Février 2020

Intégration technique de l'agent FSI

Conditions cadres du point de vue du Relying Party

Objet du présent document

L'agent FSI met en œuvre techniquement la fédération des identités. Le présent document explique les différentes options d'exploitation de l'agent FSI et précise les conditions cadres qu'un Relying Party doit prendre en compte lors de l'intégration de l'agent FSI.

Définitions

Identity Provider (IdP) : Service électronique qui gère les identités numériques des utilisateurs et vérifie les identités des utilisateurs (l'utilisateur est authentifié), p. ex. par moyen d'un mot de passe ou d'une carte à puce ou similaires.

Authentification, authentifier : Processus par lequel un utilisateur voit son identité confirmée par un IdP, souvent appelé « Login » sur des sites web. (Le même processus du point de vue du IdP est appelé *authentification.* Un utilisateur s'authentifie auprès de l'IdP, un IdP authentifie l'utilisateur).

Utilisateur : Personne physique qui s'authentifie auprès d'un IdP.

Ticket de sécurité : Un paquet de données émis par l'IdP, qui confirme l'authentification réussie de l'utilisateur. Le ticket de sécurité contient au minimum un numéro d'identification de l'utilisateur et peut contenir autres données personnelles.

Attributs : Données personnelles de l'utilisateur, que l'IdP fournit avec le ticket de sécurité.

Relying Party (RP) : Un service ou une ressource qui nécessite un utilisateur authentifié. Le RP laisse la tâche de l'authentification à un IdP et s'appuie sur les informations contenues dans le ticket de sécurité.

Situation initial

Les RP modernes sont construits de telle manière qu'ils ne procèdent pas eux-mêmes à l'authentification, mais intègrent un IdP (externe) auquel ils font suffisamment confiance. Un autre but est de faciliter la tâche pour l'utilisateur en lui offrant une sélection d'IdP parmi lesquels il peut choisir et effectuer le login. Idéalement, un utilisateur ne devrait pas effectuer le login séparément auprès du RP et devrait plutôt pouvoir effectuer le login auprès de l'un des IdP disponibles.

Ce principe exige que le RP établisse une position de confiance pour chaque IdP qu'il propose aux utilisateurs comme "option de login" et qu'il puisse interpréter et valider leur ticket de sécurité. Généralement les tickets de sécurités des différents IdP sont structurés différemment, ce qui entraîne des coûts techniques et organisationnels supplémentaires pour les RP, car chaque IdP doit être intégré individuellement.

La solution : Un service intermédiaire prend en charge l'intégration technique et organisationnelle des IdP et se présente au RP comme un IdP. Ce dernier, pour sa part doit intégrer techniquement le RP. Du point de vue du RP, il n'y a qu'un seul IdP, qui agit théoriquement comme un substitut pour un nombre arbitraire d'autres IdP. Cet IdP central est appelé *Agent des identités (Identity Broker)*, la procédure décrite est appelée *fédération des identités (Identity Federation)*.

Base conceptuelle

Cas d'utilisations génériques pour le fédération des identités

Un agent des identités est du point de vue du RP un IdP et couvre les mêmes principaux cas d'utilisations génériques :

(1) *authentification* (Authentication Brokering). L'agent des identités fournit un IdP approprié pour l'authentification auprès du RP.

(2) *identification* (Identity Brokering). Ce cas est moins souvent que l'authentification pure et est utilisé par exemple pour l'enregistrement d'un utilisateur. L'agent des identités fournit un IdP, qui est capable de fournir des attributs de l'utilisateur, c'est-à-dire des données personnelles, en plus d'une confirmation d'authentification.

(3) *requête du statut* (Attribute Brokering). L'Agent des identités fournit un IdP approprié pour la requête (récurrente) d'attribut changeant avec le temps. Ces attributs peuvent être : « a plus de 18 ans » (isOver18) ou « est membre de » (isMemberOf).

