«Public Sandbox Trust Infrastructure» Factsheet

Français

Nous vous prions de lire attentivement le présent document avant de renvoyer le formulaire d'inscription à la sandbox publique pour l'infrastructure de confiance dûment rempli.

1. Qu'est-ce que la «Public Sandbox Trust Infrastructure»?

De manière générale, une sandbox constitue une zone de test ou une phase d'exploitation pilote isolée permettant d'expérimenter de nouvelles applications et approches technologiques. Dans le cas de la sandbox publique pour l'infrastructure de confiance, dite «Public Sandbox Trust Infrastructure», il s'agit de tester des composants et des processus techniques non seulement au sein de l'administration fédérale, mais aussi avec les futurs participants à l'écosystème, que ces derniers soient issus des pouvoirs publics ou des milieux économiques. La sandbox répond à un besoin important du public spécialisé, car elle lui offre la possibilité de participer au processus relatif à l'e-ID et à l'infrastructure de confiance sur laquelle elle repose.

2. Objectifs visés

- Acquérir de l'expérience technique (fonctionnalités, ajustement, sécurité, exploitation, etc.)
- Acquérir de l'expérience en matière d'organisation (intégration, assistance, etc.)
- Acquérir de l'expérience dans le domaine des moyens de preuve électroniques (test de cas d'application, interopérabilité interorganisationnelle, convivialité, etc.)
- Convaincre d'autres acteurs de participer à l'écosystème

3. Rôles des différents acteurs

Rôle	Description	Qui peut jouer ce rôle?
Émetteur	Un émetteur délivre des moyens de preuve électroniques. Il a également le droit de révoquer les moyens de preuve électroniques qu'il a délivrés.	Les acteurs autorisés par l'OFIT.
Titulaire	Après en avoir fait la demande auprès d'un émetteur, un titulaire obtient un moyen de preuve électronique, qu'il peut présenter à un vérificateur.	Aucune restriction technique. Toute personne disposant d'un portefeuille numérique et pouvant établir une connexion avec un émetteur. Autrement dit, toute personne à qui un émetteur a envoyé une invitation.
Vérificateur	Un vérificateur peut demander à un titulaire de lui présenter un moyen de preuve électronique, qu'il contrôle de manière cryptographique.	Aucune restriction technique. Le titulaire peut choisir à quel vérificateur il transmet un moyen de preuve pour vérification. L'OFIT peut accorder aux vérificateurs l'accès au registre de base.
Basisregister	Il s'agit du répertoire central des clés publiques et des identifiants des acteurs autorisés. **Veuillez noter que le registre de base ne contient pas de moyens de preuve électroniques ni d'informations relatives à leur émission.**	Exploité par l'OFIT. Les données figurant dans le registre de base sont accessibles au public. Les émetteurs disposent de droits d'écriture restreints.
Registre de confiance	Le champ d'application de la sandbox publique pour l'infrastructure de confiance n'inclut pas de registre de confiance.	

