen Ausstellerinnen (muss) und Verifikatorinnen (optional)<br>• Information, wo die Information zur Revokation eines Nachweises abgerufen werden kann (Verweis auf System von Ausstellerin)<br>• Von der Ausstellerin eingesetzte resp. auf dem Basisregister erfasste Credential-Schemas<br>• Nachweis Definition: Autorisierung pro Ausstellerin, Nachweise gemäss einem Schema auszustellen. |
| **Datensammlung BIT** (Verwaltung der am System angeschlossene Teilnehmenden) | Händische Erfassung und Bearbeitung der Daten auf dem Anmeldeformular, nur vom BIT als verwaltende Einheit der Sandbox einsehbar.<br><br>In diesem Formular erhobene Informationen zu:<br>• Informationen zu Organisation,<br>• Kontaktpersonen,<br>• Information zum Business Case,<br>• technische Integratorin<br>• technische Informationen (Identifikator und öffentlicher Schlüssel)<br>• Einverständnis mit den Nutzungsbedingungen der Sandbox<br><br>Ablage in geschütztem Bereich. Zugriff nur durch berechtigte Personen im DevOps-Team der E-ID Vertrauensinfrastruktur. |