Identifiant de l'utilisateur (nameID)

Pour une distinction claire, chaque utilisateur d'un IdP reçoit un numéro, l'*identifiant de l'utilisateur,* techniquement : *nameID*. La nameID est donnée au RP dans le ticket de sécurité. Il en existe deux types différents :

- *persistant* (attribué de manière permanente) : La nameID est toujours le même dans chaque ticket de sécurité que l'IdP émet pour un utilisateur particulier au fil du temps.
- *transitoire* (attribué temporairement) : La nameID change avec chaque ticket de sécurité que l'IdP émet pour un utilisateur particulier.

Persistant est le moyen d'identification courant et permet à un RP de reconnaître l'utilisateur lors d'inscriptions répétées et de conserver un historique des actions de l'utilisateur, par exemple sous la forme d'un compte utilisateur.

Transitoire est une technique appropriée pour mettre en œuvre l'anonymat des utilisateurs. Les RP ne peuvent pas assigner les inscriptions répétées à un utilisateur et ni un profil ni un historique des actions de l'utilisateur ne peuvent être créés.

Agrégation et Identity Linking

Normalement, différents IdP sont affiliés à l'agent des identités, certains d'entre eux supportent exclusivement le cas d'utilisation de l'authentification, d'autres supportent supplémentairement le cas d'utilisation de l'identification, c'est-à-dire qu'ils disposent des données personnelles de l'utilisateur.

Agrégation

Agrégation fait référence à la fusion d'attributs de différents IdP. Exemple: IdP A contient des données personnelles telle que le nom, le prénom et autres. IdP B est lié à un registre des personnes qui contient entre autres le lieu d'origine des personnes. Un RP qui a besoin d'une confirmation d'authentification avec nom, prénom et lieu d'origine de l'utilisateur a deux possibilité d'agréger les données :

a) *contrôle par le RP :* Le RP demande dans une première requête auprès de l'agent des identités le nom et le prénom de l'utilisateur même qu'une confirmation d'authentification. Dans une deuxième requête le lieu d'origine est demandé. Il s'agit donc de deux requêtes successives auprès de l'agent des identités. Les résultats sont ensuite fusionnés par le RP.

b) *contrôle par le Broker :* Le RP demande dans une seule requête le nom, le prénom et le lieu d'origine auprès de l'agent des identités. Celui-ci coordonne à l'interne deux requêtes distinctes, une auprès du IdP A et une auprès du IdP B. Ensuite, il fusionne les résultat e les fournit au RP.

Identity Linking

Afin de fusionner les attributs de différents IdP, l'agent des identités doit savoir de chaque utilisateur, s'il est enregistré auprès d'un IdP affilié et si oui, sous quelle nameID. Seulement de cette manière il est possible pour l'agent des identités de demander avec une requête les attributs correspondants pour l'utilisateur auprès des IdP. Le principe selon lequel l'agent des identités connaît les différentes nameID est appelé *identity linking*.

Sans identity linking il est tâche du RP de fusionner les différentes nameID d'un utilisateur et de faire des requêtes individuelles auprès de l'agent des identités. Cela nécessite soit une coopération et échange de données entre le RP et tous les IdP, ce qui dans la plupart des cas pose des problèmes de protection des données, soit une coopération active de la part de l'utilisateur, de sorte qu'il communique ses différentes nameID à l'agent des identités dans le cadres d'un processus de comparaison spécial. Ce dernier est un processus complexe et aussi un défi en terme de l'ergonomie, car il est difficile à expliquer à un utilisateur.

