

INITIATIVE MONDIALE EN FAVEUR DE L'INCLUSION FINANCIÈRE (FIGI)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

11/2019

Groupe de travail sur la sécurité, l'infrastructure et la confiance

**Mise en œuvre de technologies d'authentification
sécurisée pour les services financiers numériques**

Rapport sur l'axe de travail "Sécurité"



AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

Un nouveau programme mondial visant à faire progresser la recherche sur la finance numérique et à accélérer l'inclusion financière numérique dans les pays en développement, l'Initiative mondiale en faveur de l'inclusion financière (FIGI), a été lancé par le Groupe de la Banque mondiale, l'UIT et le Comité sur les paiements et les infrastructures de marché (CPMI), avec l'appui de la Bill and Melinda Gates Foundation.

Le Groupe de travail sur la sécurité, l'infrastructure et la confiance est l'un des trois groupes de travail qui ont été créés dans le cadre de la FIGI et qui sont dirigés par l'UIT. Les deux autres sont le Groupe de travail sur l'identité numérique et le Groupe de travail sur l'acceptation des paiements électroniques. Ils sont dirigés par le Groupe de la Banque mondiale.

© UIT 2020

Le présent rapport est publié sous une licence Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International License (CC BY-NC-SA 4.0).

Pour de plus amples informations, veuillez consulter le site suivant:
<https://creativecommons.org/licenses/by-nc-sa/4.0/>.

**Mise en œuvre de technologies d'authentification sécurisée pour les
services financiers numériques**

Axe de travail "Sécurité"

À propos du présent rapport

Le présent rapport a été rédigé par Andrew Hugues et Abbie Barbir. Les auteurs tiennent à remercier les contributeurs et réviseurs suivants: Arnold Kibuuka, Vijay Mauree, Harm Arendshorst, Tiakala Lynda Yaden, M. Mayank, Vinod Kotwal, Jeremy Grant, Brett McDowell, Adam Power, Sylvan Tran, Ramesh Kesanupalli, Chunpei Feng, Hongwei (Kevin) Luo, David Pollington, Matthew Davie, Wycliffe Ngwabe, Salton Massally et Mathan Babu Kasilingam.

Si vous souhaitez nous communiquer des informations complémentaires, veuillez contacter Vijay Mauree à l'adresse tsbfigisit@itu.int.

Table des matières

1	Sommaire de direction	1
2	Acronymes	3
3	Contexte.....	4
4	Introduction	5
4.1	Section des exemples de mise en œuvre.....	6
5	Normes et réglementations applicables en matière d'authentification forte.....	6
5.1	Recommandation UIT-T X.1254	7
5.2	Publication spéciale 800-63-3 du NIST.....	7
5.3	Règlement sur les eIDAS	8
5.4	Directives sur les services de paiement.....	8
5.5	L'Alliance ID2020	9
5.6	Objectifs de normalisation	10
6	Technologies et spécifications d'authentification forte	10
6.1	Caractéristiques des systèmes d'authentification avancée	11
6.2	Spécifications de l'Alliance FIDO	12
6.3	Spécifications de Mobile Connect	17
6.4	Spécifications IFAA.....	23
6.5	Authentification Aadhaar	27
6.6	Authentification cognitive continue.....	33
6.7	Identité décentralisée et registres distribués.....	34
7	Exemples de mise en œuvre de systèmes d'authentification forte	41
7.1	Cas d'utilisation: Inscription et ouverture de compte	41
7.2	Cas d'utilisation: Authentification pour accéder à un service financier numérique.....	50
8	Conclusion	58
	Annexe A – Bibliographie.....	59
	Annexe B – Conseils aux fournisseurs de DFS	62
	Annexe C – Conseils aux fournisseurs de systèmes d'authentification	63

Liste des figures

<i>Figure 1 – L'écosystème des services financiers numériques</i>	<i>5</i>
<i>Figure 2 – Recommandation UIT-T X.1254</i>	<i>7</i>
<i>Figure 3 – Architecture du cadre d'authentification universelle</i>	<i>14</i>
<i>Figure 4 – Enregistrement FIDO de nouvelles clés</i>	<i>16</i>
<i>Figure 5 – Authentification FIDO.....</i>	<i>17</i>
<i>Figure 6 – Portefeuille de services de Mobile Connect.....</i>	<i>18</i>
<i>Figure 7 – Mise en correspondance des niveaux de garantie des eIDAS et de Mobile Connect.....</i>	<i>20</i>
<i>Figure 8 – Architecture de référence de Mobile Connect et des eIDAS</i>	<i>21</i>
<i>Figure 9 – Flux technique de Mobile Connect et des eIDAS</i>	<i>21</i>
<i>Figure 10 – Cas d'utilisation de la DSP2 avec Mobile Connect</i>	<i>22</i>
<i>Figure 11 – Architecture de référence de haut niveau de la DSP2</i>	<i>22</i>
<i>Figure 12 – Authentification forte du client avec Mobile Connect – initiée par le serveur</i>	<i>23</i>
<i>Figure 13 – Authentification forte du client avec Mobile Connect – initiée par le dispositif.....</i>	<i>23</i>
<i>Figure 14 – Authentification biométrique IFAA – modèle local</i>	<i>24</i>
<i>Figure 15 – Authentification biométrique IFAA – modèle local – enregistrement.....</i>	<i>25</i>
<i>Figure 16 – Authentification biométrique IFAA – modèle local – authentification</i>	<i>26</i>
<i>Figure 17 – Authentification biométrique IFAA – modèle local – désenregistrement</i>	<i>26</i>
<i>Figure 18 – Authentification biométrique IFAA – modèle à distance.....</i>	<i>27</i>
<i>Figure 19 – Transactions du système de paiement activé par Aadhaar.....</i>	<i>29</i>
<i>Figure 20 – Processus de la passerelle de paiement Aadhaar</i>	<i>30</i>
<i>Figure 21 – La plateforme Cognitive Continuous Authentication™ d'Acceptto</i>	<i>33</i>
<i>Figure 22 – Architecture de haut niveau Acceptto-FIDO.....</i>	<i>31</i>
<i>Figure 23 – Couches de l'infrastructure Sovrin</i>	<i>36</i>
<i>Figure 24 – Rôles et relations des parties prenantes</i>	<i>37</i>
<i>Figure 25 – Résolveur universel de DID</i>	<i>40</i>
<i>Figure 26 – Portefeuille d'identités décentralisées avec déclarations vérifiables</i>	<i>40</i>
<i>Figure 27 – Infrastructure d'identité du Bureau national de l'état civil</i>	<i>44</i>
<i>Figure 28 – Architecture de l'écosystème d'évaluation du crédit numérique.....</i>	<i>44</i>
<i>Figure 29 – Architecture de l'écosystème.....</i>	<i>45</i>
<i>Figure 30 – Identifiant national et i-PIN en République de Corée.....</i>	<i>45</i>
<i>Figure 31 – Processus d'enregistrement du service K-FIDO</i>	<i>46</i>
<i>Figure 32 – Processus d'enregistrement de la norme FIDO.....</i>	<i>48</i>
<i>Figure 33 – Inscription d'un utilisateur d'un prestataire de soins de santé</i>	<i>50</i>
<i>Figure 34 – Cas d'utilisation de l'IFAA: paiement par empreinte digitale/reconnaissance faciale avec Alipay</i>	<i>51</i>

<i>Figure 35 – Cas d'utilisation de l'IFAA: paiement par empreinte digitale/reconnaissance faciale avec Alipay – Infrastructure technique</i>	<i>52</i>
<i>Figure 36 – Processus technique des services d'authentification et d'e-KYC.....</i>	<i>53</i>
<i>Figure 37 – Processus d'authentification du service K-FIDO</i>	<i>54</i>
<i>Figure 38 – Parcours d'authentification de l'utilisateur sur un compte de jeu avec T-Auth</i>	<i>56</i>
<i>Figure 39 – Processus d'authentification de la norme FIDO</i>	<i>57</i>

Liste des tableaux

<i>Tableau 1 – Niveaux de garantie de l'authentificateur de la publication spéciale du NIST 800-63-3</i>	<i>8</i>
<i>Tableau 2 – Caractéristiques des systèmes d'authentification avancée</i>	<i>12</i>
<i>Tableau 3 – Exemples de cas d'utilisation des services financiers numériques</i>	<i>41</i>

1 Sommaire de direction

Le présent rapport a été rédigé à partir des contributions et des discussions du Groupe de travail sur la sécurité, l'infrastructure et la confiance de la FIGI sur l'axe de travail "Authentification".

L'écosystème de services financiers numériques (DFS) requiert des technologies d'authentification forte interopérables et normalisées afin d'atténuer les risques auxquels ils sont exposés et de protéger leurs actifs. Les approches d'authentification faible sur navigateur Web ainsi que les approches fondées sur des mots de passe ne garantissent plus la sûreté des DFS. Ce rapport est axé sur la mise en œuvre. Il décrit les technologies et les normes qui peuvent être utilisées dans le cadre de la mise en œuvre des systèmes d'authentification forte pour les DFS et en livre quelques exemples.

Le Groupe spécialisé de l'UIT-T sur les services financiers numériques, l'organe consultatif multipartite chargé de favoriser le développement d'écosystèmes de services financiers numériques sûrs, a précédemment formulé des recommandations sur la sécurité, l'identification et l'authentification pour les DFS. Le présent rapport aborde plusieurs de ces recommandations.

L'un des principaux objectifs des systèmes d'authentification est d'accroître la fiabilité de l'identité de l'utilisateur préalablement inscrit afin que celui-ci puisse être régi par la politique de contrôle d'accès et d'autorisation au terme de l'authentification.

Les choix de conception et les choix techniques relatifs à chaque élément du système d'authentification ont une incidence sur sa résistance aux attaques ainsi qu'aux altérations de sécurité dues aux menaces courantes. Les systèmes d'authentification forte ont été pensés pour atténuer les menaces que les systèmes d'authentification faibles ne sont pas en mesure de contourner.

Les systèmes d'authentification traditionnels utilisés aujourd'hui correspondent aux besoins de l'Internet antérieur aux appareils mobiles. Ils sont basés sur un événement d'authentification unique généralement effectué au démarrage de l'application, au terme duquel il est supposé que l'utilisateur, l'appareil et la session ne changent pas. L'expérience a montré que cette approche affaiblit les systèmes d'authentification.

Outre les éléments des systèmes d'authentification forte, les systèmes d'authentification avancée ont été conçus en adéquation avec les modèles de menaces et de conception actuels. Par rapport aux systèmes d'authentification forte, qui utilisent un logiciel client d'analyse environnementale et comportementale, l'accent est davantage mis sur la détection et l'authentification des utilisateurs humains. De nouvelles approches sont mises en œuvre pour minimiser les contraintes lors de l'authentification mobile et à plusieurs facteurs. De nombreux systèmes sont par ailleurs principalement axés sur les technologies mobiles. L'authentification s'effectue désormais à différents moments de l'interaction entre l'utilisateur et le système: au moment de l'identification, lors de la sollicitation de privilèges supplémentaires (l'authentification dite "par paliers"), et même en continu tout au long de la session.

Le présent rapport décrit les normes techniques et politiques couramment adoptées afin d'assurer la prise en charge des mécanismes d'authentification forte.

Les exemples de systèmes d'authentification forte et avancée sont classés dans l'une des deux catégories suivantes: inscription ou authentification pour l'utilisation de DFS. Ces deux catégories de cas d'utilisation affectent essentiellement les utilisateurs de DFS.

Les exemples présentés pour le cas d'utilisation relatif à l'inscription décrivent la façon dont les informations d'identité précédemment établies peuvent être utilisées pour créer de nouveaux comptes de service ainsi que pour satisfaire aux exigences relatives aux processus de KYC. Dans chacun de ces exemples, l'individu a précédemment été inscrit auprès d'une autorité: ses informations d'identité

ont donc été collectées, vérifiées et stockées. Elles peuvent ensuite être présentées aux fournisseurs de services avec l'autorisation de la personne concernée.

Les exemples du cas d'utilisation relatif à l'authentification d'entité décrivent la façon dont les mécanismes d'authentification de nouvelle génération sont exploités pour identifier une personne et l'autoriser à utiliser des services.

Ce rapport comporte plusieurs exemples de systèmes d'authentification forte et avancée qui ouvrent l'accès à des services financiers. D'autres travaux de normalisation doivent être conduits afin de veiller à ce que les technologies soient adaptées aux besoins et que les points forts et capacités des différentes approches en la matière puissent être évalués.

En définitive, il existe des solutions efficaces pour contrer les menaces accrues qui pèsent aujourd'hui sur les DFS. Il est possible, grâce à une planification minutieuse, de directives claires et d'efforts soutenus, d'en garantir l'accès de façon sûre, peu contraignante et efficace.

2 Acronymes

AUA	Agence d'utilisateurs d'authentification
API	Interface de programmation d'application
APB	Passerelle de paiements Aadhaar
AEPS	Système de paiement activé par Aadhaar
CTAP	Protocole client-authentificateur
DFS	Services financiers numériques
DSP2	Directive sur les services de paiement 2
e-KYC	Identification électronique
eIDAS électroniques	Identification électronique et services de confiance pour les transactions
FIDO UAF mot de passe	Cadre d'authentification de l'utilisateur de la norme ouverte d'authentification sans
FIDO U2F passe	Deuxième facteur universel de la norme ouverte d'authentification sans mot de
FIPS	Federal Information Processing Standards
GUID	Identificateur global unique
HSM	Module matériel de sécurité
IFAA	Internet Finance Authentication Alliance
IMEI	Identité internationale de l'équipement mobile
IMSI	Identité internationale de station mobile
KUA	Agence d'utilisateurs de KYC
MFA	Authentification à facteurs multiples
MSISDN	Numéro d'annuaire d'abonné international de station mobile
NFC	Communication en champ proche
NIST	National Institute of Standards and Technology
NPCI	Société nationale des paiements de l'Inde
OTP	Mot de passe à usage unique
RTS	Normes techniques et réglementaires
SCA	Authentification forte du client
SIM	Module d'identité de l'abonné
U2F	Deuxième facteur universel
UAF	Cadre d'authentification universelle
UIDAI	Autorité d'identification unique de l'Inde
VPA	Adresse de paiement virtuelle

3 Contexte

L'Initiative mondiale en faveur de l'inclusion financière a été créée dans le prolongement des activités du Groupe spécialisé de l'UIT-T sur les services financiers numériques ("Groupe spécialisé") constitué en tant qu'organe consultatif multipartite chargé de favoriser le développement d'écosystèmes de DFS sûrs et porteurs. Les objectifs généraux du Groupe spécialisé étaient les suivants: i) intensifier et formaliser la collaboration entre les autorités des secteurs de la finance et des télécommunications concernant les DFS; ii) établir la liste des principaux obstacles au développement d'écosystèmes de DFS sûrs et porteurs; iii) étudier le traitement concret de ces questions et échanger des informations sur les meilleures pratiques en vigueur; et iv) élaborer des recommandations politiques en la matière afin d'aider les autorités et les autres parties prenantes à relever ces défis dans leur pays. Le Groupe spécialisé a réuni des autorités des secteurs de la finance et des télécommunications, des parties prenantes du secteur privé, des défenseurs des consommateurs, des experts techniques des DFS, des partenaires de développement ainsi que d'autres parties prenantes clés des DFS en vue d'étudier conjointement ces questions et d'élaborer des recommandations consensuelles. [1]

Le présent rapport aborde les recommandations suivantes [1]:

- Il est recommandé d'utiliser des appareils mobiles compatibles avec l'utilisation des mécanismes d'authentification forte.
- Il est recommandé que les opérateurs de DFS créent une identité numérique pour leurs clients au moment de l'inscription. Ils pourront l'utiliser à la fois dans leurs transactions financières numériques et (le cas échéant) pour la valider auprès de fournisseurs de services externes.
- Il est recommandé que les opérateurs de DFS offrent à leurs clients une expérience d'enregistrement et d'authentification simple et intuitive.
- Les autorités gouvernementales chargées des politiques et les régulateurs sont encouragés à utiliser les systèmes d'identification nationaux, ou tout autre système d'identification à l'échelle du marché, pour faciliter l'ouverture de comptes de transactions, le traitement des paiements et, dans certains cas, l'amélioration de la sécurité des transactions.
- Les développeurs d'applications doivent veiller à ce que les applications DFS soient conçues et mises en œuvre conformément aux bonnes pratiques de l'industrie et des organismes de normalisation en matière de développement de logiciels sécurisés, de communication chiffrée et authentifiée ainsi que de codage sécurisé.
- Les régulateurs doivent normaliser l'enregistrement de l'identité numérique et assurer l'interopérabilité des opérateurs de services financiers numériques ainsi que des fournisseurs de services qui s'appuient sur elle.

L'écosystème des services financiers numériques se compose d'utilisateurs (usagers, entreprises, organismes publics et groupes à but non lucratif) qui ont besoin de produits et de services financiers numériques et interopérables; de fournisseurs (banques, autres institutions financières agréées et entités non bancaires) qui fournissent ces produits et services par des moyens numériques; d'infrastructures financières, techniques et autres qui les mettent en œuvre; et de politiques, lois et réglementations gouvernementales qui font en sorte qu'ils puissent être fournis de manière accessible, abordable et sûre. [2]

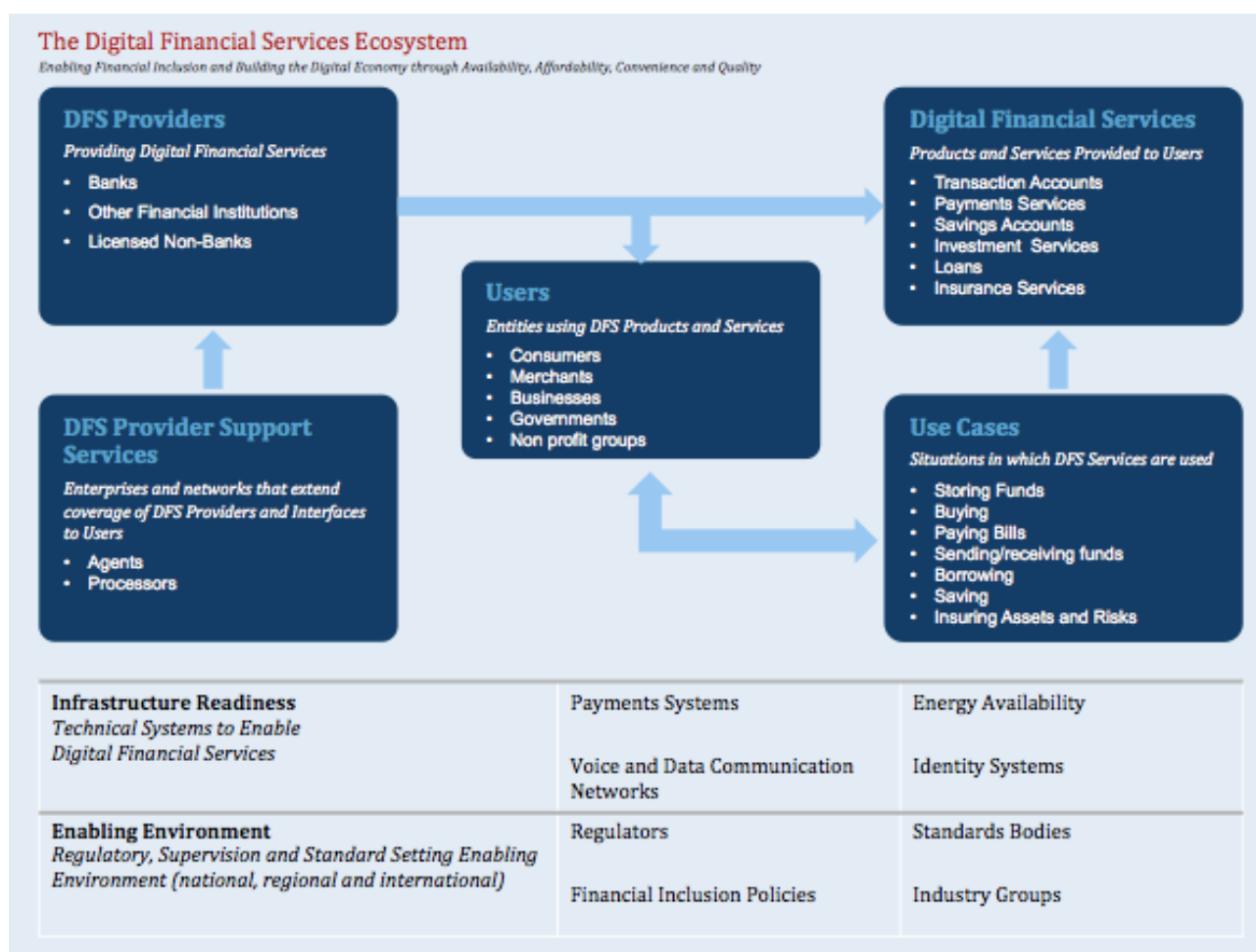


Figure 1 – L'écosystème des services financiers numériques

Le présent rapport décrit les aspects de l'infrastructure des systèmes d'identification qui rendent possible la mise en place de services financiers numériques: l'ouverture de compte (par e-KYC) et l'authentification forte des identifiants électroniques.

4 Introduction

L'écosystème de services financiers numériques (DFS) requiert des technologies d'authentification forte interopérables et normalisées afin d'atténuer les risques auxquels ils sont exposés et de protéger leurs actifs.

Afin de lutter contre le blanchiment d'argent et d'autres utilisations abusives des systèmes financiers, les organismes de réglementation sont de plus en plus nombreux à exiger que les clients suivent un processus d'identification rigoureux.

Avec l'augmentation du nombre de clients exclusivement mobiles et à distance, les institutions financières sont confrontées à de nouveaux types de fraudes, d'usurpations d'identité et de menaces pour la sécurité face auxquels les anciens systèmes d'authentification par mot de passe sont impuissants.

Les systèmes, technologies et approches décrits dans ce rapport ont été conçus pour être utilisés dans des environnements informatiques mobiles. Ils reposent sur des techniques bien établies telles que la cryptographie à clés publiques ainsi que de nouvelles techniques telles que la génération et le stockage de clés cryptographiques directement sur l'appareil plutôt que de manière centralisée. L'adoption

progressive des appareils mobiles a accéléré l'obsolescence des dispositifs de sécurité – déjà peu sécurisés – basés sur mots de passe. Par ailleurs, la disponibilité croissante des lecteurs d'empreintes digitales et d'autres capteurs biométriques rend désormais possible l'avènement des technologies d'authentification sans mot de passe et à plusieurs facteurs.

Des technologies et approches basées sur l'authentification continue et adaptative, qui réduisent le délai de détection des imposteurs, arrivent progressivement sur le marché. Les technologies qui déplacent en toute sécurité le lieu de stockage des données personnelles hors du stockage centralisé, parfois limité par l'infrastructure du réseau, vers les appareils mobiles contrôlés par les utilisateurs, progressent. Ces nouvelles approches, qui seront disponibles à grande échelle au cours des prochaines années, permettront de faire face aux menaces émergentes.

4.1 Section des exemples de mise en œuvre

La section 8 du présent rapport contient des descriptions de systèmes mis en œuvre qui couvrent deux cas d'utilisation des DFS: Inscription/ouverture de compte et authentification pour accéder à un DFS. Chacun des deux cas d'utilisation traite de l'identification d'une personne: le premier aborde la gestion d'une situation dans laquelle le système de DFS interagit avec elle pour la première fois; le second l'authentifie à l'aide des identifiants émis précédemment. Pour gérer efficacement les risques d'erreur d'identification, les fournisseurs de DFS doivent s'assurer que les processus d'inscription et d'authentification des identifiants sont effectués avec rigueur au moyen de méthodes et de technologies normalisées.

5 Normes et réglementations applicables en matière d'authentification forte

L'un des principaux objectifs des systèmes d'authentification est d'accroître la fiabilité de l'identité de l'utilisateur préalablement inscrit afin que celui-ci puisse être régi par la politique de contrôle d'accès et d'autorisation au terme de l'authentification.

Pour se conformer aux différentes étapes des systèmes de gestion des identités, il est nécessaire de garantir la sécurité de leur processus d'authentification. Le contrôle de l'identité joue par ailleurs un rôle important dans le cadre du processus d'attribution d'identifiants. La garantie de sécurité apportée par le processus de vérification détermine la nature de l'identifiant émis. Ce processus peut en outre permettre à la partie utilisatrice de prendre des décisions relatives au contrôle des accès.

