Julliet 2020

Gestion de la confiance et de la qualité

Informations et conseils utiles pour la création d'un domaine FSI

Objet du présent document

Les discussions avec des potentielles intéressées à la FSI ont montré qu'il existe certains malentendus concernant la sécurité, les normes de qualité et les relations de confiance. Ce document explique la relation entre la confiance et la qualité dans la fédération d'identités et montre comment les domaines de la FSI peuvent définir leurs propres règles. Il est possible d'en savoir plus à l'avance : Il n'est pas vrai que

- les services web doivent faire aveuglément confiance à l'agent FSI,
- les services web doivent accepter tous les IdP affiliés à la FSI pour le login,
- la FSI oblige les IdP à une certification de qualité.

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.

Domaine FSI : Une communauté d'IdP et de RP qui forment un fédération d'identités indépendant. Ils fixent leurs propres règles, définissent des niveaux de qualité et des principes de confiance mutuelle.

Situation initiale

L'agent FSI assure la médiation des identités numériques de plusieurs IdP à plusieurs RP, mais dans des cas individuels, toujours d'un IdP à un RP. Médiation signifie que la demande d'authentification du RP est transmise à l'IdP désigné par l'utilisateur, comme si l'agent lui-même demandait une authentification. L'agent crée son propre ticket de sécurité à partir du ticket de sécurité de l'IdP et le transmet au RP. Dans ce processus, tant les RP que les IdP dépendent d'informations authentiques et non altérées. L'agent joue un rôle central dans la garantie de la qualité et de la sécurité ; il est le point d'ancrage de la confiance pour les IdP et les RP.

Ceux qui rejoignent la FSI en tant que RP ou IdP auront des questions sur la qualité et la sécurité. Avant de répondre en détail à certaines d'entre elles, le principe des domaines est expliqué.

Domaines FSI

Établir un fédération d'identités signifie créer des directives techniques et organisationnelles pour les participants affiliés. Les exigences relatives aux IdP dépendent du secteur d'application, elles sont différentes dans la cyberadministration pour personnes privées, dans le secteur de la santé, dans l'environnement judiciaire ou dans le réseau universitaire. Il n'y a pas un seul fédération d'identités qui puisse couvrir tous les besoins, mais les différents secteur d'application nécessitent plutôt leur propre agent. C'est là que les domaines FSI entrent en jeu. Les domaines FSI sont mis en place par les IdP et les RP, qui sont soumis à leur propre ensemble de règles définies par les membres et qui définissent leurs propres niveaux de qualité et base de confiance.

Les domaines FSI ont en commun qu'ils utilisent la même infrastructure technique: FSI. Sinon, les domaines FSI sont des groupes d'utilisateurs autonomes qui sont isolés les uns des autres. Les membres d'un domaine ne voient que leurs propres membres, mais aucun membre des autres domaines. Par exemple, l'agent ne fera jamais une transmission entre un RP provenant d'un domaine du secteur de la santé et un IdP provenant d'un domaine du secteur de la justice.

Qualité, Confiance et Trust Framework

Qualité

Des normes nationales et internationales existent pour la qualité des systèmes de gestion de l'identité, par exemple la norme eCH-0170, le règlement eIDAS 910/2014, le certificat ISO/IEC 29115, le standard NIST SP 800-63-3 et plus encore. Tous ont leurs forces et leurs faiblesses. L'établissement du Trust Framework FSI (voir ci-dessous) est basé sur le modèle de qualité eCH-0170, qui définit quatre niveaux de confiance, qui résultent à leur tour de quatre dimensions de qualité :

- La qualité de l'authentification résulte de la force des possibles certifications d'un moyen d'authentification.
- La qualité de l'identification et de l'enregistrement d'une personne physique est déterminée par la force de l'identification et de la transmission des moyens d'authentification.
- La qualité de la gouvernance concerne la supervision, la responsabilité et la maturité.
- La qualité de la fédération est déterminée par l'authenticité, la protection de la confidentialité, la forme de transmission et la preuve de possession de la confirmation d'authentification.