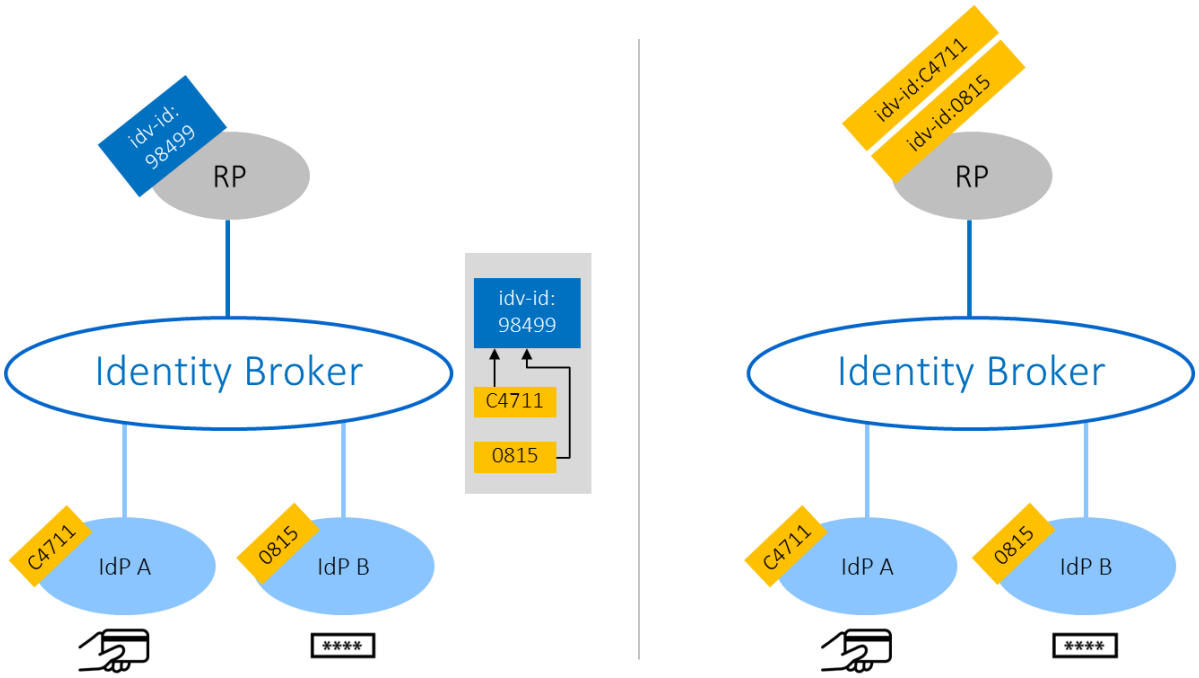

Illustration : Avec (à gauche) et sans (à droite) identity linking

Attribute linking et hamornisation des attributs

En général, chaque IdP utilise sa propre dénomination pour les attributs. Par exemple, l'attribut pour le prénom peut être dénommé auprès du IdP A *name* et auprès du IdP B *firstName.* Si un RP demande l'attribut prénom et qu'il aurait choisi le IdP B pour celui-ci, l'agent des identités demandera l'attribut *firstName* auprès de l'IdP. L'agent des identités doit donc connaître la dénomination des attributs de chaque IdP et transformer les attributs demandés par le RP selon cette nomenclature. Cette propriété de l'agent des identités est appelée *attribute linking*.

L'harmonisation des attributs signifie que tous les IdP dénomment un attribut particulier de la même manière et que donc l'attribute linking n'est plus nécessaire. Par exemple l'attribut pour le prénom pourrait être dénommé par tous les IdP *name*. L'harmonisation des attributs nécessite une unification organisationnelle, qui peut être une option pour des groupes d'IdP dans un domaine d'utilisateur ou un secteur d'activité particulier.

Méthodes d'agrégation

Il existe plusieurs méthodes qui permettent à un agent des identités d'agréger les attributs des IdPs.

(1) Requête à un IdP : L'agent des identités agit comme un Discovery Service (quel IdP gère quels attributs ?). Une agrégation n'est pas nécessaire car les attributs proviennent d'un seul IdP.

(2) Requête auprès de plusieurs IdP avec une nameID harmonisée : La méthode convient aux groupes d'IdP et aux domaines d'utilisateurs qui sont soumis à un ensemble de règles communes et utilisent la même nameID pour tous les utilisateurs, par exemple le numéro d'assurance sociale AVSN13 ou le numéro SuisseID.

(3) Requête auprès de plusieurs IdP sans nameID harmonisée : La méthode la plus complexe de toutes, car elle nécessite à la fois un identity linking et un attribute linking.

Proxying

Relaying selon la norme eCH 0168 signifie que l'agent des identités transmet le ticket de sécurité original du IdP au RP sans autres transformations du nom d'attributs et de la nameID.