Les travaux initiaux du NIST, de l'UIT et de l'ISO ont consisté à définir quatre niveaux de garantie des entités. Ces niveaux portent notamment sur le contrôle de l'identité et l'attribution d'identifiants. Les enseignements tirés des mises en œuvre ont mis en évidence que la garantie conjointe de la sécurité de l'authentification et du contrôle de l'identité présentait quelques lacunes, notamment concernant la vérification de l'accès par une seule entité – à laquelle la vérification de l'identité du véritable demandeur aurait pu se substituer. C'est pourquoi les nouvelles versions de la publication NIST 800-63 ont séparé les différents niveaux de garantie du contrôle d'identité des niveaux d'attribution d'identifiants et ont encouragé l'adoption de trois niveaux au lieu des quatre initiaux. Les normes UIT X.1254 et ISO 29115, afin de tenir compte des travaux du NIST, font en ce moment l'objet de mises à jour.

Un récent rapport du Groupe d'action financière [3] livre un aperçu exhaustif des solutions qui peuvent être adoptées afin de répondre aux exigences de contrôle d'identité.

Cette section décrit les normes relatives à l'authentification forte ainsi que les technologies d'authentification qui en prennent en charge les mécanismes.

5.1 Recommandation UIT-T X.1254

La recommandation UIT-T X.1254, *Cadre de garantie d'authentification d'entité* [4], décrit un modèle de garantie de sécurité d'authentification que les fournisseurs de services et les fournisseurs d'authentification peuvent utiliser pour faire part de leurs attentes et communiquer au sujet des mécanismes d'authentification disponibles. Le modèle de garantie d'authentification comprend actuellement quatre niveaux croissants de garantie. De nombreuses données de base sont utilisées pour déterminer le niveau de garantie des méthodes d'authentification. La norme UIT-T X.1254 en cours de révision alignera son modèle de garantie sur le modèle à trois niveaux de la publication spéciale 800-63-3 du NIST. Il est important de noter que la norme ISO 29115 [5] est équivalente à la norme UIT-T X.1254. La norme ISO 29115 en cours de révision inclura les dernières mises à jour de la publication 800-63 du NIST.

Lors de la phase d'authentification de l'entité, celle-ci utilise son identifiant pour attester de son identité auprès d'une partie utilisatrice. Le processus d'authentification vise uniquement à établir la fiabilité du processus de revendication ou d'assertion d'identité, et n'a aucun rapport avec les mesures que la partie utilisatrice peut choisir de prendre sur la base de cette revendication ou assertion.

Technical			Management and organizational
Enrolment phase	• Application and initiation • Identity proofing and identity information verification	• Record-keeping/recording • Registration	• Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities
Credential management phase	• Credential creation • Credential pre-processing • Credential issuance • Credential activation • Credential storage	• Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping	
Entity authentication phase	• Authentication • Record-keeping		

Figure 2 – Recommandation UIT-T X.1254

La section 10.3 de la recommandation UIT-T X.1254 décrit les menaces auxquelles la phase d'authentification est exposée ainsi que les dispositifs de contrôle y afférents.

5.2 Publication spéciale 800-63-3 du NIST

La publication spéciale 800-63B du NIST intitulée *Digital Identity Guidelines Part B* (Lignes directrices pour l'identité numérique, partie 1) [6] traite de la manière dont un individu peut s'authentifier à l'aide d'un système d'authentification. Tout comme la recommandation UIT-T X.1254, le document du NIST indique l'efficacité relative des authenticateurs et des protocoles d'authentification au moyen de niveaux de garantie.

Tableau 1 – Niveaux de garantie de l'authentificateur de la publication spéciale du NIST 800-63-3

Niveau de garantie de sécurité de l'authentificateur	Description
AAL1	AAL1 fournit une certaine garantie que le demandeur contrôle un authentificateur lié au compte de l'abonné. AAL1 requiert qu'une authentification à un ou plusieurs facteurs soit effectuée au moyen d'une des nombreuses technologies d'authentification disponibles. Pour que l'authentification soit réussie, le demandeur doit prouver qu'il possède et contrôle l'authentificateur par le biais d'un protocole d'authentification sécurisé.
AAL2	AAL2 fournit une forte garantie que le demandeur contrôle le ou les authentificateurs liés au compte de l'abonné. La preuve de la possession et du contrôle de deux facteurs d'authentification distincts est requise par un ou plusieurs protocoles d'authentification sécurisés. Des techniques de chiffrement approuvées sont requises à partir de la norme AAL2.
AAL3	AAL3 fournit une très forte garantie que le demandeur contrôle le ou les authentificateurs liés au compte de l'abonné. L'authentification au niveau AAL3 est basée sur la preuve de la possession d'une clé par le biais d'un protocole de chiffrement. L'authentification AAL3 DOIT utiliser un authentificateur matériel ainsi qu'un authentificateur à l'épreuve de l'usurpation d'identité du vérificateur; le même appareil PEUT remplir ces deux conditions. Afin de s'authentifier au niveau AAL3, les demandeurs DOIVENT prouver qu'ils possèdent ou contrôlent deux facteurs d'authentification distincts par le biais d'un ou de plusieurs protocoles d'authentification sécurisés. Des techniques de chiffrement approuvées sont requises.

La publication énumère les types d'authentificateurs ainsi que les capacités des protocoles d'authentification acceptables à chaque niveau de garantie.

5.3 Règlement sur les eIDAS

Le règlement (UE) N° 910/2014¹ sur l'identification électronique et les services de confiance pour les transactions électroniques (règlement eIDAS) fournit un cadre réglementaire d'interaction électronique sécurisée entre entreprises, citoyens et autorités publiques aux membres de l'Union européenne. Il consiste notamment à décrire les niveaux de garantie de l'identification électronique. Les niveaux de garantie de sécurité du règlement eIDAS remplissent les mêmes fonctions que celles de la recommandation X.1254 et de la publication spéciale 800-63-3 du NIST.

5.4 Directives sur les services de paiement

La directive sur les services de paiement 2 (DSP2) est en vigueur en Europe, et l'authentification forte du client (SCA) sera requise pour accéder aux comptes bancaires en vue d'agréger des informations ou d'initier un paiement. Les normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication (RTS) publiées par l'Autorité bancaire européenne décrivent les principes ainsi que les exigences de l'authentification à plusieurs facteurs et de la génération de codes d'authentification.

¹ http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

Les RTS comprennent les exigences suivantes:

- Les utilisateurs doivent s'authentifier au moyen d'une authentification à deux facteurs au minimum.
- L'authentification d'un utilisateur doit aboutir à la génération d'un code d'authentification, qui constitue la signature cryptographique de la transaction. Le code d'authentification doit, dans le cas des paiements à distance, être relié au montant et au bénéficiaire approuvés par l'utilisateur.
- Le matériel cryptographique de l'utilisateur doit être protégé de toute divulgation non autorisée.

5.5 L'Alliance ID2020

L'Alliance ID2020 [7] est un partenariat public-privé qui s'engage à améliorer la vie des usagers grâce à l'identité numérique. Constituée d'institutions internationales, d'organisations à but non lucratif, d'organisations philanthropiques, d'entreprises et de gouvernements, son but est d'établir des normes techniques qui garantissent la sûreté, la sécurité et l'interopérabilité de l'identité numérique détenue et contrôlée par l'utilisateur. Elle finance des projets pilotes à fort impact qui mettent l'identité numérique à la portée des populations vulnérables, et utilise les données générées pour trouver des solutions évolutives ainsi qu'éclairer l'élaboration de politiques publiques en la matière.

L'objectif global de l'Alliance ID2020 est d'autonomiser les individus, de multiplier les opportunités économiques et de faire progresser le développement mondial en améliorant l'accès à l'identité numérique.

D'ici à 2030, l'Alliance vise à faciliter la mise à l'échelle d'un système d'identification numérique sûr, vérifiable et permanent conformément à la cible 16.9 des objectifs de développement durable des Nations Unies: "D'ici à 2030, garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances". De 2017 à 2020, le travail de l'Alliance portera sur deux axes: développer et tester les meilleures solutions technologiques d'identification numérique; et travailler avec les gouvernements ainsi que les agences en place et établies pour les mettre en œuvre.

La marque de certification ID2020 [8] est à l'initiative de l'Alliance ID2020. Son but est de reconnaître les identités numériques qui répondent à nos exigences techniques. Cette marque de certification se fonde sur les exigences techniques ID2020, qui sont régulièrement mises à jour par une équipe d'experts afin de tenir compte de l'évolution du domaine de l'identité numérique. Le formulaire de demande de marque de certification comprend 50 questions déclinées dans sept domaines d'intérêt: applicabilité, identification et vérification, authentification, confidentialité et contrôle, attestations et confiance, interopérabilité, et récupération et recours.

5.6 Objectifs de normalisation

Les normes internationales relatives aux mécanismes d'authentification forte font l'objet d'une amélioration constante. Les domaines qui nécessitent une attention supplémentaire sont les suivants:

- La modélisation comportementale
- Les points forts des authenticateurs
- Les exigences relatives aux capacités des appareils mobiles en matière de sécurité par rapport au niveau de sécurité de l'authentificateur
- Les exigences en matière d'expérience utilisateur de l'authentification forte

La Commission d'études (CE) 17 de l'UIT-T est la principale commission d'études portant sur la gestion des identités. Actuellement, le Groupe du rapporteur pour la Question 10/17 met à jour la Recommandation UIT-T X.1254 "Garantie d'authentification des entités" afin de tenir compte des récentes modifications de la publication spéciale 800-63-3 du NIST "Digital Identity Guidelines".

En outre, les protocoles FIDO UAF 1.1 et FIDO CTAP ont été normalisés par la Commission d'études 17 avec la rédaction des recommandations UIT-T X.1277 et UIT-T X.1278.

Les travaux présentés dans ce rapport ont été rédigés en vue d'être soumis au Groupe du rapporteur pour la Question 10/17 de la CE 17 de l'UIT-T et d'être normalisés plus avant dans le cadre des travaux X.1254, X.1277 et X.1278.

6 Technologies et spécifications d'authentification forte

Pour être opérationnels, les systèmes d'authentification requièrent l'intervention des utilisateurs, leurs identifiants ainsi que les authenticateurs qu'ils utilisent afin de prouver qu'ils sont les destinataires originaux enregistrés de l'identifiant. Les protocoles d'authentification définissent la façon dont chaque élément interagit lors de l'authentification de ces individus. Chaque élément présente des comportements observables ou mesurables dans l'environnement, lesquels peuvent être comparés au comportement "normal" déterminé précédemment.

Les choix de conception et les choix techniques relatifs à chaque élément du système d'authentification ont une incidence sur sa résistance aux attaques ainsi qu'aux altérations de sécurité dues aux menaces courantes. Les systèmes d'authentification forte ont été pensés pour atténuer les menaces que les systèmes d'authentification faibles ne sont pas en mesure de contourner.

Par exemple, les utilisateurs jugent les systèmes de mots de passe contraignants. Les mots de passe sont difficiles à retenir, faciles à voler, réutilisés d'un service à l'autre et très peu pratiques à utiliser. Afin d'éliminer le recours aux mots de passe et de réduire les contraintes de l'utilisateur, les systèmes d'authentification forte peuvent conditionner l'ouverture d'un coffre-fort local et sécurisé de clés de chiffrement à l'utilisation de la biométrie.

Les authenticateurs tels que les codes à usage unique délivrés par SMS, qui sont sujets au hameçonnage, pourraient être remplacés par des authenticateurs cryptographiques matériels placés dans les appareils mobiles; par exemple, un élément sécurisé ou un environnement d'exécution fiable.

Les protocoles d'authentification qui utilisent des secrets partagés ou des transmissions non chiffrées pourraient être remplacés par des protocoles de chiffrement à clé asymétrique, des canaux chiffrés et un système de clé par service. Les protocoles d'authentification à plusieurs facteurs résistent davantage aux attaques que les protocoles à facteur unique.

Les concepteurs doivent tenir compte du fait que les menaces évoluent constamment, qu'elles soient nouvelles ou courantes. Par exemple, les menaces relatives à l'accès à un site Web depuis un

ordinateur de bureau diffèrent de celles qui pèsent sur les applications et services exclusivement mobiles inventés ces dernières années.

6.1 Caractéristiques des systèmes d'authentification avancée

Les systèmes d'authentification traditionnels utilisés aujourd'hui correspondent aux besoins de l'Internet antérieur aux appareils mobiles. Ils sont basés sur un événement d'authentification unique généralement effectué au démarrage de l'application, au terme duquel il est supposé que l'utilisateur, l'appareil et la session ne changent pas. L'authentification est une activité généralement contraignante qui offre une expérience utilisateur médiocre, en particulier lorsqu'elle requiert l'utilisation d'un mot de passe ou d'une authentification à plusieurs facteurs. Les utilisateurs mobiles rencontrent des difficultés à utiliser les systèmes d'authentification de dernière génération. En effet, les événements d'authentification des appareils mobiles sont peu fréquents et dépendent de leur système de verrouillage, dont l'efficacité n'est pas toujours avérée.

Les systèmes d'authentification avancée ont été conçus en adéquation avec les modèles de menaces et de conception actuels. Par rapport aux systèmes d'authentification forte, qui utilisent un logiciel client d'analyse environnementale et comportementale, l'accent est davantage mis sur la détection et l'authentification des utilisateurs humains. De nouvelles approches sont mises en œuvre pour minimiser les contraintes lors de l'authentification mobile et à plusieurs facteurs. De nombreux systèmes sont par ailleurs principalement axés sur les technologies mobiles. L'authentification s'effectue désormais à différents moments de l'interaction entre l'utilisateur et le système: au moment de l'identification, lors de la sollicitation de privilèges supplémentaires (l'authentification dite "par paliers"), et même en continu tout au long de la session.

Les systèmes d'authentification avancée ne remplacent pas les systèmes d'authentification forte – ces technologies forment un dispositif conjoint de défense aux différentes menaces et vulnérabilités.

L'objectif des systèmes d'authentification avancée est de réduire les contraintes d'utilisation des utilisateurs tout en atténuant les risques auxquels ces derniers s'exposent ainsi qu'en augmentant leur garantie de sécurité.

Tableau 2 – Caractéristiques des systèmes d'authentification avancée

Caractéristiques des systèmes d'authentification avancée	Description
Élimination ou réduction de la dépendance aux mots de passe	Les utilisateurs rencontrent des difficultés à s'authentifier par mot de passe, notamment sur les appareils mobiles. Les systèmes de mots de passe sont de plus en plus vulnérables aux violations de bases de données et au hameçonnage.
Authentification multimodale des utilisateurs	L'étape d'authentification propose plusieurs modes d'authentification afin de minimiser les contraintes des utilisateurs. Par exemple, par application mobile, par formulaire Web, par mise en correspondance biométrique, par mot de passe ou par réponse vocale.
Analyse en temps réel du comportement de l'utilisateur pour détecter les anomalies	Détection d'anomalies incompatibles avec le mode d'accès, comme le basculement d'une session utilisateur d'un lieu géographique à un autre, l'utilisation d'un appareil non enregistré ou le changement de navigateur Web en cours de session.
Authentification continue de l'utilisateur, du logiciel et de l'appareil	Les techniques d'authentification continue interrogent l'utilisateur, le logiciel ou l'appareil tout au long de la session dans le but d'obtenir des réponses valides. Certaines techniques d'authentification continue sont invisibles par l'utilisateur, notamment au niveau de l'appareil et du logiciel.
Évaluation dynamique des risques liés à la confiance témoignée au processus d'authentification	La confiance dans le processus d'authentification tient compte de plusieurs facteurs tels que les capacités de l'appareil, la transaction demandée ainsi que le degré de sécurité des authenticateurs.
Cohérence sur tous les appareils et canaux choisis par l'utilisateur	Les systèmes d'authentification sont conçus pour optimiser l'expérience utilisateur et la sécurité. Les utilisateurs se connectent aux services à l'aide du canal qui leur convient le mieux. Les systèmes d'authentification doivent garantir la fiabilité du processus d'authentification, quel que soit le canal utilisé.

La section 7.1 "Authentification cognitive continue" comporte la description d'une solution qui rassemble les caractéristiques du système d'authentification avancée mentionné.

6.2 Spécifications de l'Alliance FIDO

Les protocoles de l'Alliance FIDO utilisent des techniques standard de chiffrement à clé publique afin de renforcer le processus d'authentification. Lors d'une inscription à un service en ligne, l'appareil client de l'utilisateur crée une nouvelle paire de clés. Il conserve la clé privée et enregistre la clé publique auprès du service en ligne. L'authentification est effectuée par l'appareil client, qui signe une récusation afin d'apporter au service la preuve de la possession de la clé privée. Les clés privées du client ne peuvent être utilisées qu'après avoir été déverrouillées localement sur l'appareil par l'utilisateur. On nomme cette opération la "vérification de l'utilisateur". La vérification de l'utilisateur peut nécessiter un certain nombre d'actions simples et sécurisées, comme faire glisser un doigt sur l'écran, effectuer une reconnaissance faciale, saisir un code PIN ou parler dans le microphone de l'appareil. Les clés privées, liées à l'appareil, prouvent que l'utilisateur est en sa possession (c'est la

partie "propriétaire" de l'authentification). De pair avec la vérification de l'utilisateur, elles garantissent la qualité multifactorielle de chaque authentification.

Les protocoles FIDO ont pour but de protéger la vie privée des utilisateurs. Ils ne fournissent pas d'informations susceptibles d'être utilisées par différents services en ligne pour suivre un utilisateur d'un service à l'autre. Les informations biométriques, si elles sont utilisées, ne quittent jamais l'appareil de l'utilisateur et ne sont utilisées que dans le cadre de la vérification de l'utilisateur en vue d'approuver l'utilisation d'une clé privée.

Les entreprises qui souhaitent mettre en œuvre des processus d'authentification qui ne fonctionnent pas par mot de passe doivent généralement prendre en charge un nombre considérable de clients et de protocoles propriétaires.

Afin d'établir l'interopérabilité des méthodes d'authentification des clients, la FIDO normalise les couches au niveau des clients et des protocoles. Ainsi, de nombreuses méthodes d'authentification des clients telles que la biométrie, les codes PIN et les authentifications à deux facteurs peuvent être utilisées avec de multiples services en ligne de manière interopérable.

Les principales spécifications de la FIDO sont le deuxième facteur universel (U2F) [5], le cadre d'authentification universelle (UAF) [6] et le projet FIDO2, qui comprend le protocole client-authentificateur (CTAP) [7] et l'authentification Web (WebAuthn) du W3C [9].

Le projet FIDO2 est un ensemble d'initiatives imbriquées qui visent à établir une norme d'authentification FIDO pour le Web et étendent considérablement l'écosystème FIDO.

FIDO2 comprend la spécification d'authentification Web (WebAuthn) du W3C ainsi que le protocole client-authentificateur (CTAP) correspondant de la FIDO. De pair, ils permettront aux utilisateurs d'utiliser leurs appareils pour s'authentifier facilement auprès de services en ligne aussi bien dans des environnements mobiles que de bureau.

6.2.1 Cadre d'authentification universelle

L'objectif du cadre d'authentification universelle est de fournir un cadre large et complet d'authentification à plusieurs facteurs sécurisée par des technologies de chiffrement. Celui-ci comprend le premier facteur (par exemple, le code PIN et la biométrie), le second facteur, ainsi qu'une architecture et un protocole généralisés qui peuvent être étendus à n'importe quelle plateforme ou intégrés à n'importe quel système.

La spécification UAF normalise quatre éléments:

1. L'authentificateur, un appareil qui crée et stocke de manière sécurisée les secrets d'authentification.
2. Le serveur, qui enregistre les utilisateurs et valide ensuite les demandes d'authentification.
3. Le client, qui joue le rôle de multiplexeur et applique les politiques d'usage entre plusieurs serveurs et authentificateurs.
4. Le protocole, qui définit les formats de message, les objets cryptographiques, etc. qui circulent entre l'authentificateur et le serveur par l'intermédiaire du client.

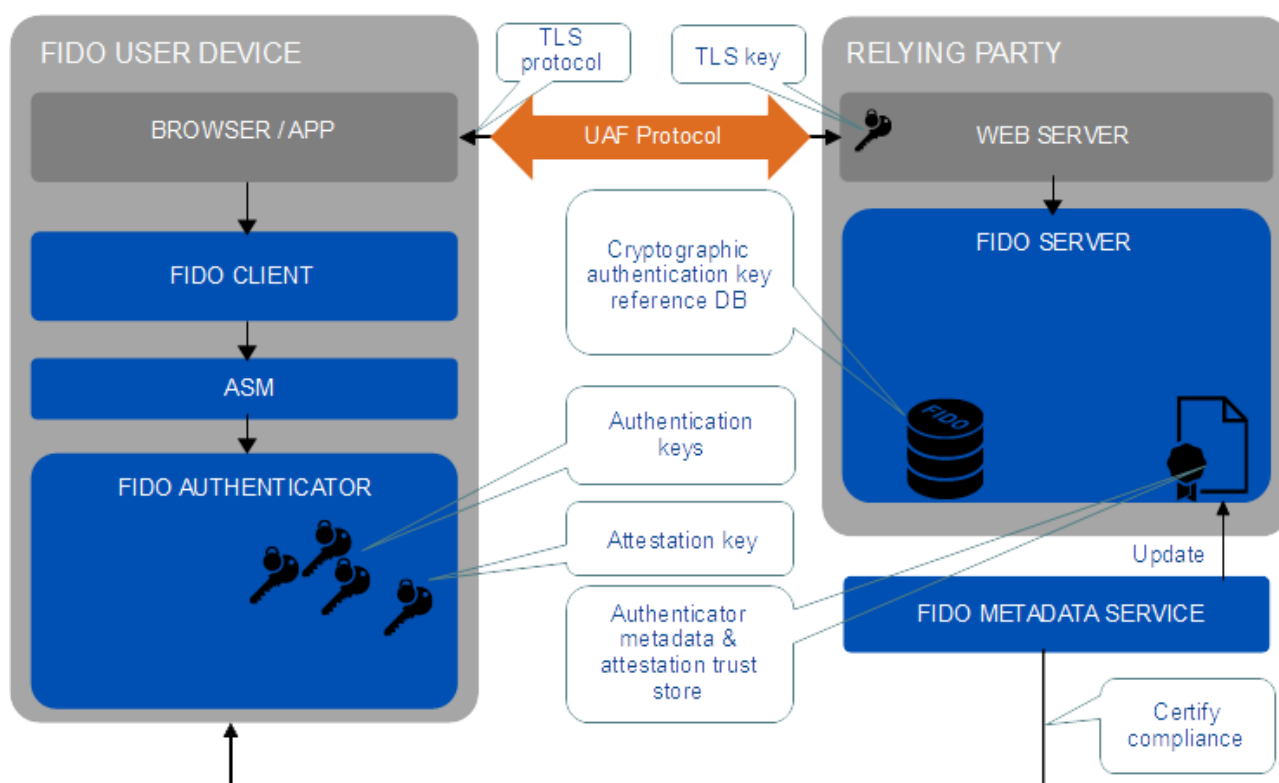


Figure 3 – Architecture du cadre d'authentification universelle

Cette architecture est réutilisée par les autres spécifications de la FIDO.

6.2.2 Deuxième facteur universel

La spécification FIDO U2F vise précisément à intégrer l'authentification à second facteur aux navigateurs. Elle définit une API JavaScript qui permet aux navigateurs d'effectuer une authentification à second facteur à l'aide des fonctions JavaScript `register()` et `sign()`. Elle définit également des protocoles de communication NFC, Bluetooth Low Energy (BLE) et USB afin que les processus d'enregistrement et d'authentification puissent être effectués avec des clés de sécurité. Ces spécifications améliorent l'expérience utilisateur et renforcent la sécurité de l'authentification à second facteur.

Remarque: L'API JavaScript FIDO U2F a été remplacée par WebAuthn et les spécifications de transport pour NFC, BLE et USB ont été fusionnées dans les dernières spécifications FIDO CTAP.

6.2.3 Protocole client-authenticateur

La spécification CTAP décrit un ensemble de protocoles de communication entre plusieurs dispositifs d'authentification externes et un client ou une plateforme, ainsi que les liens entre ce protocole d'application et un ensemble de protocoles de transport utilisant différents protocoles relatifs à la communication entre appareils (USB, NFC, Bluetooth). Chaque liaison de transport définit en détail la manière dont un client (tel qu'un navigateur ou un système d'exploitation) peut adresser des demandes à un dispositif d'authentification dans le but de s'enregistrer ou de s'authentifier auprès de divers services.