Les dimensions de la qualité donnent une image globale de la qualité de l'identification et de l'authentification, bien que la dimension la plus faible détermine plus ou moins le résultat final. En d'autres termes : si une dimension est faible, la qualité globale l'est aussi. C'est tout à fait logique, car une qualité élevée exige une qualité élevée dans tous les dimensions. À quoi sert une transmission techniquement bien protégée d'une identité numérique (fédération) si l'identification de la personne n'a été obtenue que par courrier électronique et que vous ne savez pratiquement pas à qui vous avez affaire ?

La FSI ne se fixe pas à un modèle de qualité spécifique et laisse la définition des critères de qualité à chaque domaine FSI, car seul le domaine même sait ce dont il a besoin. Pour des raisons techniques, FSI fixe quelques limites pour le modèle de qualité, par exemple, on ne peut pas distinguer plus de quatre niveaux de qualité dans un domaine. L'agent n'a pas besoin de savoir ce que chaque niveau signifie et quels sont les critères qui le sous-tendent. Un domaine peut définir les niveaux 1 à 4, un autre seulement trois, A à C, et un autre encore les appelle argent, or et platine. Tout cela est insignifiant pour la FSI, tant que la qualité la plus élevée ne dépasse pas celle de l'agent. Qu'est-ce que cela signifie ? Parmi les quatre dimensions de la qualité, une seule touche directement l'agent FSI, à savoir la fédération. L'agent soutient le niveau de confiance 3 selon la norme eCH-0170, qui correspond à une qualité rarement exigée. La FSI ne pourrait pas supporter un domaine FSI dont les exigences vont jusqu'au niveau de confiance 4. Toutefois, cette limitation ne devrait pratiquement pas poser de problème pour les cas d'utilisation prévues par la FSI. A titre de comparaison : SuisseID serait classé au niveau 2.

Confiance

La question suivante se pose : Pour quelles raisons doit-on s'appuyer sur un service extérieur qui affecte la propre sécurité et pourrait la même mettre en danger ? Dans le contexte de la FSI, ce service externe comprend deux composantes, d'une part le ticket de sécurité d'un IdP inconnu et, d'autre part, la transmission du ticket de sécurité par l'agent FSI. Le danger est que soit l'IdP, soit l'agent ou les deux n'exécutent pas leurs tâches respectives avec suffisamment de conscience ou de compétence et

que le RP autorise ensuite l'utilisateur sur la base d'un ticket de sécurité qualitativement insuffisant sans en avoir conscience.

La principale relation de confiance est celle qui existe entre le RP et l'agent FSI. Le RP compte sur le fait que l'agent ne se procure que des tickets de sécurité de qualité suffisante et qu'auprès d'IdP affiliés et que l'utilisateur ne reçoit que des IdP appropriés à sélectionner lors de son login au RP. Lors de la transmission, l'agent doit relier les exigences de qualité du RP à la force d'authentification de l'IdP, ce qui nécessite un modèle de qualité qui est interprété et accepté de la même manière par tous les IdP et RP affiliés.

Base pour faire confiance dans l'FSI

Dans l'exemple ci-dessous, le domaine a défini un modèle de qualité à trois niveaux, qu'il appelle Level of Assurance (LOA). Une compréhension commune de la qualité au sein du domaine constitue la base des tâches de transmission de l'agent.