Proxying selon la norme eCH 0168 signifie que l'agent des identités utilise le ticket de sécurité du IdP comme base pour son propre ticket de sécurité et qu'il transmet celui-ci au RP.

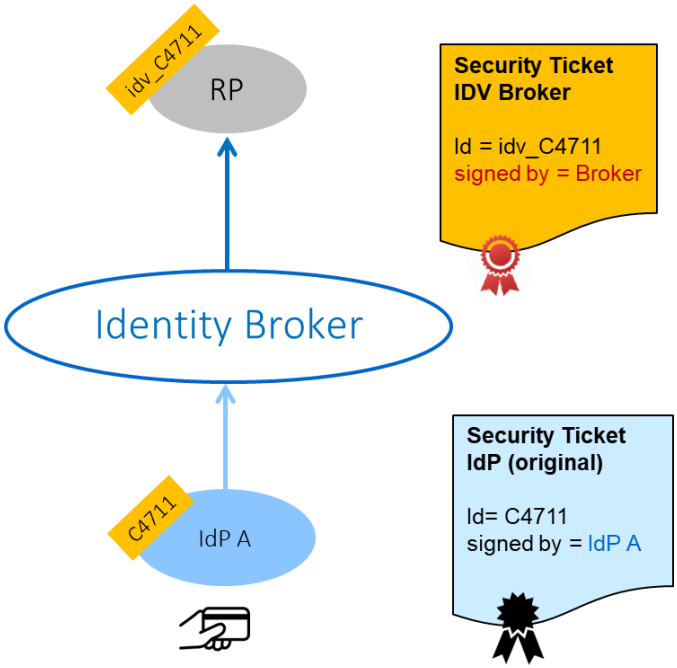

Illustration : Proxying

L’agent FSI (IDV Broker)

L'agent FSI est un agent des identités et met en œuvre le principe de la fédération des identités. Différents IdP et RP sont affiliés à l'agent FSI. Ceux-ci utilisent une interface standardisée pour la communication depuis et vers l’agent FSI.

L’agent FSI ne procède pas lui-même à l'authentification, mais délègue cette tâche à l'un des IdP (A ou B dans l'illustration). Dès que l'utilisateur veut se loger au RP, l’agent FSI intervient et propose à l’utilisateur la sélection des IdPs affiliés. L'utilisateur choisit un IdP, par exemple A, et effectue l'authentification avec ce IdP.

La procédure décrite suppose que l'utilisateur est enregistré auprès de minimum un des IdP affilié et peut y effectuer une authentification. Si cette condition n'est pas remplie, l'utilisateur doit s'enregistrer et s'authentifier auprès du RP de manière conventionnelle.

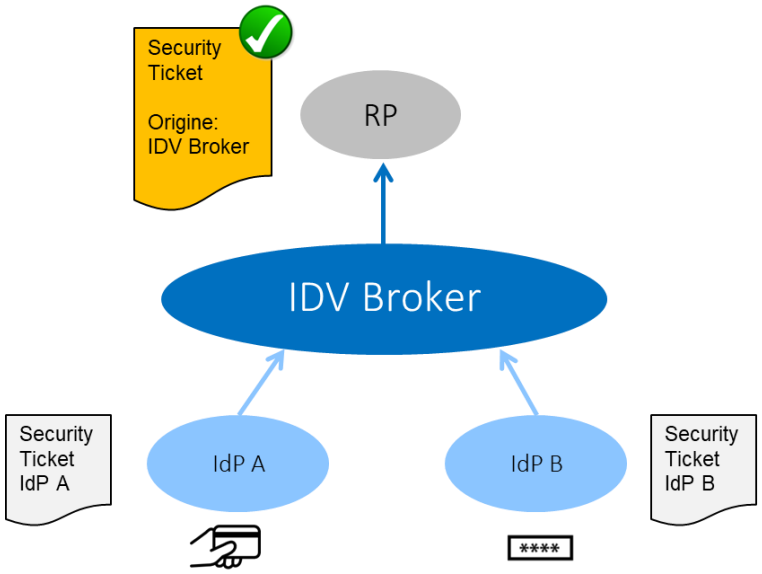

Illustration : fédération des identités avec l’agent FSI

Mode de fonctionnement de l’agent FSI

L’agent FSI soutient le mode de fonctionnement du *Proxying* selon la norme eCH 0168 avec des extensions. Concrètement cela veut dire :