CTAP, par exemple, sert lorsqu'un utilisateur interagit avec une partie utilisatrice (un site Web ou une application native) sur une plateforme (par exemple, un PC) qui l'invite à interagir à son tour avec un authentificateur externe (par exemple, un smartphone).

Afin de fournir une preuve de l'interaction de l'utilisateur, tout authenticateur externe chargé de mettre en œuvre ce protocole est censé disposer d'un mécanisme permettant d'inviter l'utilisateur à interagir. Exemples d'interactions de l'utilisateur : bouton de consentement, mot de passe, code PIN, données biométriques ou une combinaison de ces éléments.

La spécification CTAP a été créée dans le cadre du projet FIDO2 conjointement avec la spécification WebAuthn. Elle contient deux protocoles distincts: 1) les protocoles de transport U2F d'origine, qui permettent aux dispositifs d'authentification d'effectuer l'authentification à second facteur, nommés rétroactivement "CTAP1"; 2) un ensemble étendu et reformaté de protocoles de transport U2F qui rendent possible l'authentification à plusieurs facteurs, nommé "CTAP2".

6.2.4 Authentification Web

L'Alliance FIDO a collaboré avec le World Wide Web Consortium (W3C) dans le cadre du projet FIDO2 en vue de normaliser les API JavaScript pour navigateurs chargées d'effectuer une authentification forte à plusieurs facteurs en s'appuyant sur des technologies de chiffrement – il s'agit de l'authentification Web. La spécification WebAuthn est une recommandation proposée par le W3C. Elle comprend à la fois des éléments d'authentification spécifiques au navigateur (API et règles de traitement du navigateur) et des formats de message génériques (assertions et attestations) qui peuvent être réutilisés dans le cadre d'implémentations non relatives au navigateur – par exemple, de serveurs, de systèmes d'exploitation et d'authentificateurs communiquant à l'aide du protocole CTAP. La spécification WebAuthn définit également un ensemble d'éléments extensibles. Elle offre notamment la possibilité d'ajouter de nouveaux formats d'attestation ainsi que de nouvelles extensions du protocole et de définir leurs règles de traitement.

6.2.5 Flux d'enregistrement FIDO

La figure ci-dessous montre les flux de messages simplifiés d'enregistrement et d'authentification. Remarque: la paire de clés publique-privée est créée par l'authentificateur FIDO, et non par la partie utilisatrice. Ainsi, l'individu détermine la manière dont il souhaite être connu de la partie utilisatrice et ne divulgue aucune partie de la clé privée aux systèmes externes.

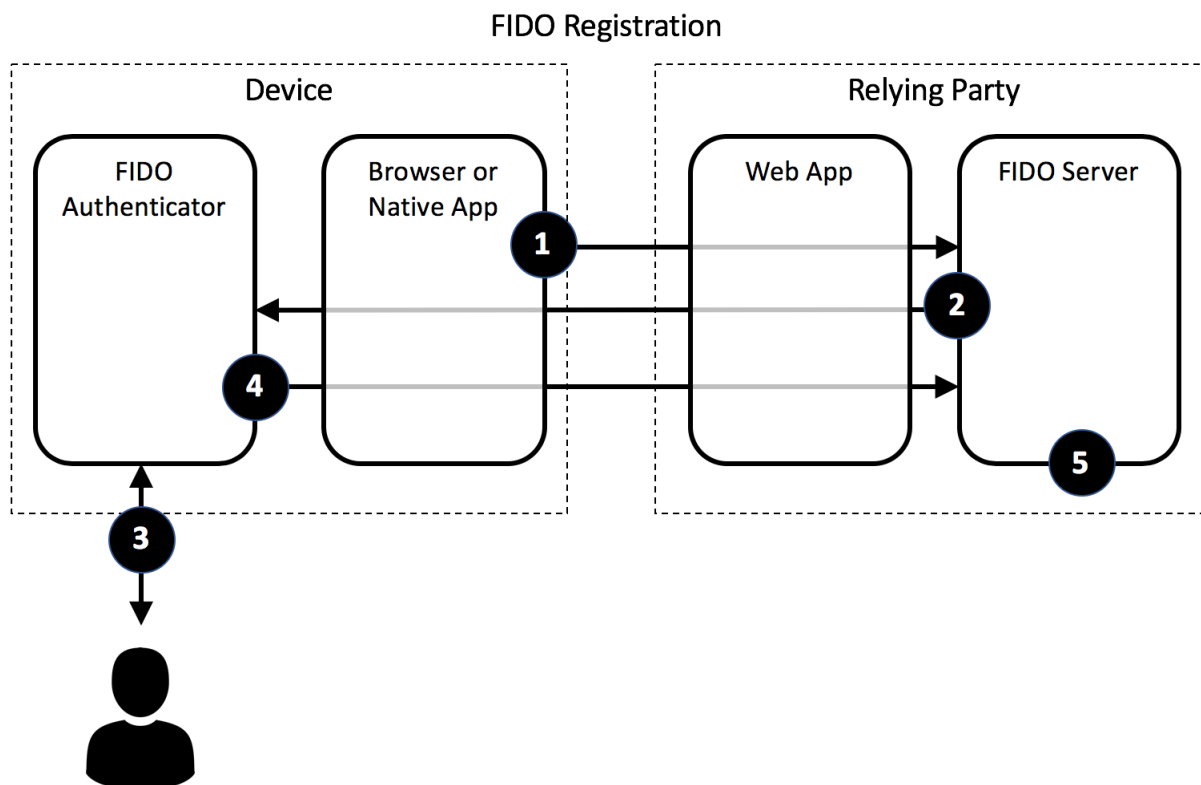


Figure 4 – Enregistrement FIDO de nouvelles clés

1. Lancement de l'enregistrement auprès de la partie utilisatrice
2. Le serveur FIDO envoie une récusation d'enregistrement ainsi que les options d'enregistrement demandées.
3. L'authentificateur effectue une vérification de l'utilisateur sur l'appareil afin de signaler son consentement à s'enregistrer auprès du service.
4. L'authentificateur génère une nouvelle paire de clés pour le service en question et associe la clé privée à l'origine du service. La clé publique et le numéro de modèle de l'appareil sont signés par une clé privée d'attestation spécifique au modèle de l'appareil (partagée par au moins 100 000 appareils). L'authentificateur envoie une réponse d'enregistrement: numéro de modèle de l'appareil + signature d'attestation de l'appareil + clé publique de l'utilisateur.
5. Validation de la réponse et de l'attestation. Le numéro de modèle de l'appareil (identificateur global unique de l'attestation de l'authentificateur) peut être utilisé pour rechercher des métadonnées à son sujet, telles que la clé publique d'attestation, le type de vérification de l'utilisateur effectuée (par exemple, biométrie, PIN) et les caractéristiques de sécurité de l'appareil (par exemple, la manière dont les clés privées et les modèles biométriques sont protégés, ou encore les certifications de sécurité et biométriques tierces).
6. Le service stocke la clé publique de l'utilisateur à des fins d'authentification ultérieure.

6.2.6 Flux d'authentification FIDO

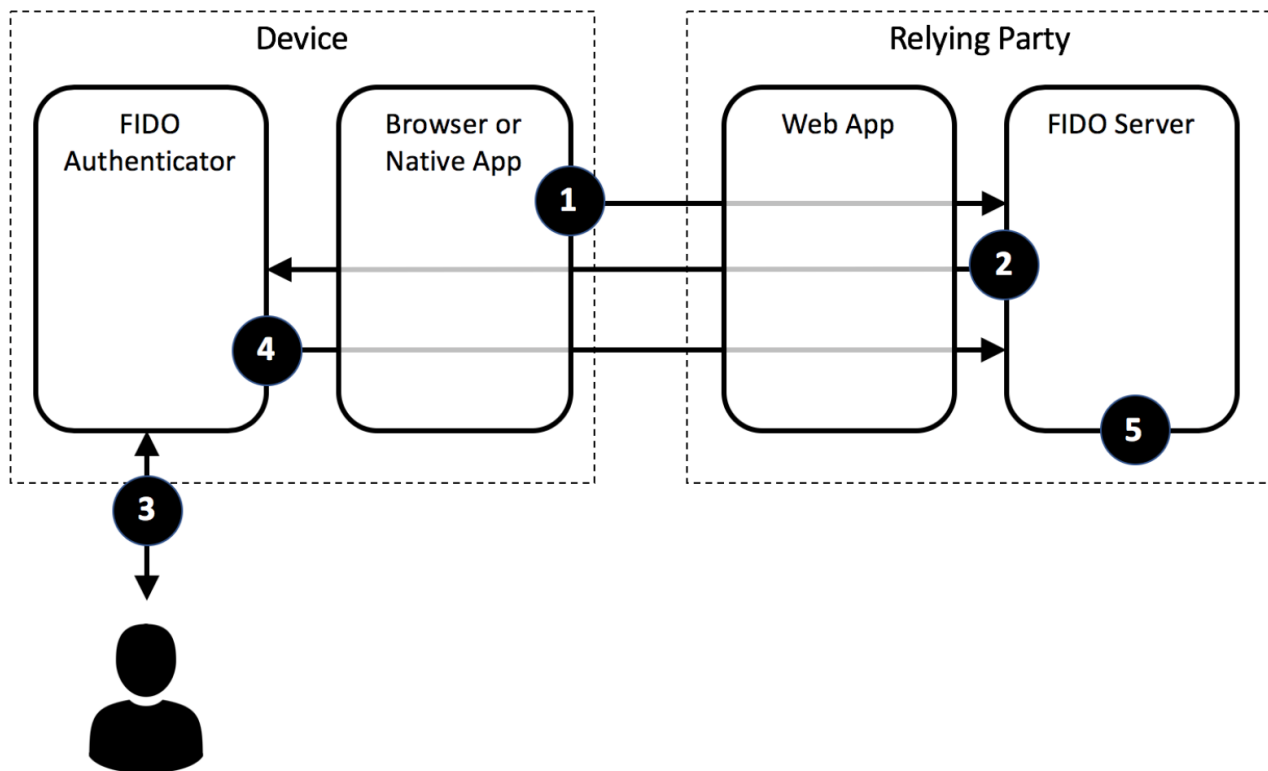


Figure 5 – Authentification FIDO

1. Initiation de l'authentification avec la partie utilisatrice.
2. Le serveur FIDO envoie la récusation d'authentification ainsi que les préférences en matière d'authentificateurs ou d'identifiants.
3. L'authentificateur effectue une vérification de l'utilisateur sur l'appareil afin de signaler son consentement à s'authentifier auprès du service.
4. L'authentificateur utilise la clé d'origine du service pour rechercher la clé privée d'authentification, qu'il utilise à son tour pour signer la récusation du serveur. Le serveur envoie une réponse d'authentification: récusation + signature.
5. Le serveur récupère la clé publique de l'utilisateur et valide la signature de la récusation.

Des rapports ainsi que des livres blancs élaborés par l'Alliance FIDO prodiguent des conseils de mise en œuvre, notamment concernant les applications de services financiers. Plusieurs rapports pertinents à cet égard sont énumérés à l'annexe B du présent rapport.

6.3 Spécifications de Mobile Connect

Le développement de la solution d'identification universelle sécurisée Mobile Connect a été facilité par les opérateurs mobiles et réalisé en collaboration avec la GSMA. La GSMA représente les intérêts de près de 800 opérateurs de téléphonie mobile dans le monde ainsi que de plus de 230 entreprises de l'écosystème mobile au sens large. À ce jour, Mobile Connect, par l'intermédiaire de plus de 70 opérateurs couvrant plus de 40 pays et plus de 3 milliards de personnes, compte plus de 470 millions d'utilisateurs actifs.

Mobile Connect est un portefeuille de services mobiles qui peuvent être intégrés à l'application d'un fournisseur de services afin de faciliter l'accès à ses services. Mobile Connect garantit la sécurité de l'authentification ainsi que de l'autorisation du client et lui accorde l'accès à l'identité de l'utilisateur ainsi qu'aux attributs contextuels du réseau. La figure 6 décrit la gamme de services fournis par Mobile Connect.

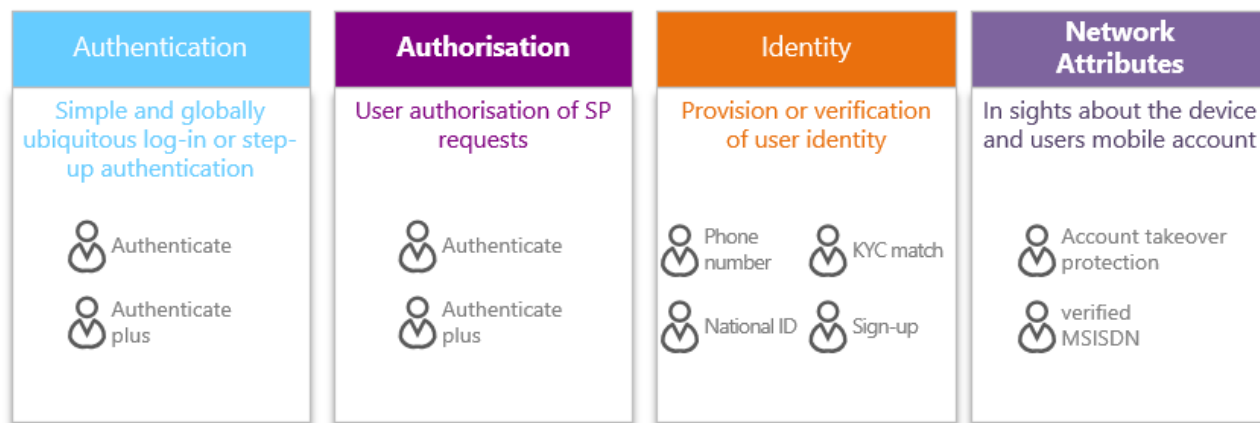


Figure 6 – Gamme de services de Mobile Connect

Mobile Connect est basé sur une architecture distribuée au sein de laquelle chaque opérateur mobile déploie les services Mobile Connect dans sa propre base d'utilisateurs. Tous ces déploiements respectent néanmoins un ensemble strict de normes techniques afin d'assurer la cohérence de l'expérience d'utilisation des services Mobile Connect avec n'importe quel opérateur mobile du point de vue du fournisseur de services.

Mobile Connect est basé sur le protocole OpenID Connect (OIDC), qui appose une couche d'identité sur le protocole OAuth 2.0. Il donne la possibilité aux utilisateurs d'être identifiés par leur MSISDN (ou toute autre référence client pseudonyme associée) et d'être authentifiés de manière sécurisée par leur appareil mobile grâce à leur carte SIM. Mobile Connect comprend deux profils OIDC qui visent à prendre en charge les demandes d'authentification, d'autorisation ou d'accès autorisé aux attributs de l'utilisateur initiées par l'appareil ou le serveur.

L'opérateur mobile concerné prend en charge et sélectionne l'authentificateur approprié afin de présenter les demandes d'authentification ainsi que d'autorisation à l'utilisateur sur son appareil mobile. Ce dernier doit par la suite y répondre. L'authentificateur peut également être utilisé pour obtenir le consentement de l'utilisateur afin que l'opérateur concerné partage ou valide les attributs de l'utilisateur avec le fournisseur de services. L'authentificateur est choisi en fonction de la politique de l'opérateur, des capacités de l'appareil et du niveau de garantie de sécurité requis.

Les facteurs d'authentification et les informations de Mobile Connect sont basés sur:

- La preuve de propriété (quelque chose que j'ai); la possession de l'appareil mobile par l'utilisateur. Il s'agit du premier facteur utilisé lors de l'authentification avec Mobile Connect.
- La connaissance/le secret (quelque chose que je sais); par exemple, le code PIN/code personnel.
- L'inhérence active (quelque chose que je suis); par exemple, biométrie: empreintes digitales, balayage de l'iris, biométrie faciale.
- L'inhérence passive (quelque chose que le réseau connaît); éléments d'inhérence basés sur le réseau mobile, tels que les sites cellulaires habituels (peuvent également être utilisés comme "quelque chose que l'utilisateur fait") à la disposition de l'opérateur mobile. Cette séparation

entre l'appareil et le réseau est essentielle pour lutter contre la fraude et établir la propriété de l'appareil.

- Contextuel (quelque chose que je fais); par exemple, compléter l'authentification basée sur l'appareil par des informations basées sur le réseau pour renforcer le mécanisme d'authentification à plusieurs facteurs (comme le statut d'appariement entre IMSI, IMEI et MSISDN).

Les niveaux de garantie de Mobile Connect indiquent le degré de confiance accordé aux processus d'authentification. Les niveaux de garantie de l'écosystème Mobile Connect sont essentiels à son fonctionnement. Ils sont utilisés dans l'API de Mobile Connect (OpenID Connect), dans le jeton d'identité à signature cryptographique envoyé comme preuve d'authentification au fournisseur de services, dans la politique de sélection des authenticateurs ainsi que dans la politique d'activation des produits Mobile Connect.

6.3.1 Mobile Connect dans le cadre des eIDAS

Les niveaux de garantie de Mobile Connect ont été mis en correspondance avec les exigences de spécifications techniques minimales du Règlement d'exécution de la Commission (UE) 2015/1502 portant sur la définition de spécifications techniques minimales et de procédures relatives aux niveaux de garantie des moyens d'identification et d'authentification électroniques.

La figure 7 illustre la mise en correspondance entre le niveau de garantie de Mobile Connect et des eIDAS.

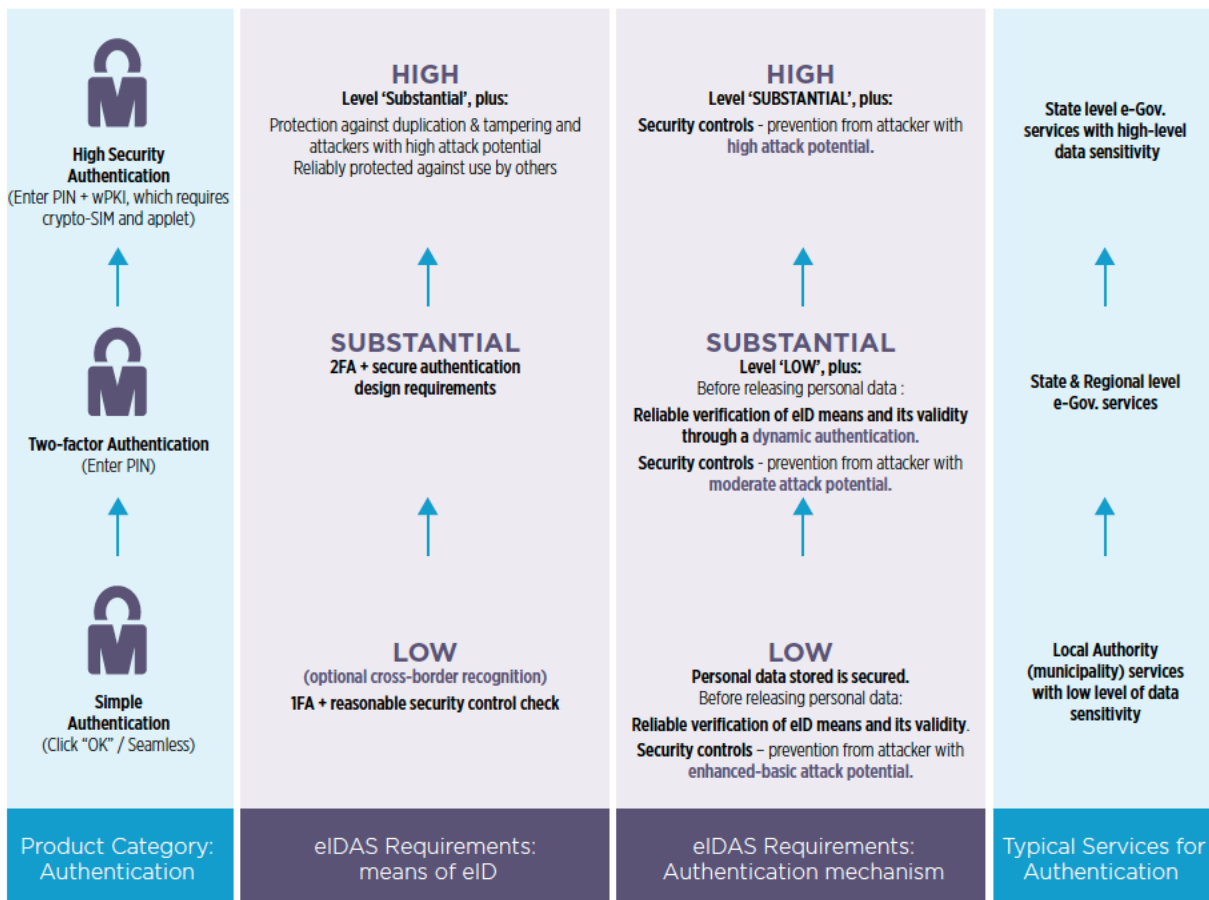


Figure 7 – Mise en correspondance des niveaux de garantie des eIDAS et de Mobile Connect

Mobile Connect répond également aux spécifications techniques ainsi qu'aux exigences d'interopérabilité des eIDAS en matière d'intégration avec l'identifiant national, telles qu'elles ont été définies par les nœuds des eIDAS des États membres de l'UE en collaboration avec le projet Mécanisme pour l'interconnexion en Europe (MIE) de la Commission européenne². La figure 8 présente un exemple d'architecture de référence des eIDAS intégrable à Mobile Connect.

² <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+eID+Profile>.

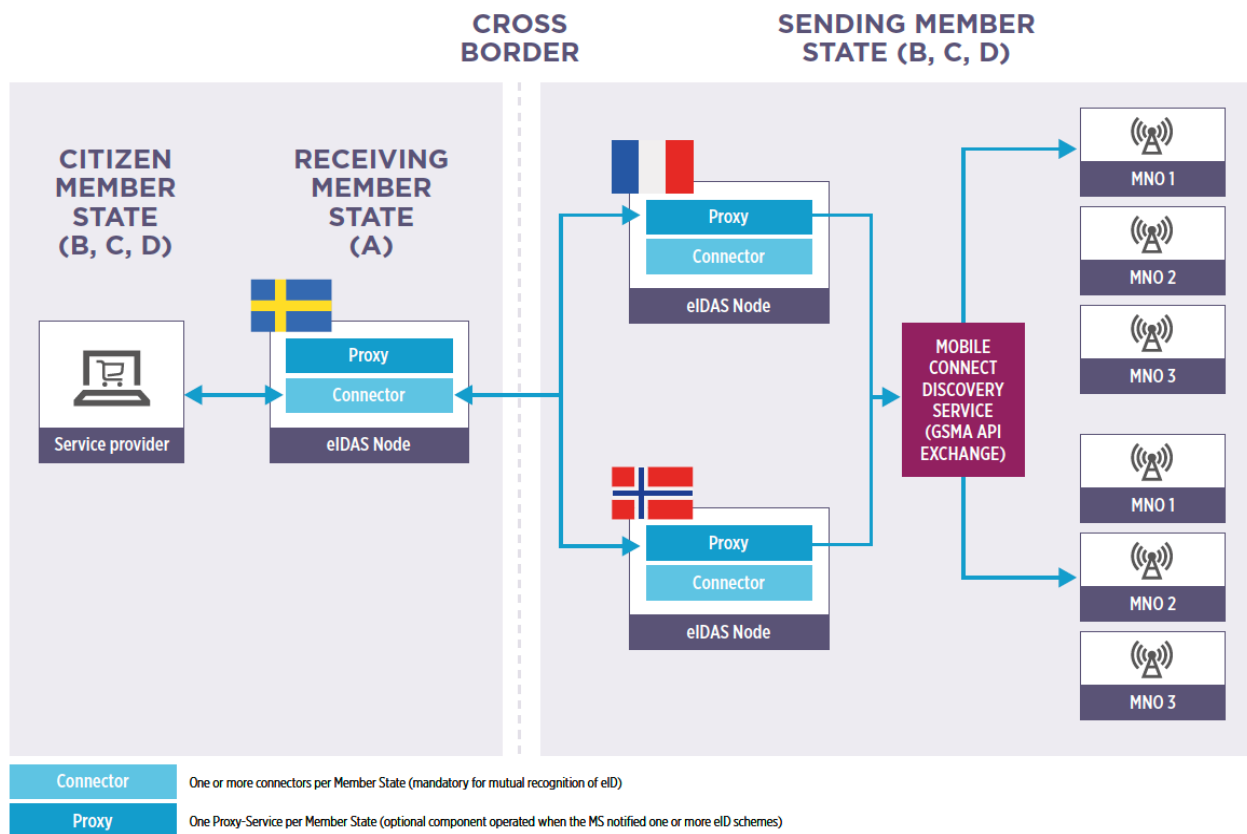


Figure 8 – Architecture de référence de Mobile Connect et des eIDAS

La figure 9 présente un organigramme de Mobile Connect utilisé dans un déploiement des eIDAS.