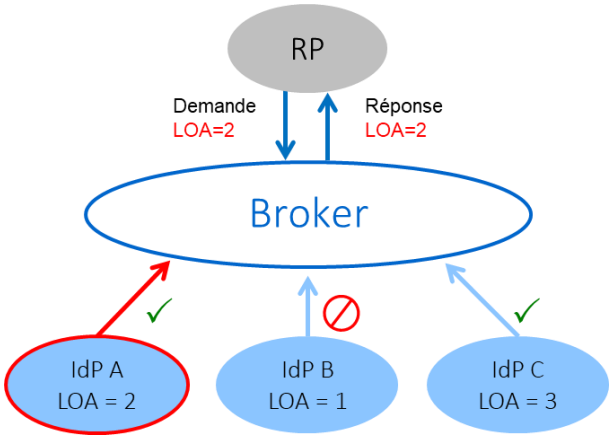

Illustration : conformité du niveau de qualité lors de la transmission

Le RP exige la qualité LOA=2 dans sa demande, ce qui exclut l'IdP B. L'utilisateur se voit proposer les IdP A et C et il utilise A. La réponse de l'agent au RP contient le niveau de qualité réel LOA=2. Si l'utilisateur avait utilisé l'IdP C, LOA=3 serait dans la réponse.

Pour que la confiance dans ces opérations soit justifiée, deux conditions doivent être remplies. Premièrement, le RP doit disposer d'informations pour pouvoir décider si l'agent fonctionne correctement, en toute sécurité et dans le respect de tous les critères de protection des données. Deuxièmement, un RP doit pouvoir vérifier de manière indépendante et à tout moment que la qualité d'un IdP est bien celle qui est indiquée comme valeur de LOA. Cela ne signifie pas que les contrôles et les recherches doivent être effectués automatiquement à chaque authentification, mais cela signifie qu'il doit y avoir un moyen hors ligne pour les RP de vérifier la qualité d'un IdP si nécessaire.

La première condition concerne la relation de confiance entre la FSI et le RP. L'exploitation, l'entretien et le développement de l'agent FSI seront à l'avenir gérés par un organisme de droit public, dont les comités de pilotage comprennent entre autres des représentants des domaines FSI. La confiance en la FSI est la confiance en une administration publique qui fonctionne et en la qualité de ses services. Si un domaine veut mettre l'agent FSI hors-jeu en ce qui concerne la confiance, la meilleure manière possible est de configurer le domaine de manière à ce que l'agent attache le ticket de sécurité de l'IdP au sien, ce qui permet au domaine de vérifier le ticket de sécurité original.

La deuxième condition concerne la relation de confiance entre l'IdP et le RP. L'agent lui-même transmet au RP les informations fournies par l'IdP, qui, selon lui, ne peuvent être vérifiées. L'opérateur de l'agent FSI ne peut et ne veut pas assumer aucune garantie pour cette information, sa tâche est la transmission sécure, confidentielle et intégrale du ticket de sécurité d'un bout à l'autre. L'agent n'est pas responsable du contenu, c'est la responsabilité de l'IdP émetteur. Mais exactement là se trouve le fond de la confiance, dont le RP doit faire preuve.

Le projet FSI a montré comment le problème peut être résolu. Dans le cadre du développement de la plate-forme de l'agent FSI, un *Trust Framework* a été élaboré pour aider les futurs domaines. Cela permet à un domaine de configurer et saisir l'établissement de la confiance entre les IdP et les RP.

Trust Framework pour des applicaitons de cyberadministration

Le Trust Framework est une mesure organisationnelle qui permet aux membres d'un domaine FSI d'établir la confiance nécessaire. Un certain nombre d'organes cantonaux ont participé activement au développement de la FSI et il y a eu une volonté de l'utiliser pour l'identification et l'authentification mutuelle entre les cantons. Ils l'ont fait à condition qu'il existe un instrument approprié pour la reconnaissance mutuelle des niveaux de qualité des IdP cantonaux, sur lequel chacun puisse compter.