- L'agent FSI permet l'authentification respectivement l'obtention d'attributs à partir d'un des IdP affiliés (voir la méthode d'agrégation 1 à la page 3).
- L’agent FSI utilise le ticket de sécurité de l'IdP auquel l'utilisateur s'est authentifié et crée un nouveau ticket de sécurité à son propre nom et signé par lui.
- L'agent FSI peut être configuré de manière à ce que la *nameID* soit par la fois persistant ou transitoire. Persistent aide le RP à reconnaître l'utilisateur lors d’inscriptions répétées en tel que même client, tandis que transitoire rend l'anonymat effectivement du client.
- Il ne peut pas être exclu que deux personnes différentes auprès des IdP différents puissent avoir la même nameID. L’agent FSI garantit l'unicité de la nameID auprès de tous les IdP, c'est-à-dire qu'il crée sa propre nameID et la transfère au RP par le moyen du ticket de sécurité.
- L'agent FSI met en œuvre l'harmonisation des attributs en les transformant selon des règles prédéfinies. La dénomination des attributs que l'IdP utilise à l’interne est cachée et n'est pas pertinente. Par exemple, l'agent FSI donne toujours au RP l'attribut *firstName* pour les prénoms, même si l'IdP utilise un nom différent pour cet attribut.
- Le RP fait confiance à l’agent FSI et peut renoncer à un contrôle séparé du ticket de sécurité original du IdP.

Il existe une exigence supplémentaire :

- L’agent FSI peut être configuré de manière que le ticket de sécurité originale de l’IdP soit joint à celui du Broker. Cela permet au RP de vérifier l’origine et l’authenticité des données confirmées par l’IdP.

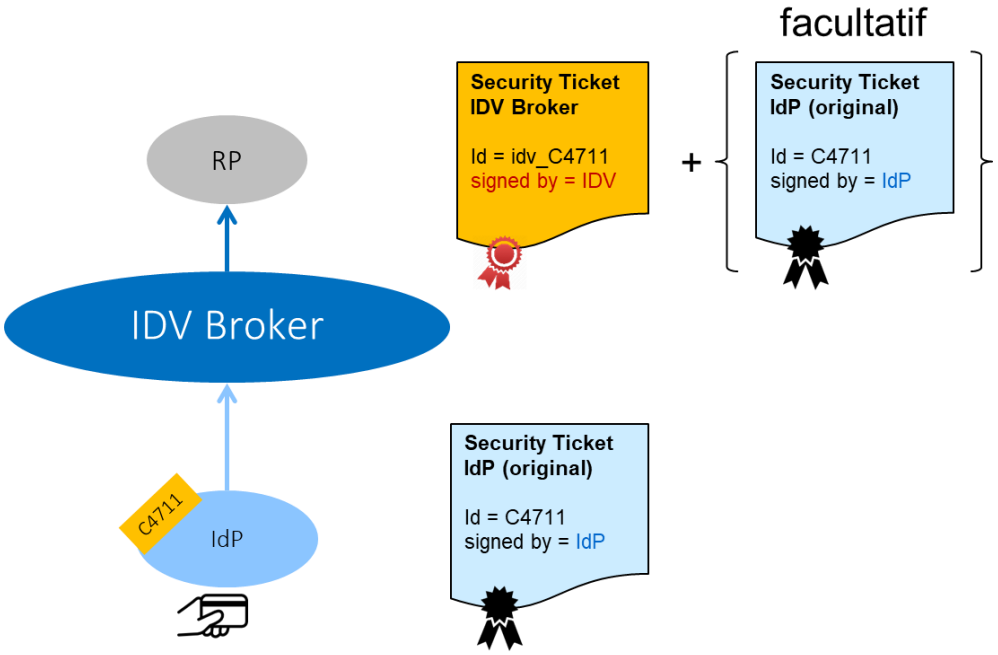

Illustration: Proxying avec un ticket de sécurité originale

Avec le mode du proxying, l'agent FSI reçoit des informations sur la connexion entre l'utilisateur et le RP et entre l’utilisateur et l’IdP et traite les attributs qu'il transmet. Pour cette raison les RP doivent avoir confiance totale dans l’agent FSI, en particulier ils ne peuvent pas vérifier quel IdP a émis le ticket de sécurité original. Proxying est le "réglage d'usine normal" de l’agent FSI et les RP fondent leur gestion d'identité en grande partie sur lui.