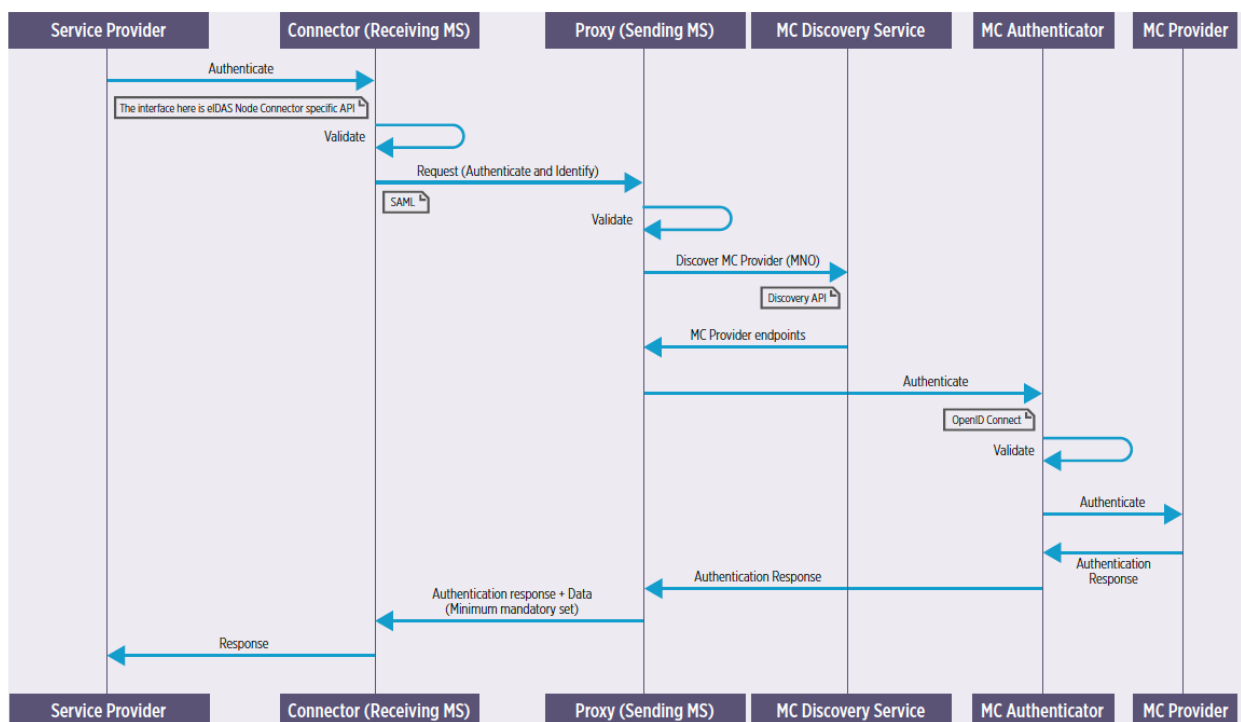


Figure 9 – Flux technique de Mobile Connect et des eIDAS

6.3.2 Mobile Connect dans le cadre de la DSP2

Dans le cadre de la DSP2, l'infrastructure de Mobile Connect utilise l'authentification hors bande; c'est-à-dire que le canal d'authentification, afin d'être entièrement conforme à la DSP2 et en plus de fournir une liaison dynamique, est séparé du canal de demande de service et utilise l'appareil mobile compatible avec la carte SIM ainsi que le support du réseau mobile. Mobile Connect peut prendre en charge la SCA aussi bien en mode découplé qu'en mode OAuth.

Les figures suivantes présentent les cas d'utilisation, l'architecture et les flux liés à la DSP2.

Scenario	Mobile Connect as Second Factor Solution (upgrade from SMS OTP)	Mobile Connect as Two-Factor Solution
Login to account	 authenticate  verified MSISDN  authenticate plus	 authenticate plus
Payment authorisation	 authorise  authorise plus	 authorise plus
Scenario	Mobile Connect providing risk factors into fraud decision engine	
Transaction risk monitoring, incl. for TRA*	 account takeover protection  verified MSISDN  KYC match	
Other products on roadmap (Proximity, Roaming...)		

*TRA: Transaction Risk Analysis exemption

Figure 10 – Cas d'utilisation de la DSP2 avec Mobile Connect

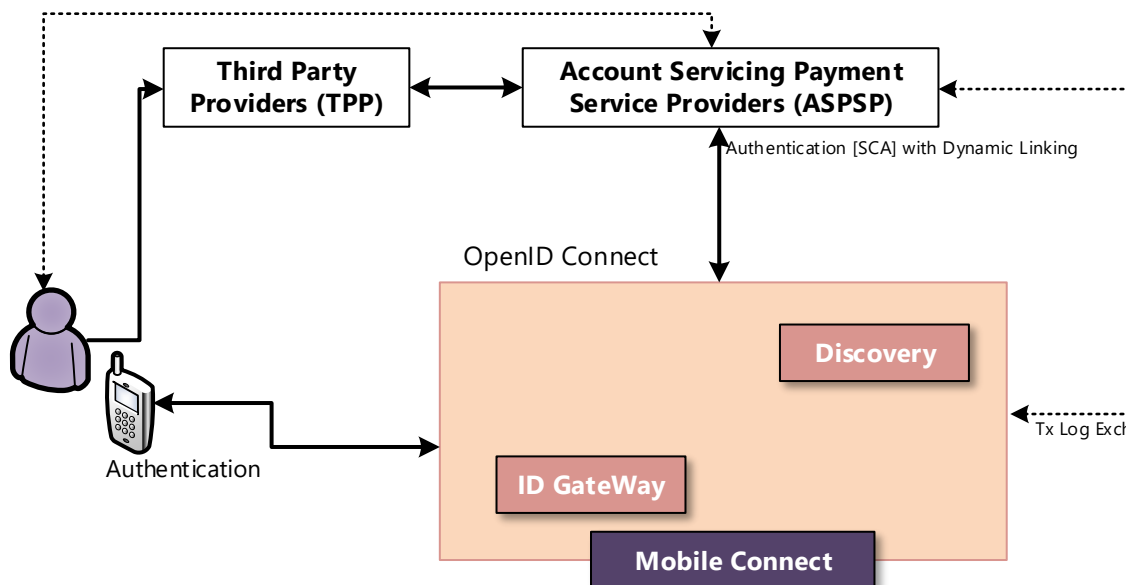


Figure 11 – Architecture de référence de haut niveau de la DSP2

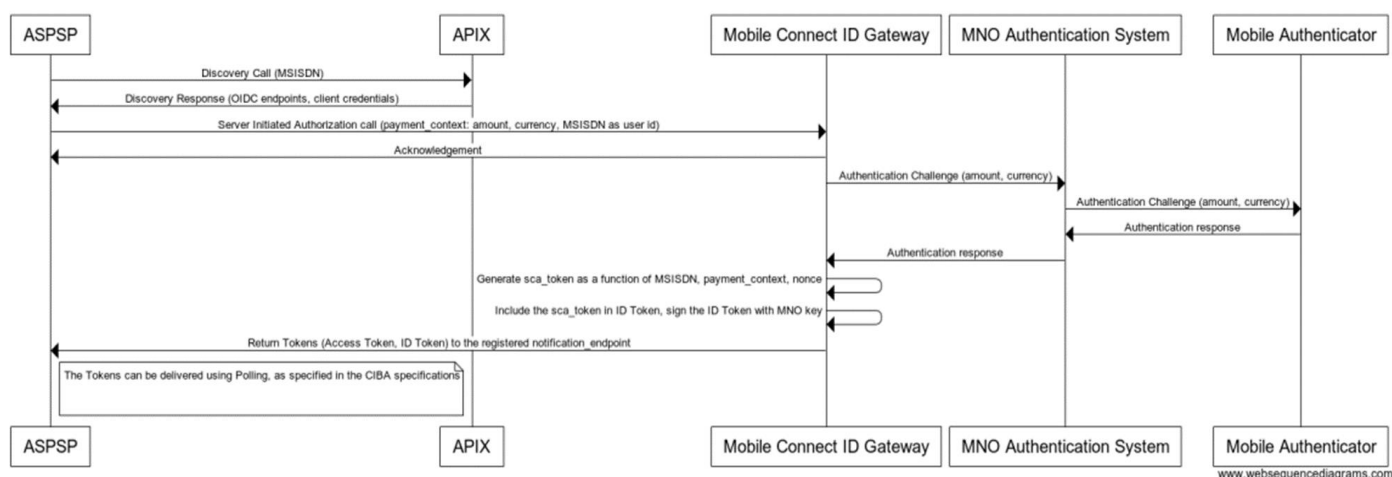


Figure 12 – Authentification forte du client avec Mobile Connect – initiée par le serveur

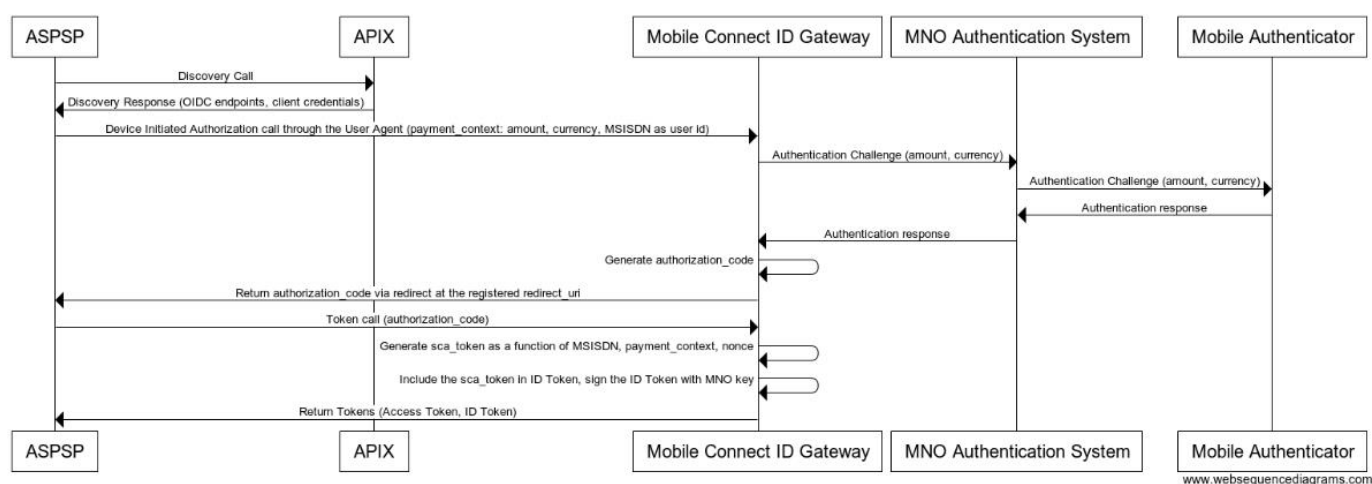


Figure 13 – Authentification forte du client avec Mobile Connect – initiée par le dispositif

D'autres informations relatives au déploiement de Mobile Connect se trouvent dans l'annexe C de ce rapport.

6.4 Spécifications IFAA

L'Internet Finance Authentication Alliance (IFAA) a été créée en juin 2015. Environ 200 entreprises et instituts internationaux membres y collaborent en vue d'innover dans le domaine de l'authentification, de définir des normes basées sur la biométrie et de fournir des solutions d'authentification interopérables pour les services financiers.

L'IFAA, en réduisant le coût de l'adaptation des appareils et en améliorant l'efficacité de l'authentification, s'efforce de relever les défis en la matière. La principale spécification de l'IFAA est la spécification technique sans mot de passe local (T/IFAA 0001-2016). Celle-ci requiert une protection stricte des données de l'utilisateur dans l'environnement d'exécution fiable. À ce jour, cette spécification a été prise en charge par plus de 1,2 milliard d'appareils mobiles et 360 modèles d'appareils. Une version actualisée de la spécification technique IFAA Local Passwordless (T/IFAA 0002-2018) a été publiée en juillet 2018. Celle-ci présentait une solution facultative de sécurité

renforcée qui consistait à utiliser un élément sécurisé pour protéger les applications, les clés et les données sensibles.

Les spécifications de l'IFAA ont favorisé l'adoption massive de l'authentification par empreinte digitale dans les secteurs du commerce électronique, de la finance numérique, des banques, du voyage, des bureaux mobiles ainsi que de l'Internet des objets. Ce mode d'authentification s'est répandu au sein des banques ces derniers mois.

L'IFAA distingue deux modèles techniques d'authentification biométrique: le modèle local et le modèle à distance. Bien que les spécifications de l'IFAA portent actuellement sur le modèle local, le modèle à distance est également au programme de l'Alliance.

6.4.1 Authentification biométrique IFAA – modèle local

Dans le modèle local, le système biométrique se trouve dans l'équipement de l'utilisateur. Les données biométriques sont collectées, stockées et comparées localement par le système biométrique lorsque l'application de l'utilisateur l'appelle. La décision d'authentification n'est toutefois pas prise au niveau local. Un identifiant est fourni sur la base des données sortantes du système biométrique local et envoyé par l'application de l'utilisateur au serveur. La décision d'authentification sera prise par le serveur d'authentification sur la base de l'identifiant fourni par l'équipement de l'utilisateur.

La figure 14 illustre l'infrastructure technique de ce modèle.

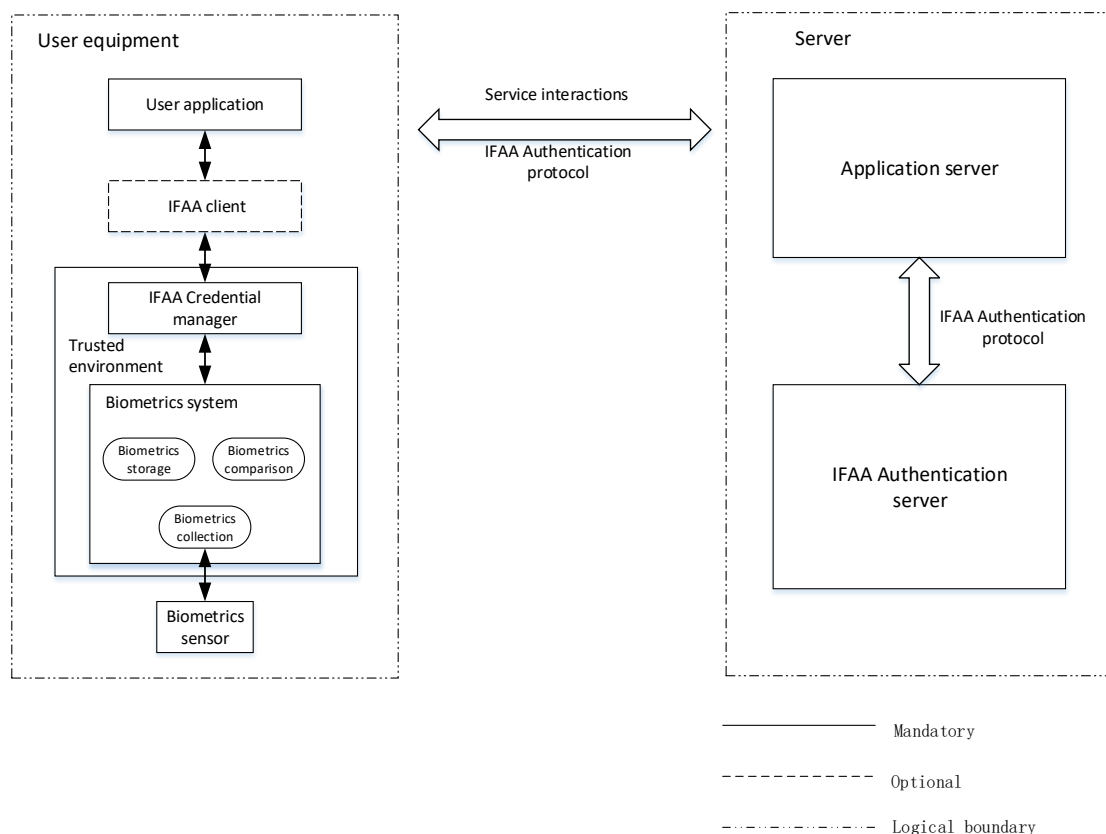


Figure 14 – Authentification biométrique IFAA – modèle local

Les spécifications IFAA définissent les trois principaux protocoles du modèle local: l'enregistrement, l'authentification et le désenregistrement.

La figure 15 présente le flux de messages du protocole d'enregistrement:

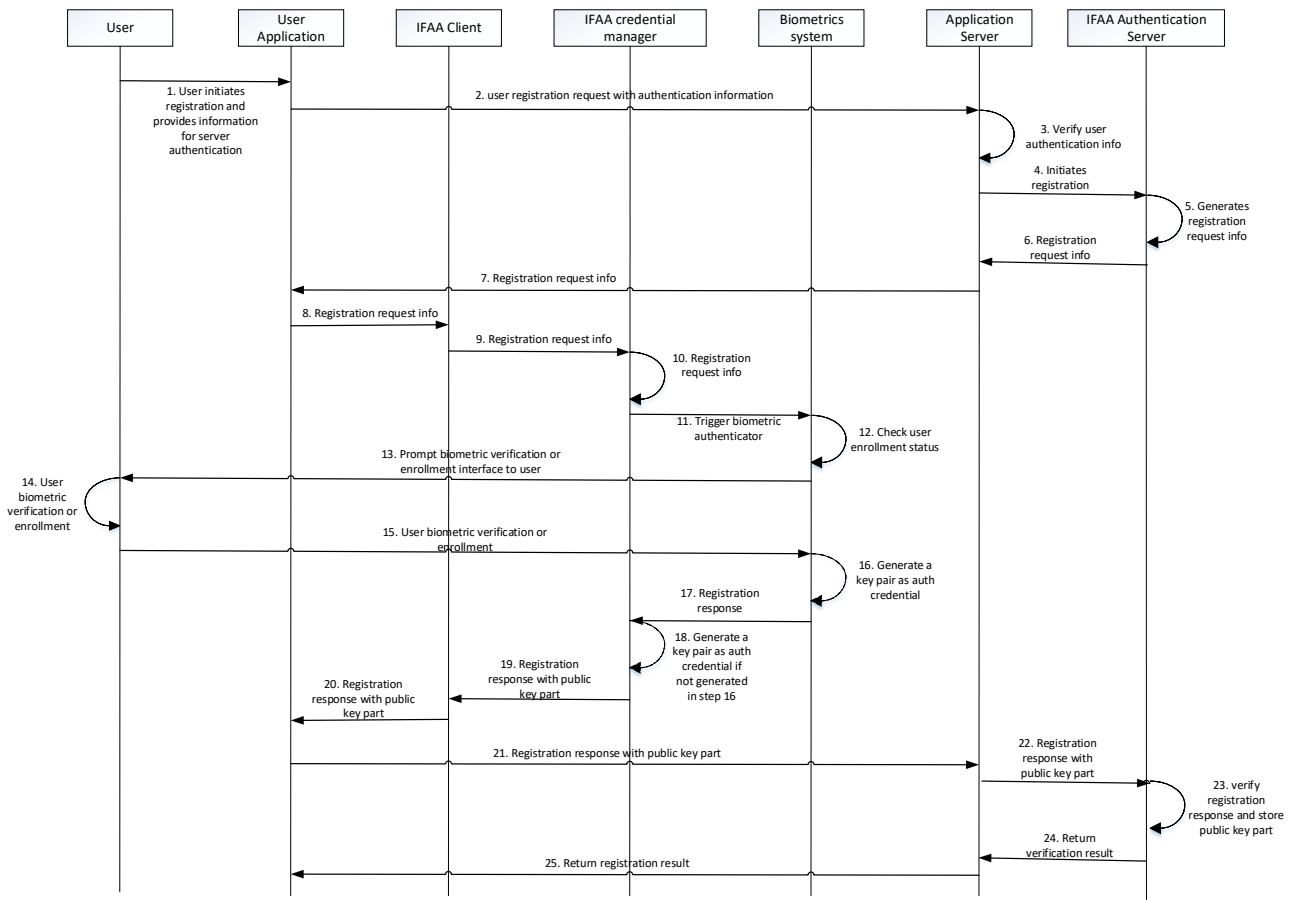


Figure 15 – Authentification biométrique IFAA – modèle local – enregistrement

La figure 16 illustre le flux de messages du protocole d'authentification:

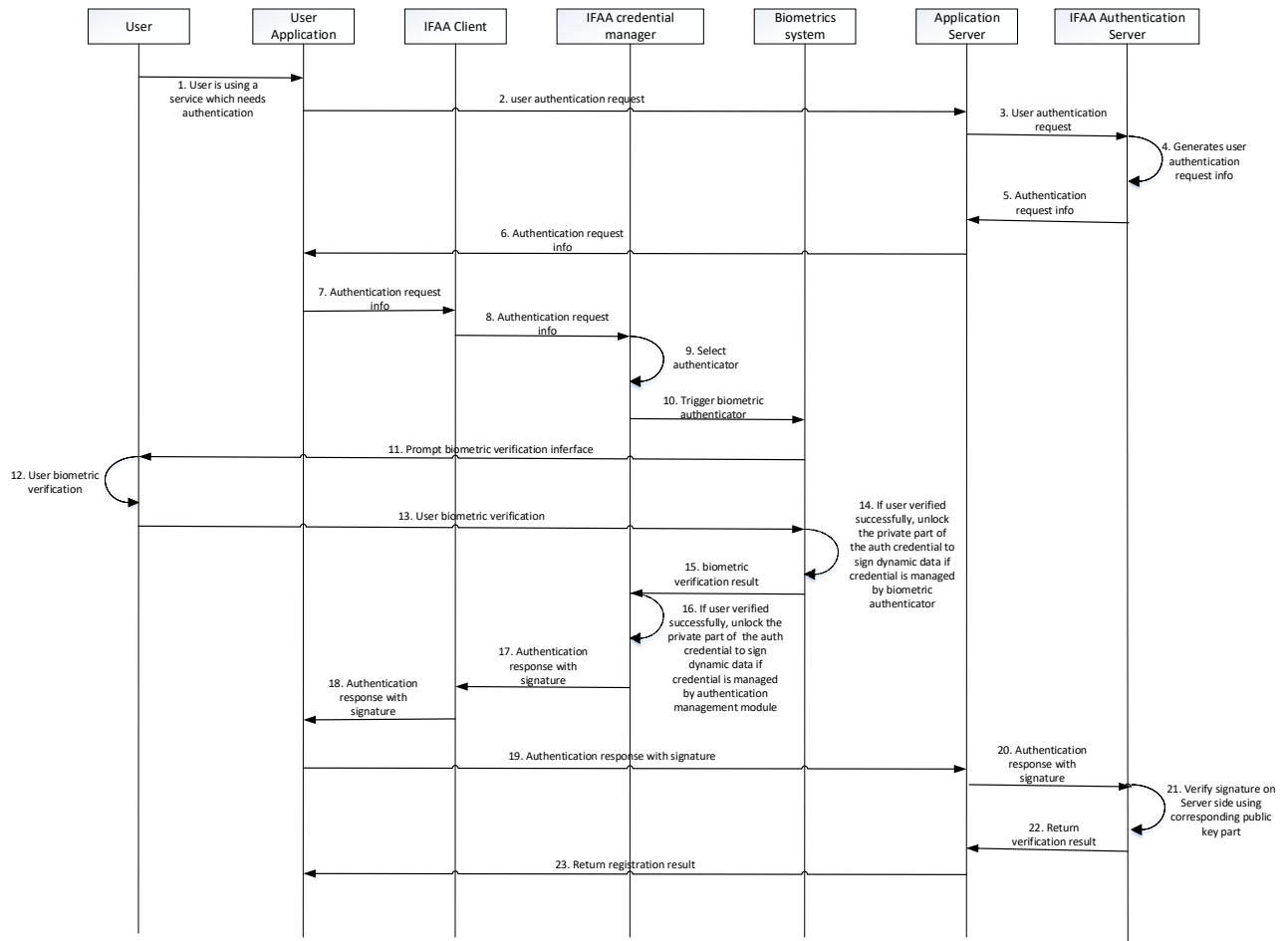


Figure 16 – Authentification biométrique IFAA – modèle local – authentification

La figure 17 illustre le flux de messages du protocole de désenregistrement:

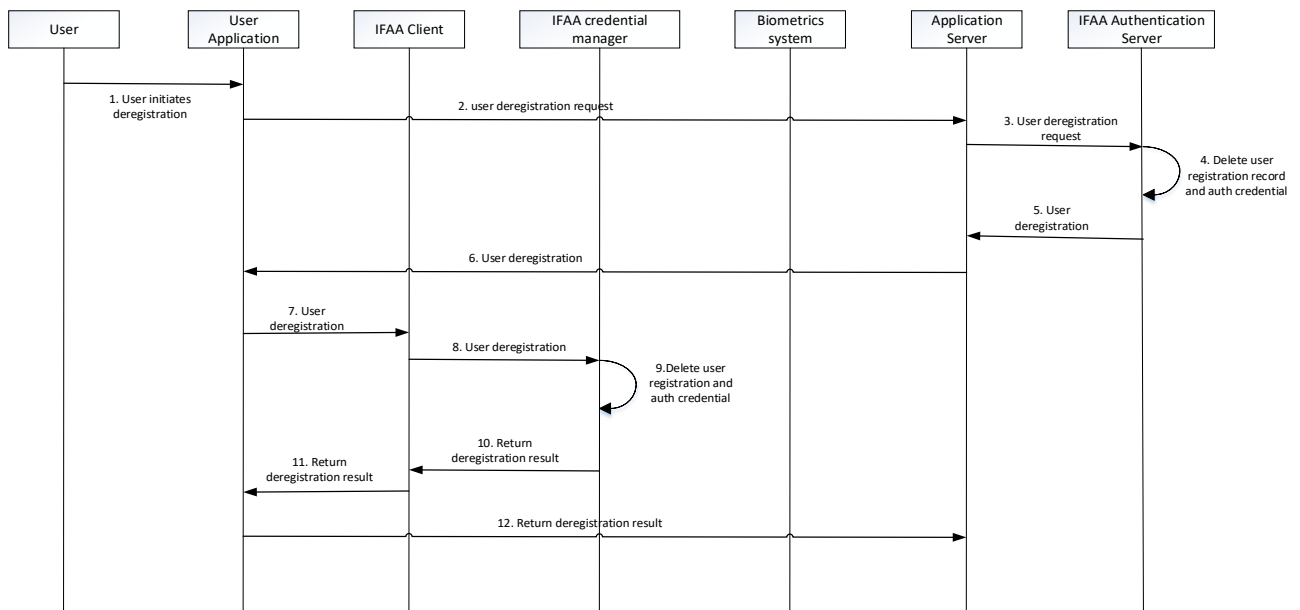


Figure 17 – Authentification biométrique IFAA – modèle local – désenregistrement

6.4.2 Authentification biométrique IFAA – modèle à distance

Dans le modèle à distance, le système biométrique est divisé en deux parties: le module de collecte des données biométriques, qui se trouve dans l'équipement de l'utilisateur, et le module de stockage, qui se trouve dans le serveur d'authentification de pair ainsi que le module de comparaison des données biométriques. Les données biométriques sont collectées au niveau local, mais ne sont ni stockées ni comparées localement. Elles sont envoyées au serveur par l'application de l'utilisateur et vérifiées par le système biométrique du serveur d'authentification. La figure 18 présente l'infrastructure technique de ce modèle.