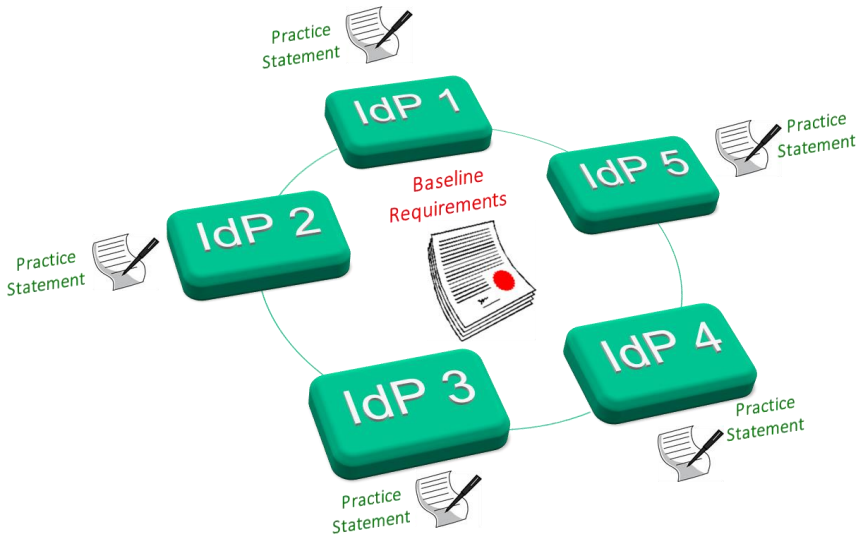

Illustration : Trust Framework

Le cadre de confiance comprend deux principaux artefacts : exigences de base (Baseline Requirement) et déclaration de pratique (Practice Statement). Ce sont des documents qui s'adressent principalement aux IdP d'un domaine.

Les exigences de base décrivent les niveaux de qualité et contiennent une spécification détaillée des mesures techniques et organisationnelles lesquelles les IdP doivent remplir lors de l'identification des personnes et de l'émission des tickets de sécurité. À l'aide de ce document, les RP apprennent quel modèle de qualité est utilisé, comment ils communiquent leurs exigences de qualité à l'agent et quelles exigences un IdP doit remplir s'il prétend satisfaire un certain niveau de qualité.

Les déclarations de pratique sont des auto-déclarations des IdP sur leur propre qualité. Dans ces documents, chaque IdP documente la manière dont les exigences de base sont mises en œuvre en détail. Les déclarations de pratique doivent être mises à la disposition de tous les membres du domaine. Les IdP peuvent utiliser ces informations comme base de comparaison, les RP les utiliseront pour justifier leur volonté d'accepter des ticket de sécurité des IdP inconnus jusqu'à ce moment, ou plus simplement de faire confiance aux IdP.

La FSI n'effectue pas d'audits sur les IdP et n'est pas un organe de conciliation approprié. La mise en œuvre d'un Trust Framework est uniquement à l'affaire du domaine. Il peut formuler les exigences de base de la manière qu'elle souhaite et peut, par exemple, prévoir le droit à l'inspection mutuelle, l'obligation d'effectuer régulièrement des audits externes ou internes, exiger une certification et prévoir des sanctions.

Ce que fait FSI, et ce pour quoi l'agent FSI a été construit, c'est la transmission garanti et sécure d'IdP d'une certaine qualité aux RP. L'agent s'appuie sur les informations contenues dans les demandes d'authentification respectivement dans les métadonnées stockées des IdP et RP affiliés. Ce que fait l'agent est une transmission purement technique de données de sécurité.

Afin de fournir aux cantons membre une base pour l'établissement d'un domaine, des exigences de base exemplaires ont été établies. Dans ce document ils sont décrits en détail sur 25 pages les mesures, les processus et les fonctions techniques qu'un IdP doit mettre en œuvre s'il veut atteindre le niveau LOA 2 selon la norme eCH-0170. Le document "*Baseline Requirements for the E-Gov Domain of the Identity Network Switzerland (INS)"* peut être téléchargé à l'adresse suivante : www.idv-fsi.ch Les futurs domaines sont invités à utiliser ces exigences de base comme modèle pour leur propre domaine.

Questions d’un Relying Party

Quelles sont les mesures techniques de sécurité mises en œuvre par la FSI ? La sécurité de l’agent a été développée selon l'état de la technique. La communication des données est cryptée et protégée contre toute manipulation non autorisée par des signatures numériques. L’agent met en œuvre plusieurs SAML bindings, en particulier Web SSO over HTTP et le artifact binding. L’agent atteint ainsi le niveau LOA 3 selon la norme eCH-0170, *modèle de qualité pour l'authentification des sujets*.