Avec la possibilité d'inclure le ticket de sécurité original, le RP ne doit pas seulement compter sur la confiance accordée à l’agent FSI. Le RP reçoit des informations supplémentaires sur la connexion entre l'utilisateur et l'IdP, ce qui peut être négatif en terme de protection des données.

Login pour des IdPs changeantes

Scénario : L'utilisateur effectue le login auprès RP en utilisant alternativement différents IdP, par exemple une fois via l'IdP A et une autre fois via l'IdP B. Dans le premier cas, la nameID *C4711 est* indiquée, dans le second, la nameID *0815*.

Pour que le RP puisse reconnaître une personne comme étant le même utilisateur lorsqu'il utilise différents IdP, l’agent FSI devrait offrir un identity linking et mettre en œuvre une procédure qui permet de relier logiquement les différents nameID de l'utilisateur dans le Broker. Sans identity linking, le RP ne peut pas distinguer si la nameID de deux IdP différents appartient ou non au même utilisateur.

L'identity linking n'a pas été mis en œuvre chez l’agent FSI pour des raisons de l’ergonomie et de protection des données. C'est l'une des raisons pour lesquelles l’agent FSI n'exige pas de comptes d'utilisateur. Les utilisateurs ne doivent pas gérer de paramètres ou de données, l'agent FSI n'est qu'une fonction de recherche qui permet de trouver des IdP appropriés et qui, sinon, reste en arrière-plan.

Un RP est libre d'offrir à l'utilisateur son propre identity linking. Pour ce faire, il doit impliquer l'utilisateur dans un processus de coordination, ce qui peut représenter un défi en termes de l'ergonomie, de sécurité et de protection de données.

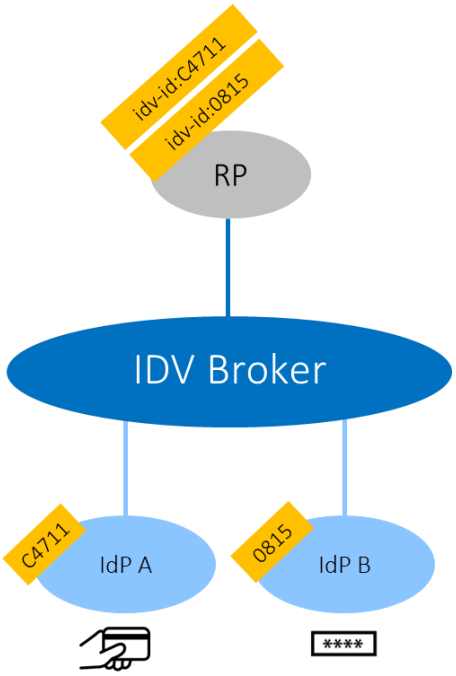

Illustration : login d'un utilisateur auprès des IdPs changeantes

Anonymisation de l'IdP

Dans certains cas, il est souhaité de cacher l'origine d'un ticket de sécurité, on parle d'*anonymisation de l'IdP*. Dans la plupart des cas, le RP ne devrait pas être en mesure d'identifier l'IdP auquel l'utilisateur s'est inscrit, car cela permet de tirer des conclusions sur l'utilisateur lui-même. Exemple : Un utilisateur qui utilise l'IdP de la police ne doit pas être identifié par le RP comme un membre des forces de police. Pour cette raison, l'IdP n'est pas indiqué dans le ticket de sécurité.