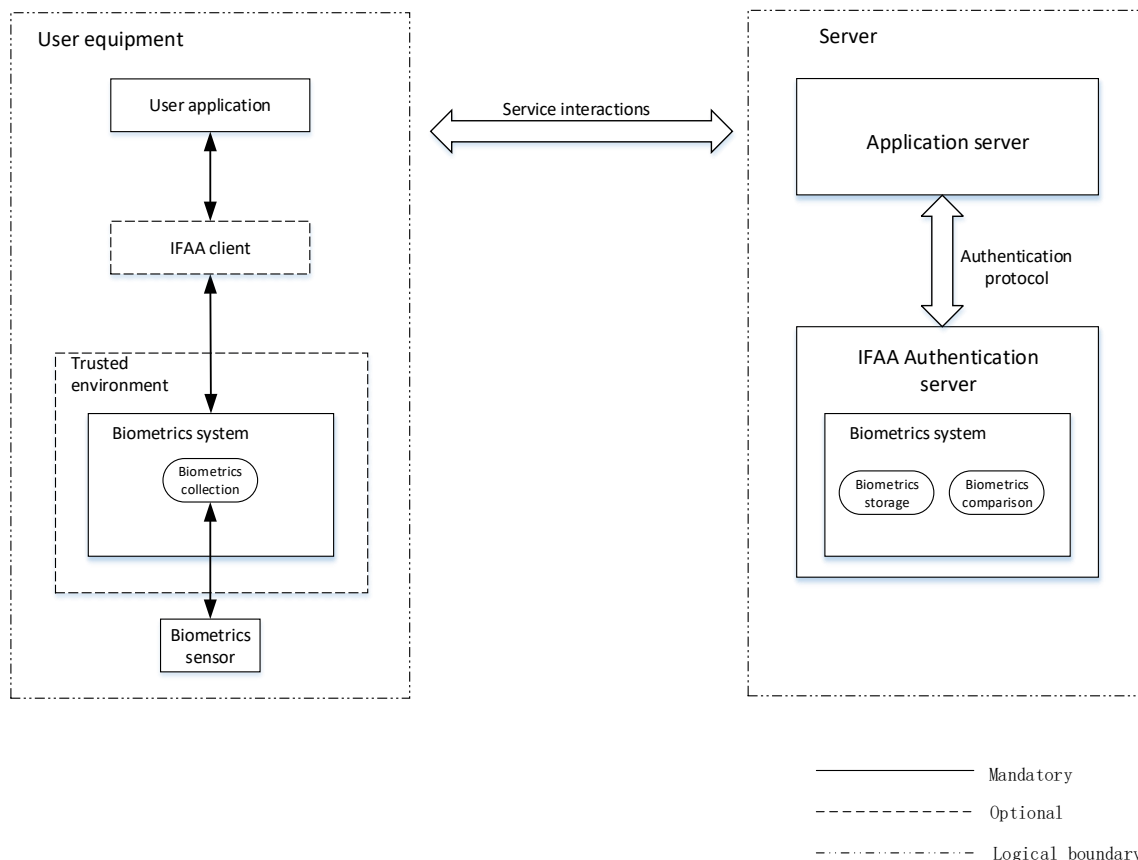


Figure 18 – Authentification biométrique IFAA – modèle à distance

6.5 Authentification Aadhaar

Aadhaar se réfère au numéro d'identification aléatoire à 12 chiffres émis par l'Autorité d'identification unique de l'Inde (UIDAI). Il s'agit de la plus importante base de données biométriques nationale au monde: à ce jour, l'autorité a émis plus de 1 180 millions de numéros Aadhaar.

L'UIDAI est en charge de trois processus fonctionnels clés: l'inscription, l'identification et l'authentification. Au moyen d'un vaste réseau d'agences d'inscription, l'UIDAI recueille les informations démographiques (nom, date de naissance, genre, adresse) et biométriques (empreintes digitales, balayage de l'iris et photographie) des individus en vue de les inscrire dans le système Aadhaar.

Ces données biométriques et démographiques sont conservées dans un référentiel central de données d'identités, et les revendications d'identité ainsi que les services d'authentification sont fournis par le biais d'API ouvertes comprenant des questions auxquelles il est demandé de répondre par oui ou non.

Plusieurs applications, telles que eSign, les casiers numériques, les applications bancaires mobiles, etc., utilisent les services d'authentification biométrique d'Aadhaar.

L'UADAI fournit les processus fonctionnels suivants permettant d'inscrire et de vérifier l'identité des utilisateurs d'Aadhaar:

- **Processus d'inscription:** création et stockage de registres de données d'inscription d'individus soumis au processus de capture biométrique conformément à la politique d'inscription. Ces derniers présentent généralement leurs caractéristiques biométriques à un capteur ainsi que leur référence d'identité. L'échantillon biométrique capturé est traité afin d'en extraire des caractéristiques qui serviront de données de référence dans la base de données d'inscription, de même que la référence d'identité.
- **Processus de vérification:** vérification de l'affirmation selon laquelle l'individu qui fait l'objet du processus de capture biométrique est la source de la référence biométrique spécifiée. Le sujet présente sa référence d'identité ainsi que ses caractéristiques biométriques au dispositif de capture, afin de revendiquer une identité. Ce dispositif collecte ensuite le ou les échantillon(s) biométrique(s) et les compare avec la référence biométrique liée à la référence d'identité à identifier. Le processus de vérification peut avoir un impact sur la confidentialité des informations du sujet dans la mesure où il requiert à la fois une référence biométrique et une référence d'identité. Le processus d'identification nécessite une recherche exhaustive dans la base de données d'inscription. Il peut donc également avoir un impact sur la vie privée physique du sujet. Il est généralement admis que le processus de vérification est moins susceptible de porter atteinte à la vie privée que le processus d'identification. Dans le système Aadhaar, la vérification est effectuée par le biais d'une question d'authentification en ligne à laquelle il suffit de répondre par oui ou non.

L'UIDAI s'est associée à différentes parties prenantes, dont la Banque de réserve de l'Inde, la Société nationale des paiements de l'Inde (NPCI) ainsi que plusieurs banques en vue de mettre en place deux plateformes clés:

- **La passerelle de paiements Aadhaar (APB):** un système qui facilite le transfert transparent de l'ensemble des paiements des programmes d'aide sociale vers le compte bancaire Aadhaar (AEBA) des résidents bénéficiaires.
- **Le système de paiement activé par Aadhaar (AEPS):** un système qui s'appuie sur l'authentification en ligne Aadhaar afin que les AEBA puissent être utilisés en mode bancaire sur des terminaux bancaires mobiles à tout moment et en tout lieu par les populations marginalisées et financièrement exclues de la société.



Figure 19 – Transactions du système de paiement activé par Aadhaar

Le système de paiement activé par Aadhaar est un service de paiement proposé par la Société nationale des paiements de l'Inde aux banques et aux institutions financières qui utilisent Aadhaar. Ce modèle, soutenu par les banques, permet de réaliser des transactions d'inclusion financière en ligne depuis des terminaux bancaires mobiles par l'intermédiaire des correspondants commerciaux de n'importe quelle banque utilisant l'authentification Aadhaar. Ce système traite les demandes ONUS et OFFUS de manière transparente et efficace en établissant une passerelle d'authentification pour chaque titulaire de compte relié à Aadhaar.

L'AEPS permet aux populations marginalisées et exclues d'effectuer des transactions financières (crédit, débit, envoi de fonds, consultation de solde, etc.) par le biais de terminaux bancaires mobiles déployés par les banques dans leurs villages. Quatre types de transactions sont pris en charge par l'AEPS:

- Consultation de solde
- Retrait d'espèces
- Dépôt d'espèces
- Transfert de fonds
- Paiement/achat avec Aadhaar
- Mini relevé
- Statut Aadhaar (lié à la banque) par le biais de l'AEPS

Pour utiliser l'AEPS, les informations suivantes doivent être fournies:

- Type de transaction
- Numéro Aadhaar,
- Numéros d'identification d'entité émettrice (IIN) de la banque³,
- Empreinte digitale
- Le numéro Aadhaar du bénéficiaire (uniquement en cas de transfert de fonds).

Les étapes clés à suivre pour effectuer des transactions par AEPS sont les suivantes:

³ L'IIN est un numéro à six chiffres qui identifie la banque à laquelle la personne a associé son numéro Aadhaar.

- L'individu fournit son numéro Aadhaar, le nom de la banque ainsi que les détails de la transaction financière souhaitée et appose son empreinte digitale sur le terminal bancaire mobile.
- Des paquets de données signés numériquement et chiffrés sont transférés par le commutateur de la banque à la NPCI et à l'UIDAI afin d'authentifier l'utilisateur.
- L'UIDAI traite la demande d'authentification et communique le résultat sous forme de réponse "oui/non".
- Si la réponse d'authentification est "oui", la banque exécute le processus d'autorisation requis et informe le terminal bancaire mobile des prochaines étapes à suivre.

La passerelle de paiement Aadhaar est le référentiel des numéros Aadhaar des résidents ainsi que de leur numéro de compte bancaire principal – celui qu'ils utilisent pour recevoir leurs paiements de sécurité sociale ainsi que diverses allocations d'organismes gouvernementaux. Elle demande le numéro Aadhaar comme clé primaire pour tous les paiements de prestations. Procéder ainsi permettrait de maintenir l'intégrité du système et de garantir que ces sommes parviennent aux bénéficiaires prévus, d'autant plus que les programmes de sécurité sociale délaissent progressivement les subventions en nature au profit des subventions en espèces.

6.5.1 Étapes du processus APB

Les principales étapes de l'enregistrement des paiements par APB sont les suivantes:

- L'agence de prestation de services chargée de verser des paiements à ses bénéficiaires (salaires, bourses d'études, pension de retraite, etc.) fournit à sa banque (appelée banque de parrainage) un fichier APB contenant les détails du numéro Aadhaar, le numéro de référence du programme d'aide sociale ainsi que le montant à payer.
- La banque de parrainage ajoute le numéro d'identification de l'institut (IIN) fourni par la NPCI aux banques participantes au fichier APB et le télécharge sur le serveur de la NPCI.
- La NPCI traite les fichiers téléchargés, prépare les fichiers des banques bénéficiaires et génère le fichier de règlement.
- Le fichier de règlement est ensuite enregistré sur les comptes bancaires auprès de la Banque de réserve de l'Inde.
- Les banques destinataires peuvent télécharger les fichiers entrants afin de traiter les crédits au terme du traitement du fichier de règlement.

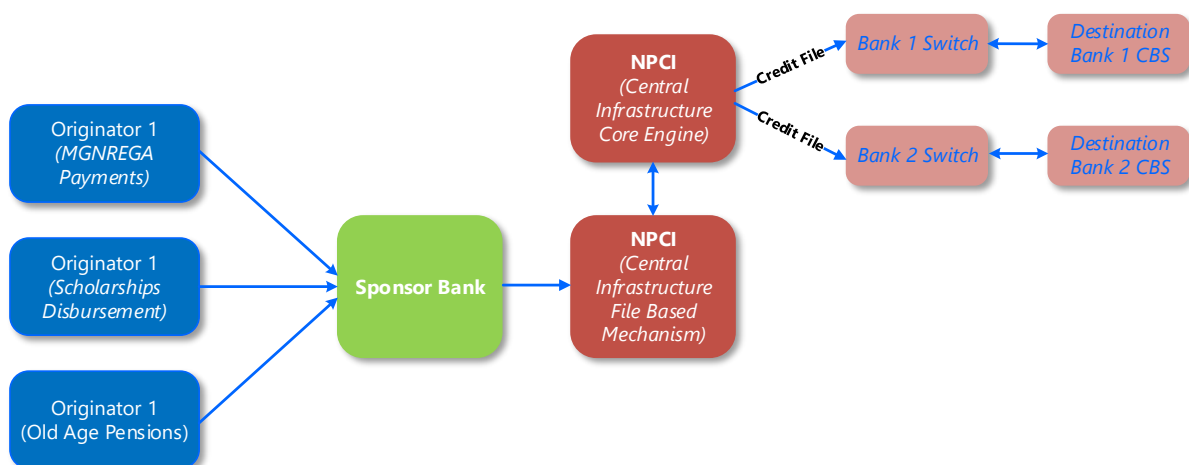


Figure 20 – Processus de la passerelle de paiement Aadhaar

6.5.2 Types et modes d'authentification avec Aadhaar

Il existe deux types d'authentification:

- a) Le système d'authentification par réponse "oui/non",
- b) L'authentification par e-KYC, qui ne peut être effectuée qu'à l'aide des modes d'authentification OTP et/ou biométrique.

Les modes d'authentification suivants sont pris en charge:

- a) **Authentification démographique:** Le numéro Aadhaar ainsi que les informations démographiques de son titulaire (obtenues auprès de ce dernier) sont mis en correspondance.
- b) **Authentification basée sur un code PIN à usage unique:** Un code PIN à usage unique (OTP), dont la validité est limitée dans le temps, est envoyé au numéro de téléphone mobile et/ou à l'adresse électronique du titulaire du numéro Aadhaar enregistré auprès de l'autorité concernée, ou généré par tout autre moyen approprié. Le titulaire du numéro Aadhaar doit fournir cet OTP et son numéro Aadhaar lors de l'authentification. Ces derniers sont alors comparés à l'OTP généré par l'autorité concernée.
- c) **Authentification biométrique:** Le numéro Aadhaar ainsi que les informations biométriques soumis par le titulaire du numéro Aadhaar sont mis en correspondance. Il peut s'agir d'une authentification effectuée par empreinte digitale, par balayage de l'iris ou selon toute autre modalité biométrique basée sur les informations biométriques stockées.
- d) **Authentification à plusieurs facteurs:** Deux ou plusieurs des modes ci-dessus peuvent être choisis conjointement par une entité requérante à des fins d'authentification afin d'en renforcer la sécurité.

L'authentification par e-KYC n'est pas réalisée à l'aide d'une authentification démographique. Elle s'appuie sur un OTP et/ou une authentification biométrique.

6.5.3 Préoccupations en matière de sécurité de l'authentification avec Aadhaar

Idéalement, aucun système ne devrait demander aux utilisateurs de s'identifier et de s'authentifier sans leur consentement. Dans le système Aadhaar, l'identifiant unique requis pour identifier l'utilisateur dans de multiples domaines s'est trouvé au centre des problèmes de sécurité. Le numéro Aadhaar est par exemple nécessaire au moment de l'authentification.

Voici certaines des menaces de sécurité concernant les informations relatives aux usagers et la confidentialité des données dans Aadhaar:

1. **Corrélation des identités entre domaines:** Il pourrait devenir possible de suivre les activités d'un individu à l'aide de son identifiant Aadhaar. Son identification serait alors effectuée sans son consentement.
2. **Identification sans consentement à l'aide des données Aadhaar:** Il existe un risque que les données biométriques soient utilisées dans le but d'identifier un individu de manière illégale.
3. **Traçage illégal d'individus:** Les individus peuvent être suivis sans autorisation appropriée ni sanction légale à l'aide des enregistrements et des pistes d'authentification et d'identification qui se trouvent dans la base de données Aadhaar, ou dans une ou plusieurs bases de données de l'AUA. Ces enregistrements contiennent généralement des informations sur le lieu, l'heure et le contexte précis de l'authentification ou de l'identification, ainsi que sur les services utilisés.

4. La collusion éventuelle d'un attaquant avec le personnel interne peut également entraîner des violations de données au titre des points 2 et 3 ci-dessus.

6.5.4 Récentes mesures de sécurité visant à contrer les menaces

En 2018, pour faire face à ces menaces, le gouvernement indien a mis en œuvre un certain nombre de mesures de sécurité:

a) **Identifiant virtuel**

L'UIDAI a conçu un système d'identification virtuelle à l'attention des titulaires de la carte Aadhaar afin d'éviter que les informations des utilisateurs de la base de données ne fassent l'objet d'une violation de sécurité. Grâce à cet "identifiant virtuel", les titulaires de la carte peuvent générer un numéro temporaire à 16 chiffres qui peut être utilisé pour accéder à diverses plateformes telles que les banques, les assurances ou les fournisseurs de services de télécommunications. Les agences qui procèdent à l'authentification ne seront pas autorisées à générer l'identifiant virtuel au nom du titulaire de la carte Aadhaar. Bien que l'identifiant virtuel soit lié au numéro Aadhaar, il n'est pas permanent par nature. Il est temporaire: il y a donc moins de risques qu'il soit utilisé à mauvais escient. Avec l'identifiant virtuel, l'utilisateur n'est plus tenu de communiquer son numéro Aadhaar au moment de l'authentification. Il est révocable et peut être remplacé.

- b) Le **KYC restreint** ne renvoie pas le numéro Aadhaar. Ainsi, seul un jeton UID unique spécifique à l'agence est généré afin de mettre à l'écart les nombreuses agences qui stockent des AUA⁴ Aadhaar locales et des AUA globales. Les AUA globales pourront accéder à l'e-KYC avec le numéro Aadhaar. Les autres AUA ne pourront accéder qu'à un KYC restreint dans le cadre des processus dématérialisés de KYC. Dès que l'UIDAI reçoit une demande d'authentification de l'AUA locale, elle lui prête un jeton d'identité unique: une chaîne alphanumérique de 72 caractères uniquement compatible avec le système de l'AUA locale. Le jeton UID permet aux agences de garantir l'unicité de leurs bénéficiaires, clients, etc. sans avoir à stocker le numéro Aadhaar dans leurs bases de données. Il les empêche également de fusionner leurs bases de données, ce qui a pour effet d'en renforcer la confidentialité.

c) **Verrouillage biométrique**

Ce service a pour but d'aider les utilisateurs à protéger leurs données biométriques de toute utilisation abusive. Il convient de noter que de nombreuses agences demandent aux candidats de vérifier leurs données à l'aide du service d'authentification biométrique Aadhaar. L'UIDAI peut permettre à un titulaire de numéro Aadhaar de verrouiller de façon permanente ses données biométriques et de les déverrouiller temporairement pour les besoins de l'authentification biométrique.

Toute authentification biométrique effectuée avec de tels enregistrements biométriques verrouillés recevra une réponse négative ("non") ainsi qu'un code de réponse approprié. Le titulaire du numéro Aadhaar en question sera autorisé à déverrouiller temporairement ses données biométriques à des fins d'authentification. Ce déverrouillage temporaire prendra fin au terme de la période spécifiée par l'UIDAI ou de la transaction d'authentification.

⁴ L'AUA fournit des services aux utilisateurs authentifiés avec succès. Parmi les AUA et les services figurent des banques, les ministères de différents États et du gouvernement central fournissant des services, ainsi que des organismes privés tels que les opérateurs de téléphonie mobile. Les AUA doivent conclure un contrat officiel avec l'UIDAI afin d'utiliser les services d'authentification Aadhaar

L'UIDAI peut autoriser les titulaires de numéro Aadhaar à supprimer ces verrouillages permanents à tout moment et de manière sécurisée.

6.6 Authentification cognitive continue

Les systèmes actuels de gestion de l'identité des usagers dans le secteur financier présentent de fortes lacunes en matière de sécurité, de respect de la vie privée et de simplicité d'utilisation. Pour y remédier, il convient d'abandonner l'utilisation des noms d'utilisateur, des mots de passe et de toute autre forme de contrôle temporel, binaire et biométrique au profit de nouveaux systèmes.

Cette transition est aujourd'hui possible grâce à un ensemble de contrôles multimodaux et contextuels qui protègent de manière continue et précise l'identité ainsi que la vie privée des utilisateurs, même lorsque leurs identifiants en ligne sont déjà compromis. La plateforme Cognitive Continuous Authentication™ utilise l'intelligence artificielle et l'apprentissage automatique (AIML) de pair avec un ensemble de contrôles multimodaux et contextuels qui protègent de manière continue et précise les transactions des utilisateurs ainsi que leur identité et leur vie privée. L'appariement de l'intelligence artificielle (IA) avec l'AIML peut être utilisé en arrière-plan, de sorte à apprivoiser le comportement numérique des utilisateurs en contexte. En adoptant une approche globale des transactions effectuées par les usagers, l'IA peut déterminer si un acteur malveillant tente d'initier une transaction frauduleuse.

La plateforme Cognitive Continuous Authentication™ initie la collecte de renseignements avant l'authentification, puis réalise une nouvelle authentification de pointe basée sur le risque à l'aide d'un riche ensemble de données contextuelles au lieu d'une authentification binaire afin de diminuer la contrainte des usagers bien intentionnés. Il procède ensuite à une étape particulièrement importante, à savoir une authentification continue après autorisation en vue de détecter les anomalies de transaction en tirant parti des nouveaux mécanismes de contrôles, y compris l'AIML.

La figure 21 ci-dessous illustre le parcours des utilisateurs sur la plateforme Cognitive Continuous Authentication™ d'Acceptto. Cette plateforme s'appuie sur des données de préauthentification, sur l'authentification contextuelle basée sur le risque ainsi que sur l'authentification continue après autorisation.