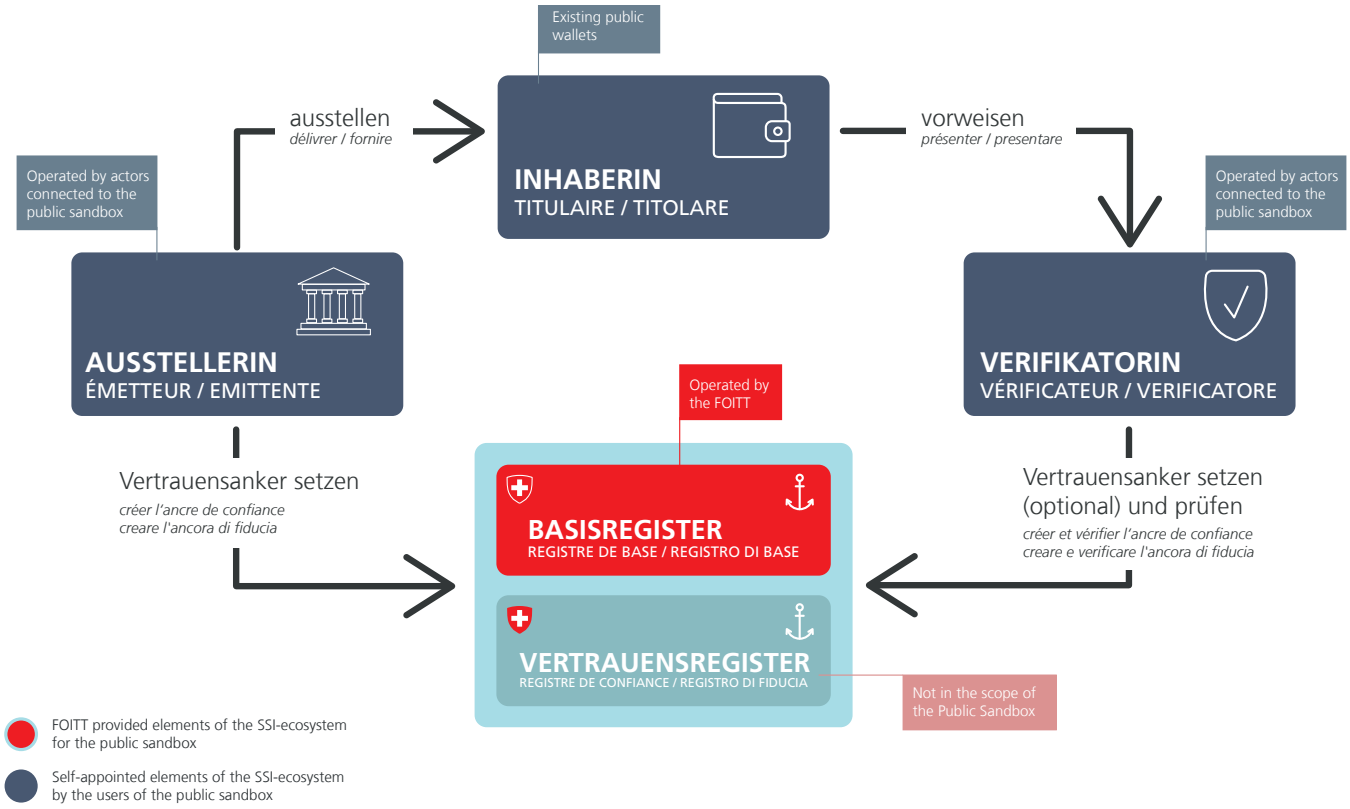

Schéma du champ d'application de la sandbox

4. Traitement des données par les différents acteurs

Rôle	Traitement des données
Émetteur	Figurant dans le registre de base • Identifiant personnel • Clé publique personnelle • Définition du schéma (décrivant les champs de données constituant le moyen de preuve électronique) Par rapport au titulaire • Ensemble des attributs qui constituent le contenu du moyen de preuve électronique. Dans de nombreux cas, ces données sont liées à la personne. L'émetteur les transmet directement au titulaire, et réciproquement. Concernant une solution de révocation (exploitée par l'émetteur) • Information relative à la révocation d'un moyen de preuve.
Titulaire	Par l'émetteur • Ensemble des attributs qui constituent le contenu du moyen de preuve électronique. Dans de nombreux cas, ces données sont liées à la personne. Elles sont cryptées de bout en bout. L'émetteur les transmet directement au titulaire, et réciproquement. Par rapport au vérificateur • Ensemble des attributs transférés constituant le contenu du moyen de preuve électronique. Dans de nombreux cas, ces données sont liées à la personne. Elles sont cryptées de bout en bout. Le titulaire les transmet directement au vérificateur, et réciproquement.

Vérificateur	Figurant dans le registre de base (facultatif) • Identifiant personnel • Clé publique personnelle Par rapport au titulaire • Attributs transférés par le titulaire constituant le contenu du moyen de preuve électronique. Dans de nombreux cas, ces données sont liées à la personne. Elles sont cryptées de bout en bout. Le titulaire les transmet directement au vérificateur, et réciproquement.
Registre de base	Composants techniques (exploités par l'OFIT) • Identifiants des émetteurs connectés (obligatoire) et des vérificateurs (facultatif) • Clés publiques des émetteurs connectés (obligatoire) et des vérificateurs (facultatif) • Indication de l'endroit où se trouvent les informations relatives à la révocation d'un moyen de preuve (renvoi au système de l'émetteur) • Schémas des identifiants utilisés par l'émetteur ou saisis dans le registre de base • Définition du moyen de preuve: autorisation pour chaque émetteur d'émettre des moyen de preuve selon un schéma
Collecte de données par l'OFIT (administration des participants connectés au système)	Saisie et traitement manuels des données figurant dans le formulaire d'inscription. Celles-ci sont consultables uniquement par l'OFIT en sa qualité d'administrateur de la sandbox. Les informations figurant dans le formulaire concernent: • l'organisation; • les interlocuteurs; • le business case • l'intégrateur technique; • des thèmes techniques (identifiant et clé publique); • l'acceptation des conditions d'utilisation de la sandbox. Stockage dans un environnement sécurisé accessible uniquement par les personnes autorisées au sein de l'équipe DevOps chargée de l'infrastructure de confiance e-ID.