Quelle est la force d'authentification offerte par les IdP ? Chaque IdP authentifie l'utilisateur avec les moyens dont il dispose. La FSI ne donne pas de directives et la qualité varie d'un IdP à l'autre. Il appartient au domaine de définir une échelle de qualité dans les exigences de base et de classer les IdP en fonction des critères. Ce n'est qu'alors que les RP peuvent décider de la qualité qu'ils veulent exiger de l’agent, et donc des IdP du domaine.

Comment évaluer la qualité d'un IdP ? Chaque domaine définit sa propre échelle de qualité, qu'il rend accessible dans les exigences de base. Il indique pour chaque IdP quelles mesures sont requises et à quel niveau de qualité. Si vous souhaitez savoir comment un IdP particulier remplit ces exigences en détail, il faut consulter la déclaration de pratique de l'IdP.

Peut-on demander une qualité minimale ? Oui. Selon le mode de fonctionnement de l’agent, la qualité minimale requise par un RP lors du login est mise dans les métadonnées ou transmise dynamiquement à l’agent. Dans les deux cas, l’agent ne prendra en considération que les IdP pour la transmission qui répondent aux exigences de qualité.

Chaque IdP doit-il être accepté ? Non. Les IdP potentiels sont automatiquement limités par les critères de qualité et seuls ceux qui répondent aux exigences de la RP seront placés.

Est-il possible d'exclure un IdP particulier ? L'exclusion d'un certain IdP ne fait pas partie des fonctions de base de l’agent, en principe tous les IdP qualitativement appropriés sont proposés. Toutefois, il existe une solution de contournement : si le domaine est configuré de telle sorte que l’agent fournisse le ticket de sécurité de l'IdP en plus de celui signé par lui-même, un RP peut filtrer l'IdP qui ne lui convient pas.

Quelle qualité s'applique aux attributs ? Un domaine peut définir la qualité des attributs dans les exigences de base. Il n'existe pas d'autre définition de la qualité, par exemple sous la forme d'une échelle de qualité particulière pour les attributs. Un domaine est libre de définir son échelle de qualité sur la base de n'importe quel critère et peut inclure la qualité des attributs dans la classification des IdP.

L'ensemble des attributs dépend-il de la qualité de l'authentification ? Il appartient au domaine de déterminer si et comment le niveau d'authentification doit être en corrélation avec l'ensemble des attributs fournis. Le domaine définit une telle règle dans les exigences de base.

La FSI est-elle responsable d'une fausse authentification ? On ne peut répondre à cette question qu'une fois que l'organisation opérationnelle a été déterminée. Cela se n’applique que pour la tâche principale d’agent FSI, c'est-à-dire pour la transmission des tickets de sécurité. Les domaines sont libres d'établir un régime de responsabilité afin de renforcer la confiance dans les IdP et d'imposer des sanctions en cas d'erreur.

Questions d’un Identity Provider

Quel est le niveau d'authentification requis pour participer à la FSI ? En principe, la FSI est ouvert à tout IdP car la FSI ne prédéfini pas la qualité. Un domaine déterminera lui-même les critères auxquels un IdP doit répondre pour participer.

Une certification est-elle nécessaire ? La FSI ne précise rien de tel. Chaque domaine définit pour lui-même les critères de qualité qu'il impose aux IdP, une certification peut en faire partie.

D'où viennent les critères de qualité ? Un domaine est composé de membre qui sont soumis à un ensemble de règles communes soutenues par tous. La définition des niveaux de qualité et les critères de leur conformité sont définis dans les exigences de base.

Où se situe son propre IdP par rapport aux autres ? Selon le Trust Framework de la FSI, un IdP indique en détail dans sa déclaration de pratique les mesures techniques et organisationnelles qu'il prend pour satisfaire aux exigences de qualité. Les IdP peuvent comparer leurs propres mesures avec celles des autres.

□