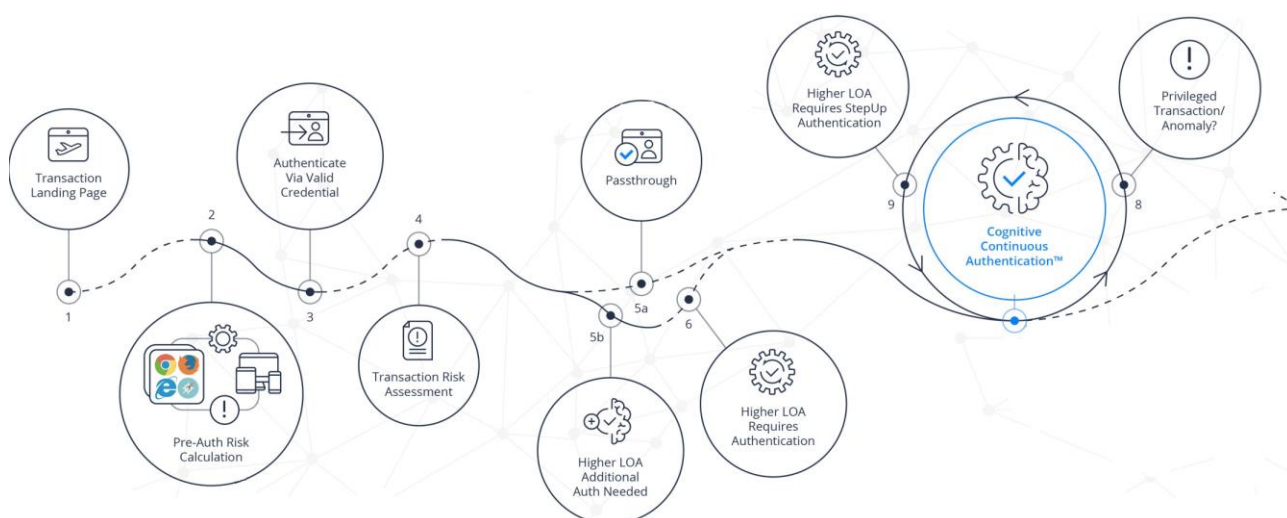


Figure 21 – La plateforme Cognitive Continuous Authentication™ d'Acceptto

Lorsque l'action d'un utilisateur dans la session en cours semble biaisée, l'IA peut rapidement le signaler à l'application. Les systèmes d'intelligence artificielle conçus pour détecter les intrusions et les anomalies, tels que la plateforme Cognitive Continuous Authentication™ d'Acceptto, emploient

des techniques d'apprentissage automatique. Ces algorithmes traitent et analysent d'importantes quantités de connexions précédemment observées et de données contextuelles. Ils *apprennent* les caractéristiques et les modèles afin de classer les demandes et de détecter les activités anormales ainsi que les éventuelles menaces.

6.7 Identité décentralisée et registres distribués

Les systèmes de gestion des identités traditionnels reposent sur des autorités centralisées telles que les services d'annuaire d'entreprise, les autorités de certification ou les registres de noms de domaine. Chacune de ces autorités centralisées à l'échelle d'une organisation constitue sa propre base de confiance. La fédération d'identité est apparue comme une solution provisoire permettant aux systèmes de gestion d'identités d'être opérationnels au sein de systèmes présentant différentes bases de confiance.

L'émergence de la technologie des registres distribués (DLT) offre la possibilité d'envisager une nouvelle approche des systèmes d'identification décentralisée. Dans les systèmes d'identification décentralisée, les entités sont libres d'utiliser n'importe quelle base de confiance partagée. Les registres distribués permettent de gérer une base de confiance sans autorité centralisée ni point de défaillance unique. De même, les registres distribués et les systèmes d'identification décentralisée permettent aux entités de créer et de gérer leurs propres identifiants sur un nombre indéfini de bases de confiance distribuées et indépendantes [10].

L'"identité souveraine" constitue l'une des approches des systèmes d'identification décentralisée. Ses partisans ont élaboré un ensemble de principes de conception [11]:

1. Existence: Les entités doivent exister de manière indépendante
2. Contrôle: Les entités doivent pouvoir contrôler leurs identités, les référencer, les mettre à jour ou les cacher.
3. Accès: Les entités doivent avoir accès à leur propre identité ainsi qu'aux données qui s'y rapportent.
4. Transparence: Le système et sa logique doivent avoir un fonctionnement transparent.
5. Persistance: Les identités doivent avoir une longue durée de vie – au moins aussi longue que l'utilisateur le souhaite –, sans toutefois contrevenir à son droit à l'oubli.
6. Portabilité: Les informations relatives aux identités doivent être transportables.
7. Interopérabilité: Les identités doivent pouvoir être utilisées dans la plus large mesure possible.
8. Consentement: Les entités doivent consentir à l'utilisation de leurs identités ainsi qu'au partage des données connexes.
9. Minimisation: La divulgation des revendications doit être réduite au minimum.
10. Protection: Lorsqu'un conflit survient entre les besoins du réseau et le droit des entités, ce dernier doit être protégé en priorité.

La prise en charge de chaque principe par la plupart des solutions d'identification d'autorité centrale actuelles, notamment en matière de contrôle de l'identité, de transparence et de portabilité, est limitée.

Les sections suivantes décrivent les principales composantes de ces nouveaux systèmes d'identification décentralisée: les identifiants vérifiables, les identificateurs décentralisés, l'authentification et la résolution d'identificateurs décentralisés ainsi que les portefeuilles de clés de chiffrement personnelles.

6.7.1 Définition des termes relatifs à l'identité décentralisée

Les normes émergentes des systèmes d'identification décentralisée proposent des définitions modernisées et détaillées des principaux termes. Cette section présente les définitions de la spécification Identifiants vérifiables [12] du W3C. Notez que la définition de certains termes peut

avoir évolué au point de ne plus correspondre à celle qui leur était précédemment attribuée, notamment dans les normes en vigueur.

sujet

Entité au sujet de laquelle des revendications sont faites.

revendication

Assertion à propos d'un sujet.

identifiant

Un ensemble d'une ou plusieurs revendications émises par un émetteur. Un identifiant vérifiable est un identifiant inviolable dont l'auteur peut être vérifié à l'aide de technologies de chiffrement. Les identifiants vérifiables peuvent servir à établir des présentations vérifiables, qui peuvent également être vérifiées à l'aide de technologies de chiffrement. Les revendications d'un identifiant peuvent porter sur différents sujets.

identificateur décentralisé

Un identifiant portable sous forme d'URL, également appelé DID, associé à une entité. Ces identificateurs sont le plus souvent utilisés pour les identifiants et sont associés à des sujets de sorte que les identifiants puissent être facilement transférés d'un référentiel à un autre sans qu'il soit nécessaire d'en émettre de nouveaux. En voici un exemple: did:exemple:123456abcdef.

identité

Un moyen de conserver la trace d'entités dans différents contextes. Les identités numériques permettent de suivre et de personnaliser les interactions des entités dans les contextes numériques, généralement à l'aide d'identifiants et d'attributs. La distribution ou l'utilisation involontaire d'informations relatives à l'identité peut compromettre la confidentialité des données. La collecte et l'utilisation de ces informations doivent respecter le principe de minimisation des données.

6.7.2 Couches d'infrastructure du système d'identification décentralisée

La Fondation Sovrin [13] a élaboré une approche visant à organiser les composantes de l'infrastructure technologique de son système d'identification décentralisée. Sovrin adopte une méthode par couches afin d'expliquer les rôles, les fonctions ainsi que les relations des différentes composantes de l'infrastructure, comme le montre la figure 23.

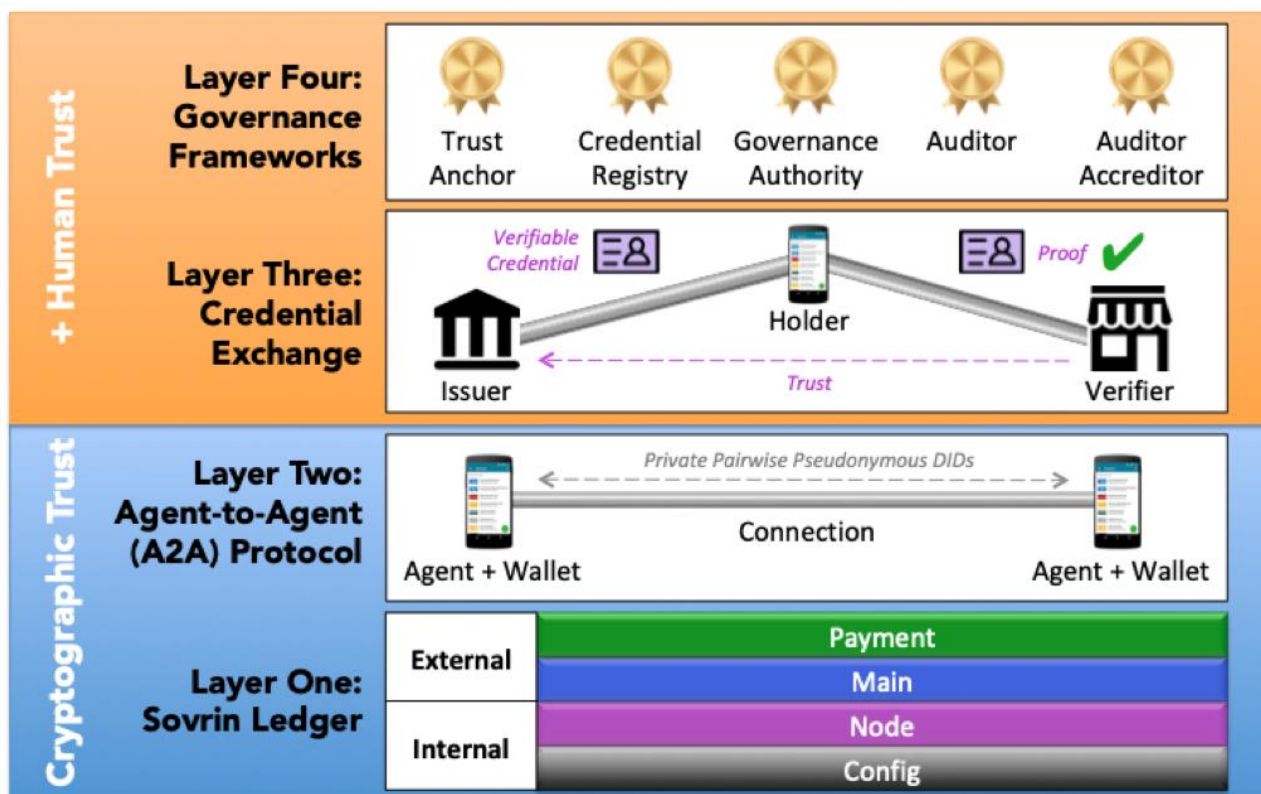


Figure 23 – Couches de l'infrastructure Sovrin

La couche 1, la couche du registre Sovrin, contient les composants des DLT qui sous-tendent la solution Sovrin. Les émetteurs d'identifiants qui souhaitent que leurs identifiants puissent être vérifiés publiquement y stockent leurs identités Sovrin ainsi que leurs identificateurs décentralisés. Les schémas, les définitions d'identifiants et les registres de révocation se situent également dans la première couche.

La couche 2, une couche d'agent à agent, contient des protocoles de communication qui lancent des communications de pair à pair directes entre l'agent, l'identifiant et le portefeuille cryptographique. Cette couche ne contient pas de DLT. Combinées, les couches 2 et 1 garantissent la fiabilité du chiffrement des composants logiciels et matériels.

La couche 3, à savoir la couche d'échange d'identifiants, fournit les mécanismes qui permettent aux émetteurs d'identifiants de délivrer des identifiants vérifiables aux titulaires, et aux titulaires de délivrer des preuves aux vérificateurs. Les vérificateurs vérifient les preuves cryptographiques afin d'avoir la certitude que la revendication de l'identifiant est valide selon l'émetteur.

La couche 4, la couche des infrastructures de gouvernance, est celle au sein de laquelle les accords commerciaux et juridiques visant à spécifier les règles des émetteurs et des vérificateurs sont établis.

6.7.3 Projets de normes sur les identifiants vérifiables et les identificateurs décentralisés

De nouvelles approches et technologies compatibles avec les registres distribués (également appelés "blockchains") sont conçues afin d'établir des réseaux d'identité qui ne dépendent pas d'autorités de données centralisées. Ces réseaux sont décrits de nombreuses manières différentes. Deux projets de normes de base sont au cœur de ces nouvelles avancées: les identifiants vérifiables du W3C [12] et les identificateurs décentralisés du W3C [10]. Cet ensemble de technologies et de normes est toujours en cours de développement et n'a pas encore été généralisé.

6.7.4 Identifiants vérifiables

Extrait de la spécification relative au modèle de données des identifiants vérifiables du W3C:

Les identifiants vérifiables peuvent représenter les mêmes informations que les identifiants physiques. L'avènement de nouvelles technologies telles que les signatures numériques complique la falsification des identifiants vérifiables. Ces derniers sont par conséquent plus fiables que leurs équivalents physiques. Les titulaires peuvent générer des présentations et les partager avec les vérificateurs pour prouver qu'ils possèdent des identifiants vérifiables présentant certaines caractéristiques. Ces identifiants et présentations peuvent être transmis plus rapidement que leurs équivalents physiques. Ils sont dans ce sens plus pratiques et plus fiables.

La figure 24 illustre les rôles et concepts de base des identifiants vérifiables.

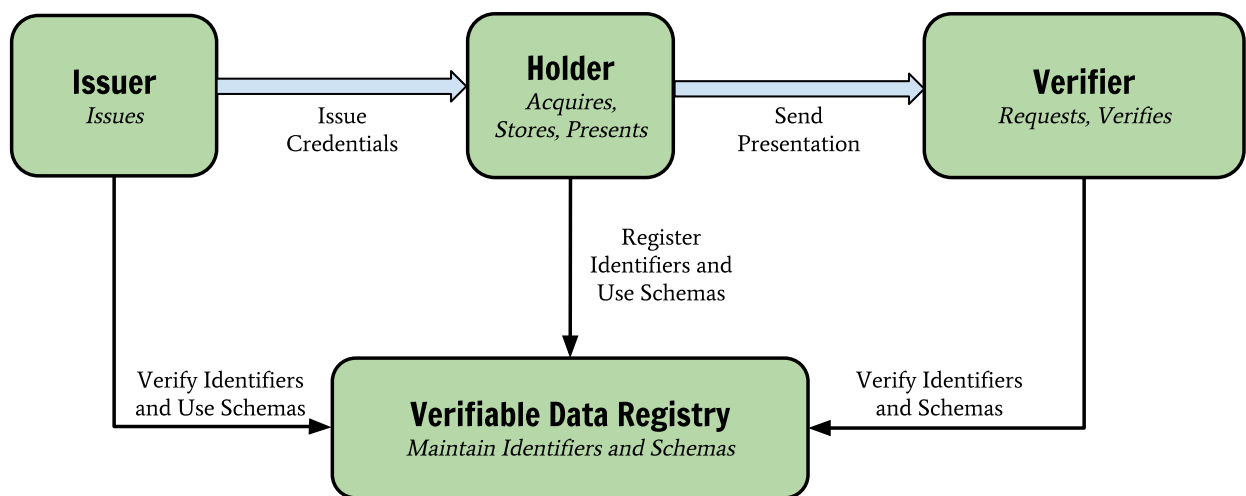


Figure 24 – Rôles et relations des parties prenantes

Les rôles sont décrits dans la spécification comme suit:

Émetteur

Une entité qui fait valoir des revendications concernant un ou plusieurs sujets, crée un identifiant vérifiable sur la base de ces revendications et transmet cet identifiant à un titulaire.

Vérificateur

Une entité qui reçoit une ou plusieurs présentations vérifiables à traiter. Dans certains contextes, elle est qualifiée de partie utilisatrice.

Titulaire

Une entité qui possède un ou plusieurs identifiants vérifiables. Le titulaire est généralement, mais pas toujours, le sujet des identifiants vérifiables qu'il détient. Les titulaires stockent leurs identifiants dans des référentiels d'identifiants.

Registre de données vérifiables

Un système qui agit en tant qu'intermédiaire dans le cadre de la création et de la vérification d'identifiants, de clés et d'autres données pertinentes telles que les schémas d'identifiants vérifiables et les registres de révocation, qui peuvent être nécessaires pour utiliser les identifiants vérifiables. Certaines configurations peuvent requérir que les sujets disposent d'identifiants corrélables. Les bases de données de confiance, les bases de données décentralisées, les bases de données d'identifiants

gouvernementaux et les registres distribués constituent des exemples de registres de données vérifiables. Un écosystème compte souvent plusieurs types de registres de données vérifiables.

Les identifiants vérifiables sont présentés en détail dans la section 8.1.4 Exemple: Identité numérique à Zoug – Identité numérique basée sur la blockchain de l'Ethereum

6.7.5 Identificateurs décentralisés

Les spécifications relatives aux DID ont été conçues pour établir un espace de noms d'identifiants vérifiables grâce à des techniques de chiffrement et adressables à l'échelle mondiale dans les systèmes de registres distribués et de blockchain. Les DID constituent le schéma d'adressage utilisé pour les identifiants vérifiables.

Extrait du projet de spécification relative aux DID du W3C:

- L'émergence de la DLT, parfois appelée technologie de la blockchain, offre la possibilité de gérer les identités de façon entièrement décentralisée. Dans les systèmes d'identification décentralisée, les entités sont libres d'utiliser n'importe quelle base de confiance partagée. Les registres distribués à l'échelle mondiale (ou tout réseau de pair à pair décentralisé offrant des capacités similaires) permettent de gérer une base de confiance sans autorité centralisée ni point de défaillance unique. De même, les registres distribués et les systèmes d'identification décentralisée permettent aux entités de créer et de gérer leurs propres identifiants sur un nombre indéfini de bases de confiance distribuées et indépendantes.
- Les entités sont identifiées par des DID. Elles peuvent s'authentifier en utilisant des preuves (par exemple, signatures numériques, protocoles biométriques préservant la confidentialité, etc.). Les DID orientent vers des documents de DID. Un document de DID contient un ensemble de points de terminaison de services qui permettent d'interagir avec l'entité. Conformément au principe de confidentialité dès la conception, chaque entité peut avoir autant de DID que nécessaire afin de respecter la séparation souhaitée des identités, des avatars et des contextes.
- Pour utiliser un DID avec un registre distribué ou un réseau donné, il convient de définir une méthode de DID dans le cadre d'une spécification de méthode de DID distincte. La méthode de DID spécifie l'ensemble des règles d'enregistrement, de résolution, de mise à jour et de révocation des DID sur le registre ou réseau en question.
- Il n'est ainsi plus nécessaire de disposer d'identifiants pour accéder aux registres centralisés ni d'avoir recours aux autorités de certification centralisées pour assurer la gestion des clés – le modèle standard de PKI hiérarchique. Les DID résident dans un registre distribué; chaque entité peut donc servir d'autorité de base. Cette architecture est appelée PKI décentralisée (DPKI).

En général, les objectifs de conception des DID sont les suivants [10]:

1. Décentralisation: L'architecture du DID est telle qu'il ne devrait plus être nécessaire d'avoir recours aux autorités centralisées ou aux points de défaillance uniques pour assurer la gestion des identités, notamment en ce qui concerne l'enregistrement des identifiants uniques au niveau mondial, des clés de vérification publiques, des points de terminaison de services et d'autres métadonnées.
2. Contrôle des identifiants par les entités: L'architecture du DID devrait donner aux entités, humaines et non humaines, le pouvoir de contrôler directement leurs propres identifiants numériques sans l'intervention d'autorités externes.

3. Protection des informations d'identification personnelle: L'architecture du DID devrait permettre aux entités de contrôler les données identifiables de leurs identités numériques ainsi que de divulguer leurs attributs ou d'autres données d'identité de façon minimale, sélective et progressive.
4. Sécurité: L'architecture du DID doit offrir un niveau de garantie suffisant pour que les parties utilisatrices puissent se fier aux DID pour leur niveau de garantie requis.
5. Mise à disposition de preuves: L'architecture du DID doit permettre aux entités de fournir une preuve cryptographique d'authentification ainsi qu'une preuve des droits d'autorisation.
6. Accessibilité: L'architecture du DID doit permettre aux entités d'accéder aux DID d'autres entités pour en savoir plus à leur sujet ou interagir avec elles.
7. Interopérabilité: L'architecture du DID doit utiliser des normes interopérables afin que l'infrastructure des DID puisse utiliser les outils et bibliothèques logicielles conçus à des fins d'interopérabilité.
8. Portabilité: L'architecture du DID doit être indépendante des systèmes et des réseaux et permettre aux entités d'utiliser leurs identités numériques dans tout système compatible avec les DID et les méthodes de DID.
9. Simplicité: Pour atteindre ces objectifs de conception, l'architecture du DID doit être "aussi simple que possible".
10. Extensibilité: Lorsque c'est possible, l'architecture du DID doit permettre l'extensibilité des identifiants, à condition qu'elle n'entrave pas excessivement leur interopérabilité, leur portabilité ou leur simplicité.

6.7.6 Authentification des DID

Le processus d'authentification des DID [14] permet aux sujets de prouver qu'ils détiennent le contrôle sur leurs DID lorsque ces derniers interagissent avec une partie utilisatrice. La partie utilisatrice doit suivre les étapes générales suivantes:

1. La partie utilisatrice récupère le document de DID associé au sujet du DID.
2. La partie utilisatrice utilise la propriété d'authentification du document de DID pour déterminer la manière d'effectuer l'authentification, par exemple au moyen de signatures numériques, en établissant la preuve du contrôle d'une clé publique ou en utilisant un point de terminaison du service d'authentification.
3. La partie utilisatrice exécute le mécanisme d'authentification fourni.

L'authentification des DID doit être compatible avec les flux Web et mobiles.

6.7.7 Résolution des DID

La spécification du DID exige que chaque registre distribué soit doté d'une spécification de la méthode de DID qui décrive le déroulement des opérations de DID. La multiplicité des spécifications de méthodes de DID complique néanmoins la résolution des chaînes de texte (le DID), une étape requise pour localiser la base de confiance et le document de DID associé. La fonction de résolution des DID pourrait devenir un obstacle majeur à leur interopérabilité. Une architecture ainsi qu'un ensemble d'outils de résolution universels de DID, qui peuvent se baser sur n'importe quel DID valide pour produire un document de DID, sont ainsi à l'étude. Les résolveurs universels ont été conçus de manière à fonctionner avec les DID ainsi qu'à prendre en charge la résolution des DID sur de nombreux types de registres distribués et de réseaux [15]. Le résolveur universel résout le problème des réseaux hétérogènes qui adoptent différentes spécifications de méthode pour leurs propres DID. La figure 25 illustre le concept de résolveur universel [15].

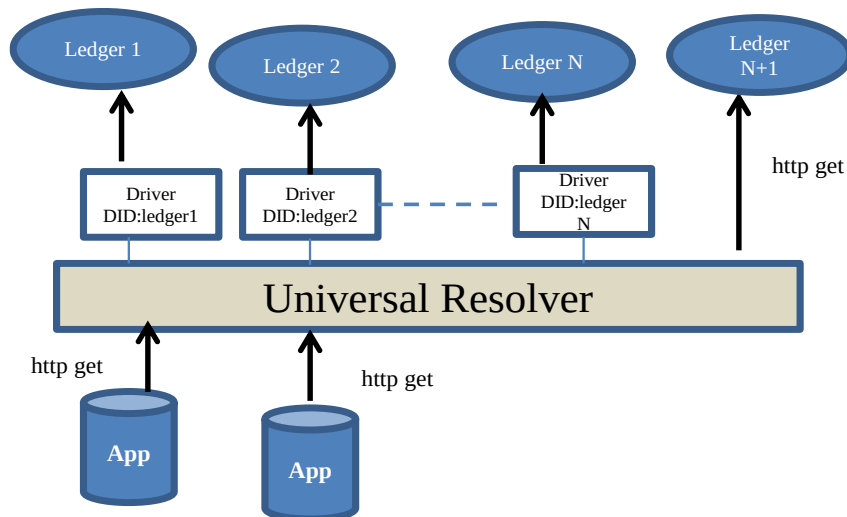


Figure 25 – Résolveur universel de DID

6.7.8 Portefeuilles d'identité décentralisée

L'individu doit disposer d'un logiciel et/ou d'un dispositif lui permettant d'interagir avec le système d'identité décentralisée. Ces composants sont les agents et les portefeuilles [16].