L'agent FSI peut être configuré de manière à ne pas révéler l'IdP auquel l'utilisateur s'est inscrit. Les RP doivent être prêts à ne pas vérifier le ticket de sécurité original ni à en déterminer l'origine. L'anonymisation de l'IdP nécessite confiance totale dans l'agent FSI.

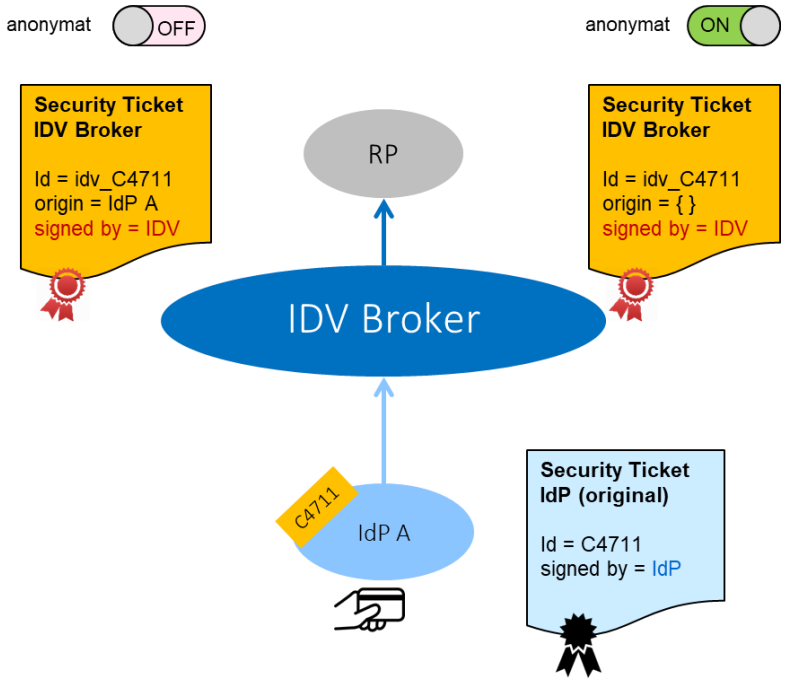

Illustration : l'anonymisation del'IdP peut être configurée

Conclusion : intégration technique de l’agent FSI pour RPs

Les RP qui utilisent l’agent FSI doivent tenir compte des conditions cadres suivantes.

1. L’agent FSI communique des identités numériques des utilisateurs des IdP affiliés et fournit au RP une nameID unique par le moyen d’un ticket de sécurité, qui ne correspond pas à la nameID de l'IdP utilisé. C'est la nameID de l’agent FSI.
2. L'agent FSI est conçu de telle manière que les IdP et RP lui font fondamentalement confiance. Valider le ticket de sécurité signifie s'assurer que l’agent FSI est l'émetteur. Ainsi, les RP n'ont à intégrer qu'une seule interface IdP, celle de l’agent FSI, pour avoir un accès aux IdP affiliés.
3. L'agent FSI peut soutenir soit des nameID persistantes soit des transitoires. Fournir la nameID de manière persistante n'est possible que si les IdP affiliés fournissent également leur propre nameID de manière persistante. La nameID transitoire peut toujours être soutenu par l’agent FSI.
4. Si un IdP utilise une nameID persistant, la nameID fourni par l’agent FSI dans son ticket de sécurité restera également persistant pour cet IdP.
5. L'agent FSI ne soutient pas l'identity linking. La nameID fourni par l’agent FSI est pour le même utilisateur différent pour chaque IdP.
6. L’agent FSI peut fournir le ticket de sécurité original de l'IdP avec le sien. Ainsi, le RP peut vérifier l'origine et l'authenticité séparément si nécessaire, c'est-à-dire que le RP ne doit pas seulement faire confiance à l’agent FSI.
7. L’agent FSI peut cacher l'IdP utilisé afin que le RP ne puisse pas l'identifier et ne sache pas où un utilisateur s'est authentifié (anonymisation de l'IdP).
8. L'agent FSI ne prend pas en charge l'agrégation d'attributs provenant de différents IdP. Si des attributs de plusieurs IdP sont nécessaires, le RP est responsable de la requête en série auprès des IdPs et de l'agrégation des attributs.