La fonction principale d'un agent est de communiquer avec d'autres agents et de coordonner la résolution ainsi que l'authentification des DID. L'agent garde la trace des DID liés à d'autres entités du réseau. Un agent contient ou est connecté à un portefeuille dans lequel les clés de chiffrement secrètes sont conservées et protégées. Ce portefeuille contient les clés privées sans lesquelles l'individu ne peut ni prouver le contrôle d'un DID ni participer au système d'identité décentralisé. L'agent et le portefeuille contiennent des identifiants ainsi que des preuves vérifiables appartenant à l'individu.

Ce portefeuille peut être entièrement localisé sur l'appareil de l'utilisateur ou se présenter sous la forme d'un portefeuille virtuel dont une partie se trouve sur l'appareil mobile de l'utilisateur et l'autre, sur le nuage. Cette dernière configuration permet de créer des agents qui agissent au nom de l'utilisateur et exécutent des services sans que l'utilisateur ait à intervenir directement.

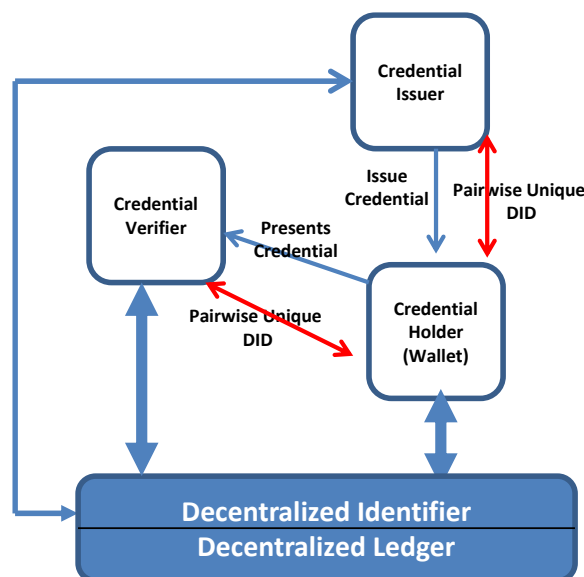


Figure 26 – Portefeuille d'identité décentralisée avec identifiants vérifiables

La figure 26 présente l'ensemble des interactions d'identité qui sous-tendent les services basés sur l'identité. Le portefeuille contient tous les éléments nécessaires à l'établissement de l'identité de son propriétaire. L'authentification requise pour y accéder doit par conséquent employer une méthode d'authentification forte, sans mot de passe.

7 Exemples de mise en œuvre de systèmes d'authentification forte

Cette section contient des exemples de systèmes d'authentification forte qui illustrent certains cas d'utilisation des DFS. Ces exemples décrivent également les mécanismes relatifs aux phases de garantie d'authentification de la Recommandation UIT-T X.1254.

Tableau 3 – Exemples de cas d'utilisation des services financiers numériques

Phase de garantie d'authentification	Cas d'utilisation des DFS	Exemples de cas d'utilisation
Inscription	Ouverture de compte (section 8.1): ▪ e-KYC ▪ Vérifications de crédit	▪ e-KYC Aadhaar (Section 8.1.1) ▪ Plateforme nationale d'identité numérique et de crédit de la Sierra Leone – Kiva (Section 8.1.2) ▪ Inscription avec K-FIDO (Section 8.1.2) ▪ Identité numérique à Zoug – Identité numérique basée sur la blockchain de l'Ethereum (Section 8.1.4) ▪ Inscription avec FIDO (section 8.1.5) ▪ Inscription d'un utilisateur d'un prestataire de soins de santé (Section 8.1.6)
Authentification	Accéder à un service financier numérique (Section 8.2): ▪ Stockage de fonds ▪ Achat ▪ Paiement de factures ▪ Envoi/réception de fonds ▪ Emprunt ▪ Épargne ▪ Assurance des actifs et des risques	▪ Paiement par empreinte digitale avec Alipay (Section 8.2.1) ▪ Authentification Aadhaar (Section 8.2.2) ▪ Authentification avec K-FIDO (Section 8.2.3) ▪ Prestataire de soins de santé: authentification de nouvelle génération (Section 8.2.4) ▪ SK Telecom – Authentification Mobile Connect (Section 8.2.5)

7.1 Cas d'utilisation: Inscription et ouverture de compte

Les exemples présentés pour le cas d'utilisation relatif à l'inscription décrivent la façon dont les informations d'identité précédemment établies peuvent être utilisées pour créer de nouveaux comptes de service ainsi que pour satisfaire aux exigences relatives aux processus de KYC. Dans chacun de ces exemples, l'individu a précédemment été inscrit auprès d'une autorité: ses informations d'identité ont donc été collectées, vérifiées et stockées. Ces informations d'identité stockées peuvent ensuite être présentées aux fournisseurs de services lors de l'authentification de la personne concernée.

L'utilisation de sources numériques d'informations d'identité dans le cadre du processus de KYC et de l'ouverture de compte en personne présente des avantages d'ordre pratique, mais aussi des risques d'usurpation d'identité. Il est donc recommandé d'utiliser des mécanismes d'authentification forte à ces fins.

7.1.1 Exemple: Service e-KYC d'Aadhaar

Le service d'e-KYC d'Aadhaar permet à l'UIDAI de partager la version électronique des informations du système (données démographiques et photographie uniquement) avec le consentement explicite de la personne concernée. Pendant le processus d'e-KYC, l'UIDAI chiffre les données de réponse du processus contenant les informations démographiques et photographiques les plus récentes du résident concerné en utilisant la clé publique de l'agence d'utilisateurs d'e-KYC (KUA) et transmet la réponse chiffrée à cette dernière. Dès réception de la réponse chiffrée, la KUA déchiffre les données à l'aide de sa propre clé privée et renvoie un fichier XML contenant les sept éléments: nom, adresse, date de naissance, genre, numéro de téléphone, adresse électronique et photographie. Il n'est donc plus nécessaire de demander une photocopie de la lettre Aadhaar au résident.

Le service d'e-KYC basé sur Aadhaar présente notamment les avantages suivants:

- Activation: il n'est pas nécessaire de remplir le formulaire de demande du client (CAF) ni de fournir des copies physiques d'un justificatif d'identité, d'un justificatif d'adresse ainsi que des photographies.
- Processus sécurisé: les données du client sont extraites du serveur central de l'UIDAI dans un format chiffré et ne sont pas stockées sur les terminaux de point de vente, sauf sur le serveur de l'entreprise.
- Aucune copie de justificatif d'identité ou de photographie n'est requise; cela augmente la confiance des clients, qui ne sont alors pas tenus de soumettre des documents qui pourraient être utilisés ultérieurement par les détaillants à des fins lucratives.
- Activation extrêmement rapide: contrairement au processus traditionnel d'activation de la carte SIM, qui peut prendre entre 12 et 24 heures, la carte SIM est très rapidement activée une fois le formulaire soumis par le terminal de point de vente à aux services administratifs de l'entreprise. La satisfaction du client est ainsi très élevée.
- Outre les avantages susmentionnés, ce processus permet aux fournisseurs de services de télécommunications (FST) d'éliminer les processus archaïques de collecte des CAF, de saisie des données, de numérisation des documents, de télévérification et de stockage physique ainsi que de récupération des CAF et des documents dans l'entrepôt. Les FST sont donc en mesure de stocker les informations relatives au processus de KYC de leurs clients dans un format électronique qui peut être récupéré très rapidement sous forme de dossier électronique.
- Ce processus présente également des avantages pour les autorités gouvernementales, tant au niveau des cellules TERM dans le cadre des audits que des organismes chargés de l'application de la loi. Ce processus à haut degré de conformité facilite en effet considérablement la traçabilité du client dans le cadre des procédures juridiques.

7.1.2 Exemple: Plateforme nationale d'identité numérique et de crédit de la Sierra Leone – Kiva

Un nouveau partenariat [15] entre Kiva, la Sierra Leone et les Nations Unies (Programme des Nations Unies pour le développement et Fonds d'équipement des Nations Unies) vise à mettre à la disposition des citoyens de la Sierra Leone un système national d'identification numérique afin qu'ils puissent bénéficier d'une identité officielle et contrôler leurs informations de crédit.

Le président de la Sierra Leone, Julis Maada Bio, a présenté cette initiative lors de son discours devant l'Assemblée générale des Nations Unies le 27 septembre 2018.

La pièce centrale de ce partenariat est le protocole Kiva [16], une plateforme technologique qui permet aux pays de concevoir et de mettre en œuvre un système national d'identification numérique basé sur la technologie de registre distribué (DLT). L'absence d'identification formelle et d'antécédents d'identifiants vérifiables figurent parmi les principaux obstacles à l'accès aux services financiers. L'objectif ultime de ce partenariat est de favoriser la prise d'initiatives d'inclusion financière au niveau national et de fournir des produits et services financiers aux populations qui en sont actuellement dépourvues.

Afin de lever ces obstacles, le protocole Kiva étend l'identification numérique civile nationale à l'ensemble des citoyens. Les institutions financières formelles et informelles peuvent ainsi effectuer des vérifications reposant sur le processus e-KYC ainsi que des évaluations de crédit presque en temps réel.

Actuellement, les personnes non bancarisées ne peuvent pas tirer parti des transactions financières de l'"économie informelle", en prenant par exemple connaissance de leurs antécédents auprès d'une institution de microfinance (IMF) locale, pour établir leurs antécédents de crédit. Les institutions bancaires, afin d'inclure leurs transactions dans les antécédents de crédit des individus (des prêts des banques commerciales aux petits prêts des IMF) et d'aider ces derniers à accéder aux services financiers dont ils ont besoin, notamment les prêts pour les entreprises, l'éducation et les services médicaux de base, ont massivement intégré le protocole Kiva. Kiva conçoit actuellement le système qui enregistrera ces transactions au moyen d'infrastructures basées sur des DLT libres et soutenues par la Fondation Linux.

Les composantes de l'écosystème des évaluations de crédit numériques sont les suivantes:

- **L'identification numérique et le processus d'e-KYC**
L'identifiant numérique mis en place par le Bureau national de l'état civil (NCRA) rend possible l'identification unique et universelle de tous les citoyens. Cette approche permet de fédérer et de profiler les crédits avec précision. En outre, cet identifiant numérique peut faire l'objet d'une vérification reposant sur le processus d'e-KYC.
- **Évaluation de crédit**
Les fournisseurs de services financiers communiquent leurs données de crédit à l'agence d'évaluation du crédit, le seul bureau de crédit à l'échelle nationale, par ailleurs hébergé par la Banque centrale de la Sierra Leone. Ces évaluations sont réalisées par des API intégrées aux plateformes des fournisseurs de services financiers.
- **Vérification des antécédents en matière de crédit**
L'agence d'évaluation du crédit génère des évaluations ainsi que des scores de crédit sur la base des antécédents de crédit du sujet, avec son consentement.
- **Évaluation du risque fondée sur les données**
L'enregistrement exhaustif des crédits permet aux fournisseurs de services financiers d'évaluer les risques et de définir des taux compétitifs avec efficacité.

Les figures 27, 28 et 29 présentent les architectures de haut niveau de l'identité, des évaluations de crédit et de l'écosystème global.

Au moment de la rédaction du présent document, les partenaires avaient déployé la solution d'identification en question au sein du Bureau national de l'état civil, et intégré la vérification reposant sur le processus e-KYC ainsi que les évaluations de crédit au fonctionnement de l'ensemble des institutions financières de la Sierra Leone. La documentation détaillée relative à cette solution sera publiée en 2020, année lors de laquelle le système sera opérationnel et les intégrations mises à la disposition des autres participants de l'écosystème financier de la Sierra Leone.

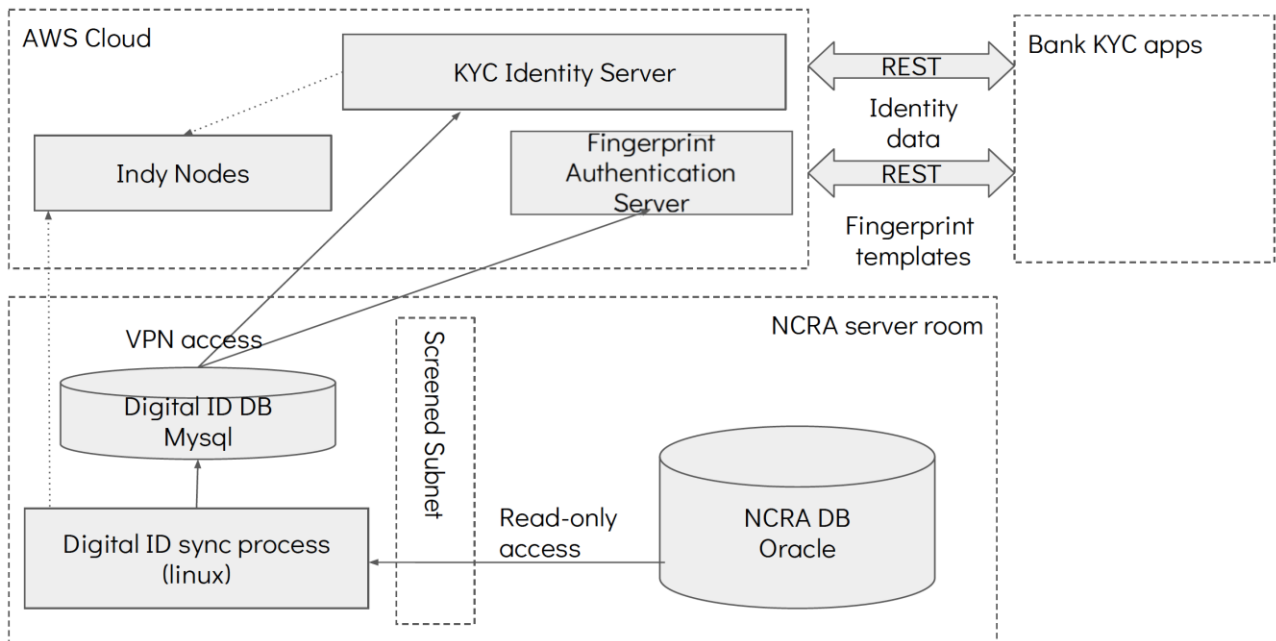


Figure 27 – Infrastructure d'identité du Bureau national de l'état civil

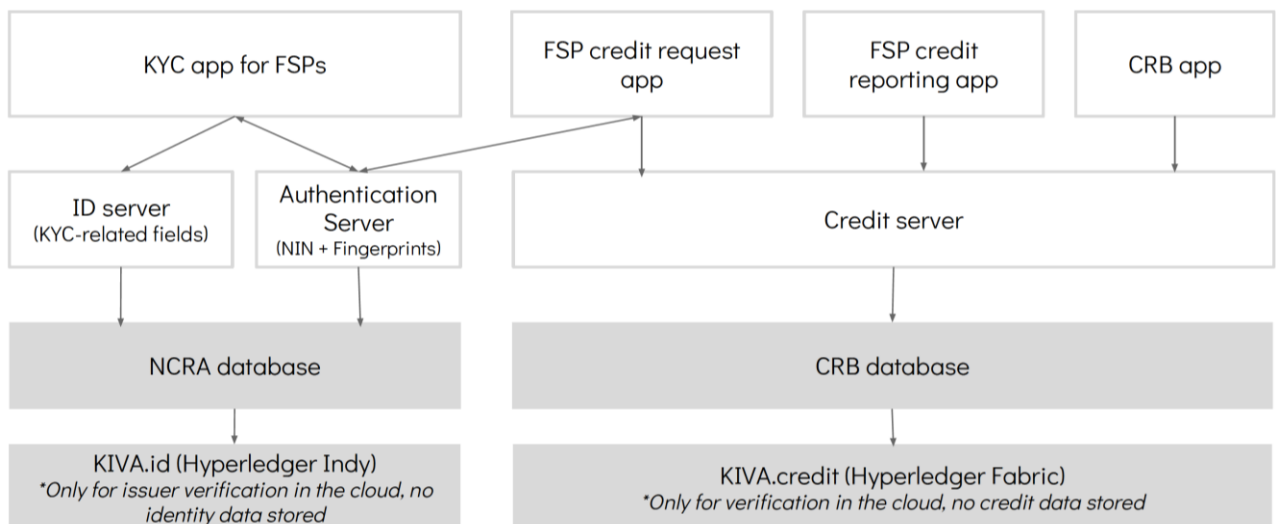


Figure 28 – Architecture de l'écosystème d'évaluation de crédit numérique

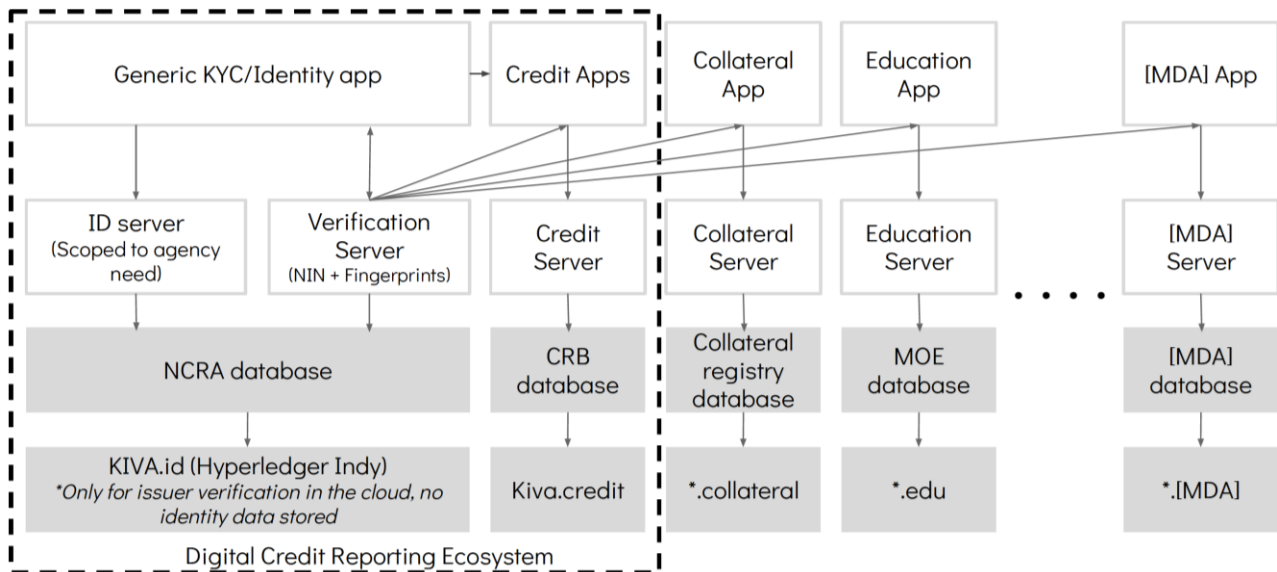


Figure 29 – Architecture de l'écosystème

7.1.3 Exemple: Exemple d'inscription avec K-FIDO

Cette section présente un cas d'utilisation fondé sur la spécification FIDO. Elle décrit la façon dont la K-FIDO a combiné la spécification FIDO UAF et la PKI pour authentifier et vérifier simultanément des identifiants dans le cadre du déploiement commercial de technologies financières en Corée. La spécification K-FIDO sera publiée par l'Agence coréenne de l'Internet et de la sécurité (KISA) afin que les services de certification biométrique accrédités soient en mesure de fournir des certificats accrédités sans mot de passe en Corée à l'aide de l'authentification FIDO.

L'identifiant national coréen est utilisé dans le cadre de l'identification hors ligne et contient un numéro de résident unique. Afin de faciliter l'identification et l'authentification privées et sécurisées en ligne, il est possible de générer un numéro d'identification personnel Internet (i-PIN) appuyé par un certificat PKI émis par un nombre restreint de fournisseurs de services et de l'associer au numéro de résident. La figure 30 illustre cette relation.

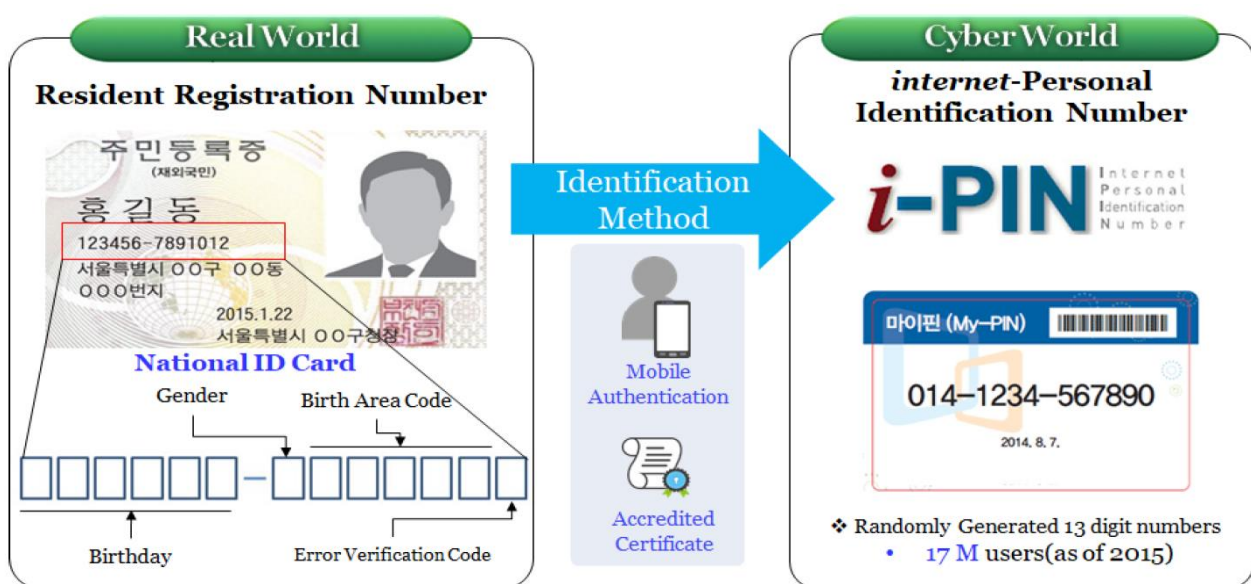


Figure 30 – Identifiant national et i-PIN en République de Corée

Lorsqu'un citoyen cherche à s'identifier sur un service Internet qui requiert une méthode d'identification en ligne (c'est-à-dire à distance), plusieurs moyens s'offrent à lui; par exemple, par certificat accrédité, par téléphone portable, par compte bancaire ou encore, par carte de crédit.

Les fournisseurs de services en ligne peuvent adopter des méthodes d'identification telles que les certificats accrédités, l'authentification mobile, i-PIN, K-FIDO ou FIDO en fonction des niveaux de garantie d'authentification requis.

Le citoyen doit s'enregistrer afin de connecter son certificat PKI et son i-PIN à son appareil mobile compatible avec la spécification FIDO. Une fois enregistrées, les données d'identification du citoyen peuvent être communiquées à d'autres fournisseurs de services au terme d'une authentification FIDO forte.

La figure 31 présente le processus d'enregistrement.

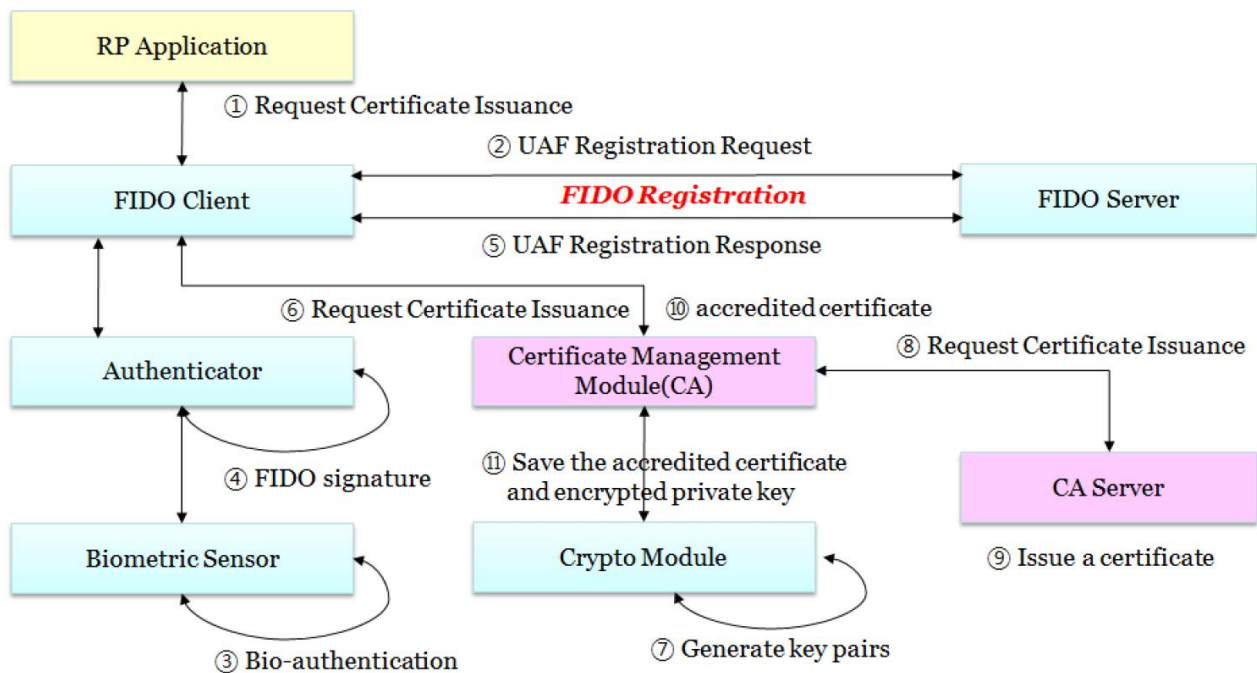


Figure 31 – Processus d'enregistrement du service K-FIDO

- ① L'application de la partie utilisatrice lance le bio-enregistrement et demande à ce qu'un certificat d'utilisateur soit émis.
- ② Le serveur FIDO envoie une demande d'enregistrement UAF au client FIDO.
- ③ L'utilisateur effectue une bio-authentification auprès des authenticateurs FIDO selon leurs méthodes de vérification de l'utilisateur respectives, par exemple par empreinte digitale, par balayage de l'iris, etc.
- ④ L'authenticateur FIDO sélectionné génère la clé privée d'authentification FIDO. L'authenticateur FIDO sélectionné génère une signature FIDO à l'aide de la clé privée d'attestation.
- ⑤ Le serveur FIDO vérifie la signature à l'aide de la clé publique d'attestation et vérifie la clé publique d'authentification. Une fois la vérification effectuée, le serveur FIDO fait confiance à l'authenticateur auquel il s'adresse ainsi qu'à la clé publique d'authentification envoyée par l'authenticateur dans la réponse d'authentification. Le serveur FIDO vérifie si le message d'enregistrement FIDO a été transmis. Le cas échéant, le serveur FIDO stocke la clé publique d'authentification.

- ⑥ Le client FIDO demande à ce que le certificat de l'utilisateur soit délivré au module de gestion des certificats.
- ⑦ Le module cryptographique génère une paire de clés privée et publique pour le certificat de l'utilisateur.
- ⑧ Le module de gestion des certificats demande à ce que l'autorité de certification délivre le certificat de l'utilisateur.
- ⑨ Le module de gestion des certificats stocke le certificat de l'utilisateur et la clé privée dans un élément sécurisé tel que USIM, Trustzone, etc. La clé privée doit toutefois être chiffrée par une clé de chiffrement dans l'élément keyStore ou keyChain. Le processus d'enregistrement est terminé.

Remarque sur l'identité de l'utilisateur:

- Avant l'étape 6, lors de laquelle le client FIDO demande à ce qu'un certificat d'utilisateur soit émis, l'utilisateur est supposé s'être identifié par l'intermédiaire de l'un des mécanismes suivants: authentification mobile, certificat accrédité, authentification du compte bancaire, etc. À la sixième étape, l'identité de l'utilisateur est donc connue.
- Une fois identifié, il utilise l'authentification FIDO tant qu'elle n'est pas étroitement couplée. Les scénarios les plus courants sont les suivants:
 - 1) L'utilisateur s'identifie selon les modalités d'identification du fournisseur de services.
 - 2) L'utilisateur utilise le service FIDO ou K-FIDO (la portée de K-FIDO).
- Les authenticateurs décident où doivent être stockés les certificats des utilisateurs. La KISA recommande notamment l'utilisation des éléments sécurisés suivants: keyStore, keyChain, USIM ou encore Trustzone.

7.1.4 Exemple: Identité numérique à Zoug – Identité numérique basée sur la blockchain de l'Ethereum

Depuis le mois de novembre 2017, la ville suisse de Zoug a délivré des identifiants numériques basés sur la blockchain à l'ensemble de ses 30 000 citoyens. [17]

L'identifiant numérique de Zoug comporte trois composantes. D'abord, le coffre-fort numérique, qui fait partie de l'application mobile et contient l'identifiant numérique chiffré. Il peut être déverrouillé par son propriétaire par un moyen biométrique ou à l'aide d'un code PIN. La deuxième composante est la blockchain Ethereum, par l'intermédiaire de laquelle l'application crée une adresse chiffrée unique pour son détenteur. Enfin, le portail de certification, que les autorités utilisent pour vérifier que le demandeur est bien un résident de Zoug.

Une fois le nom, l'adresse, la date de naissance, la nationalité et le numéro de passeport ou de carte d'identité du demandeur vérifiés, ces données sont signées numériquement par la ville de Zoug. Cette signature est par la suite stockée sous forme de certificat dans le coffre-fort numérique du citoyen. La clé publique de la ville étant accessible au public à partir de la blockchain Ethereum, toute personne recevant un identifiant numérique peut facilement en vérifier l'authenticité.

Une fois le contrôle réussi, la ville de Zoug – qui dispose également d'une identité numérique dans la blockchain, mais avec des privilèges spéciaux – signe le contrat d'identité de l'utilisateur, que chacun peut consulter et vérifier sur Internet. La responsabilité de cette identité spéciale incombe au greffier de la ville de Zoug.

Le propriétaire de l'identifiant numérique peut alors fournir ses informations d'identité grâce à l'application mobile. Pour valider l'authenticité de ces données, il suffit de vérifier leur signature numérique dans la blockchain.

Zoug a organisé une consultation auprès des titulaires d'identité numérique au deuxième trimestre 2018 afin de recueillir des idées sur un système de vote électronique fondé sur la nouvelle identité numérique.

7.1.5 Exemple: Exemple d'inscription avec FIDO

Les spécifications de la FIDO, dans une perspective de clarté et de rigueur, ont pris la décision de séparer l'étape de contrôle d'identité de l'étape d'inscription. Cette séparation accroît la modularité de l'architecture afin que n'importe quelle technique de contrôle de l'identité puisse être combinée avec l'inscription avec FIDO, y compris avec Alipay, l'e-KYC Aadhaar, les identifiants PKI existants (tels que la K-FIDO ci-dessus) ainsi que divers niveaux de garantie NIST/FIPS.

Idéalement, l'architecture de la FIDO doit être constituée de telle sorte que le contrôle de l'identité soit effectué en une fois, puis que l'identité soit associée à des identifiants sécurisés, y compris à l'aide de technologies de chiffrement.

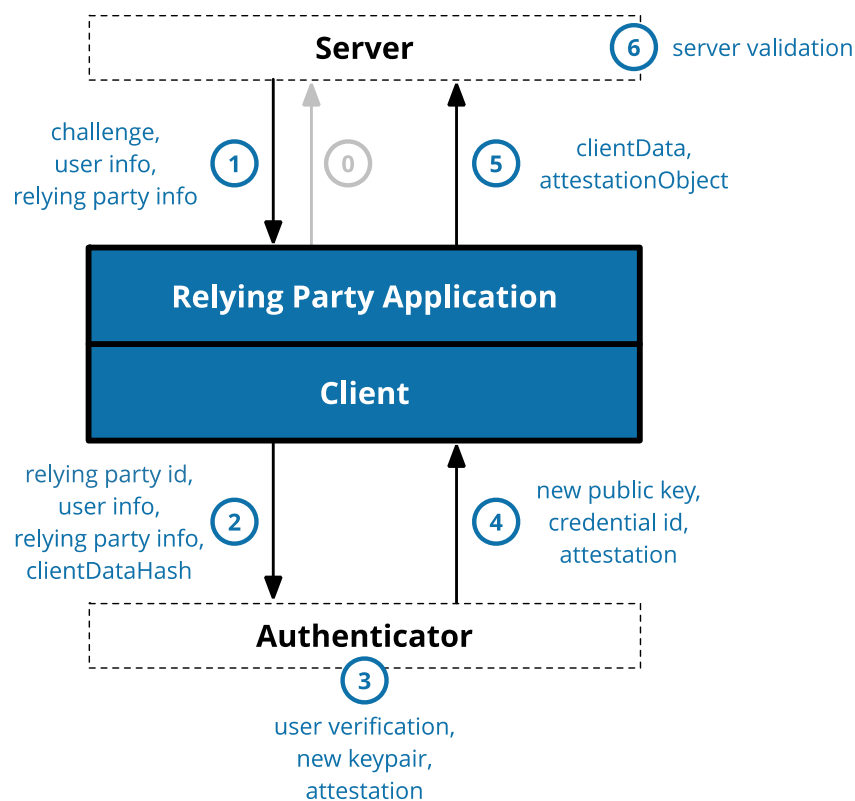


Figure 32 – Processus d'enregistrement de la norme FIDO

Le processus d'inscription se déroule comme suit:

- ⑥ **L'application demande l'inscription:** l'application dépose la demande d'inscription initiale au terme du contrôle d'identité/du processus KYC dans la même session ou le même environnement de confiance.
- ① **Le serveur émet une demande de récusation ainsi que des informations sur l'utilisateur et la partie utilisatrice:** le serveur émet une demande de récusation, des informations sur l'utilisateur ainsi que des informations sur la partie utilisatrice à l'application de la partie utilisatrice. L'application de la partie utilisatrice peut être une application mobile, Web, native ou autre, et sa mise en œuvre n'entre pas dans le cadre des spécifications de la FIDO. Le protocole de communication avec le serveur n'est pas spécifié et ne relève pas non plus de la

FIDO. En règle générale, les communications avec le serveur se font entre l'architecture REST et le protocole TLS. Elles peuvent toutefois également être effectuées par le biais de SOAP, RFC 2549 ou de tout autre protocole, à condition que le canal de communication soit sécurisé. Les paramètres reçus du serveur sont alors transmis au client pour créer les identifiants, généralement sans qu'aucune modification, ou presque, ne soit requise.

- ② **Le client appelle authenticatorMakeCredential sur l'authentificateur par l'intermédiaire du CTAP:** en interne, le client valide les paramètres et renseigne les valeurs par défaut, qui deviennent alors le clientData. Parmi ces paramètres, le plus important est l'origine. Celle-ci est enregistrée dans le clientData pour que le serveur puisse la vérifier ultérieurement. Les paramètres de l'appel credentialCreate sont transmis à l'authentificateur, de même qu'un hachage des clientData réalisé avec un SHA-256 (seul un hachage est envoyé, car il est possible que l'authentificateur soit associé à un lien NFC ou Bluetooth à faible bande passante; l'authentificateur va simplement apposer sa signature sur le hachage pour s'assurer qu'il n'est pas altéré).
- ③ **L'authentificateur crée une nouvelle paire de clés et une attestation:** avant toute chose, l'authentificateur demande généralement à ce que l'utilisateur soit vérifié à l'aide d'un code PIN, d'une empreinte digitale, d'un balayage de l'iris, etc. afin de prouver que l'utilisateur est présent et qu'il consent à l'enregistrement. Une fois l'utilisateur vérifié, l'authentificateur crée une nouvelle paire de clés asymétriques et stocke en toute sécurité la clé privée à titre de référence. La clé publique intègre alors l'attestation, que l'authentificateur signe à l'aide d'une clé privée gravée dans l'authentificateur au cours de son processus de fabrication et dont la chaîne de certificats peut être validée par une base de confiance.
- ④ **L'authentificateur renvoie les données au client:** la nouvelle clé publique (un identifiant unique au monde) ainsi que d'autres données d'attestation sont renvoyées au client. Elles deviennent alors l'attestationObject.
- ⑤ **Le client crée les données finales, l'application envoie la réponse au serveur:** l'appel authenticatorMakeCredential renvoie un PublicKeyCredential, dont le rawId est l'identifiant unique, ainsi que la réponse d'attestation de l'authentificateur contenant le clientData et l'attestationObject. L'identifiant PublicKeyCredential est renvoyé au serveur avec le formatage et le protocole souhaités.
- ⑥ **Le serveur valide et finalise l'enregistrement:** enfin, le serveur doit effectuer une série de contrôles pour s'assurer que l'enregistrement est achevé et qu'il n'a pas été altéré. Ces contrôles visent notamment à:
 1. Vérifier que la récusation est identique à celle qui a été envoyée.
 2. S'assurer que l'origine est conforme aux attentes.
 3. Valider la signature du clientDataHash et de l'attestation à l'aide de la chaîne de certificats pour ce modèle d'authentificateur

La spécification WebAuthn [9] comprend une liste complète des étapes de validation. En supposant que les vérifications sont correctes, le serveur stocke la nouvelle clé publique associée au compte de l'utilisateur pour une utilisation ultérieure – à chaque fois que l'utilisateur souhaitera utiliser la clé publique pour s'authentifier.

7.1.6 Exemple: Inscription d'un utilisateur d'un prestataire de soins de santé

Prenons l'exemple du processus d'inscription en ligne d'un prestataire de soins de santé. Ce processus tente d'abord d'intégrer un nouveau membre à l'aide des informations sur les attributs du client, puis détermine si les attributs présentés lors de l'inscription sont utilisables. L'objectif stratégique consiste

à améliorer l'expérience utilisateur ainsi que le processus d'identification des membres au moment de l'inscription, de pair avec d'autres processus d'authentification internes.

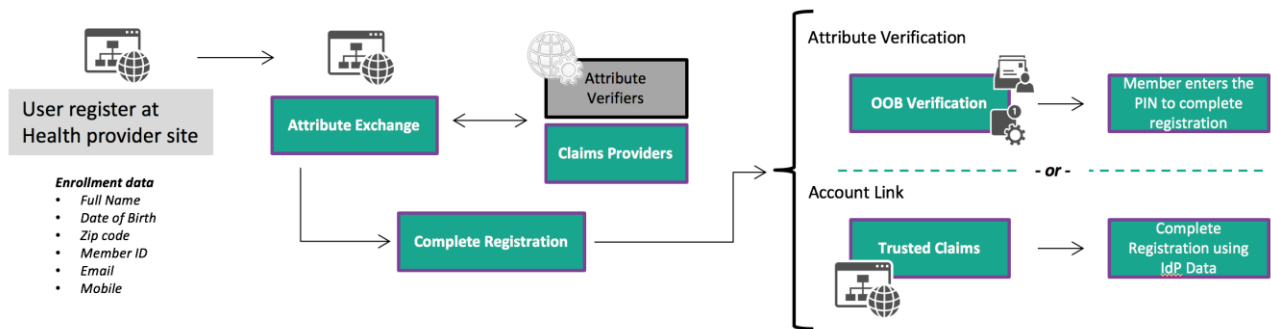


Figure 33 – Inscription d'un utilisateur d'un prestataire de soins de santé

Option 1: Liaison de comptes fédérés

Lors de son inscription en ligne, le membre peut sélectionner une option afin d'effectuer une vérification d'identité par l'intermédiaire d'un fournisseur d'identité de confiance (par exemple, une banque).

Il est alors redirigé vers la banque (fournisseur d'identité ou fournisseur d'attributs) conformément aux normes de fédération. Le membre s'authentifie auprès du fournisseur d'identité. Le prestataire de soins de santé obtient des informations sur l'utilisateur auprès du fournisseur d'identité, qu'il compare alors aux données de l'utilisateur initialement recueillies.

Le membre est autorisé à terminer son inscription auprès du prestataire de soins de santé.

Option 2: Vérification des attributs

Plutôt que d'assigner des attributs au prestataire de soins de santé pour qu'il les utilise et les évalue après avoir authentifié l'utilisateur, le prestataire de soins de santé envoie au fournisseur d'identité (avec le consentement de l'utilisateur) les attributs recueillis lors de l'inscription.

Le fournisseur d'identité fournit alors une réponse indiquant la qualité ou l'exactitude des attributs collectés lors de l'inscription. Le prestataire de soins de santé termine l'inscription du membre à l'aide des techniques de vérification hors bande.

7.2 Cas d'utilisation: Authentification pour accéder à un service financier numérique

Les exemples du cas d'utilisation relatif à l'authentification d'entité décrivent la façon dont les mécanismes d'authentification de nouvelle génération sont exploités pour identifier une personne et l'autoriser à utiliser des services.

7.2.1 Exemple: Exemple d'utilisation de l'IFAA – paiement par empreinte digitale/reconnaissance faciale avec Alipay

Alipay est l'application de paiement mobile la plus populaire de Chine. Elle prend en charge l'authentification par empreinte digitale ou par reconnaissance faciale dans le cadre des transferts d'argent réalisés depuis un appareil mobile.

Le processus d'authentification d'Alipay repose sur le modèle local de l'IFAA et se base sur le protocole d'authentification de l'IFAA, comme l'illustre la figure 16.

La figure 34 consiste en une capture d'écran de l'application Alipay.

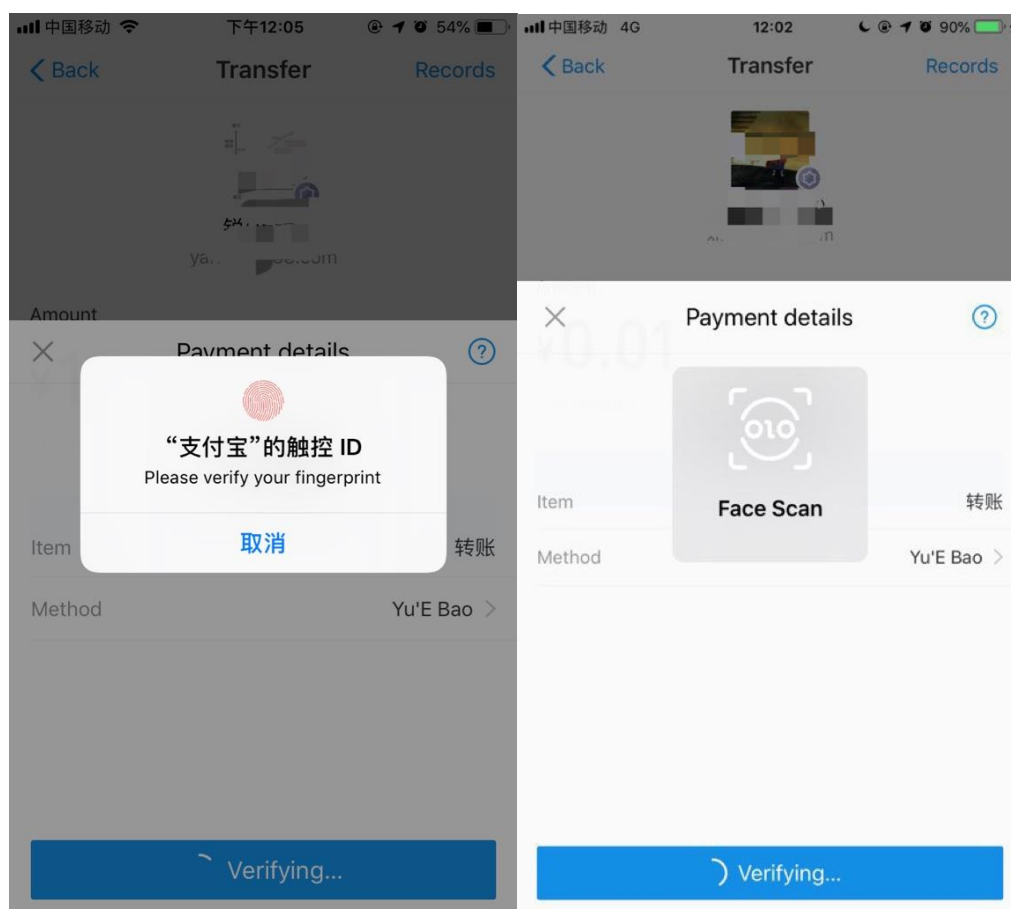


Figure 34 – Cas d'utilisation de l'IFAA: paiement par empreinte digitale/reconnaissance faciale avec Alipay

La figure 35 présente l'infrastructure technique du système d'authentification d'Alipay.

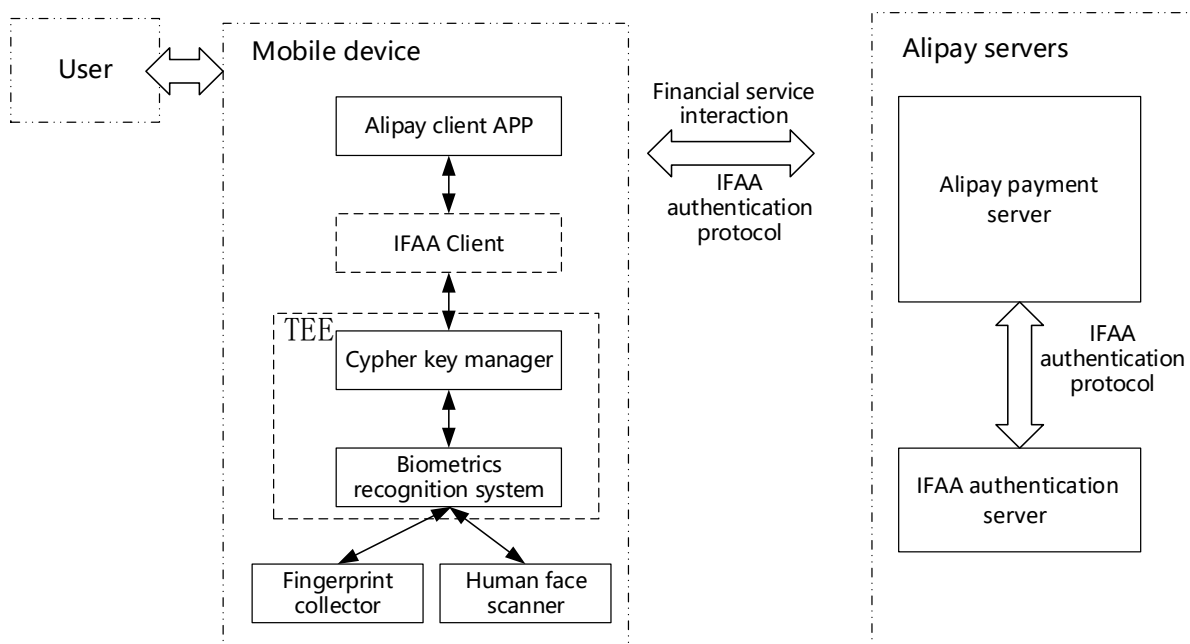


Figure 35 – Cas d'utilisation de l'IFAA: paiement par empreinte digitale/reconnaissance faciale avec Alipay – Infrastructure technique

L'utilisateur d'Alipay lance d'abord la demande d'inscription par l'intermédiaire de l'application client Alipay, puis exécute le processus d'inscription comme indiqué dans la figure 15. Une fois l'inscription réussie, l'utilisateur lance une demande de paiement par l'intermédiaire l'application client Alipay.

Avant d'initier le processus de paiement, l'application client Alipay interagit avec le serveur de paiement d'Alipay pour vérifier que le paiement mobile peut être effectué. Le cas échéant, l'application client Alipay appelle le gestionnaire de clés (ou, de manière facultative, le client IFAA) pour authentifier l'utilisateur de la manière suivante:

- 1) L'application demande à l'utilisateur d'effectuer une authentification par empreinte digitale/reconnaissance faciale sur la base du modèle local.
- 2) Une fois la vérification par empreinte digitale/reconnaissance faciale effectuée, le gestionnaire de clés invoque la clé privée d'authentification de l'utilisateur stockée localement afin de signer les informations de la transaction, qu'il envoie par la suite au serveur de paiement d'Alipay par l'intermédiaire de l'application client Alipay.
- 3) Le serveur de paiement d'Alipay envoie les informations d'authentification au serveur d'authentification de l'IFAA à des fins de vérification et en récupère les résultats.
- 4) Le serveur de paiement d'Alipay autorise le paiement une fois la vérification effectuée.

7.2.2 Exemple: Authentification Aadhaar

L'authentification Aadhaar est le processus par lequel le numéro Aadhaar ainsi que d'autres attributs, notamment les données biométriques, sont soumis en ligne au référentiel central de données d'identités pour être vérifiés sur la base des informations, données ou documents disponibles. Au cours de l'opération d'authentification, le dossier du résident est d'abord sélectionné à l'aide du numéro Aadhaar, puis les données démographiques et biométriques sont comparées aux données stockées fournies par le résident au cours du processus d'inscription ou de mise à jour. L'authentification peut également être effectuée en utilisant un OTP. Tous les systèmes d'authentification biométrique ou par OTP sont également compatibles avec le service d'e-KYC.

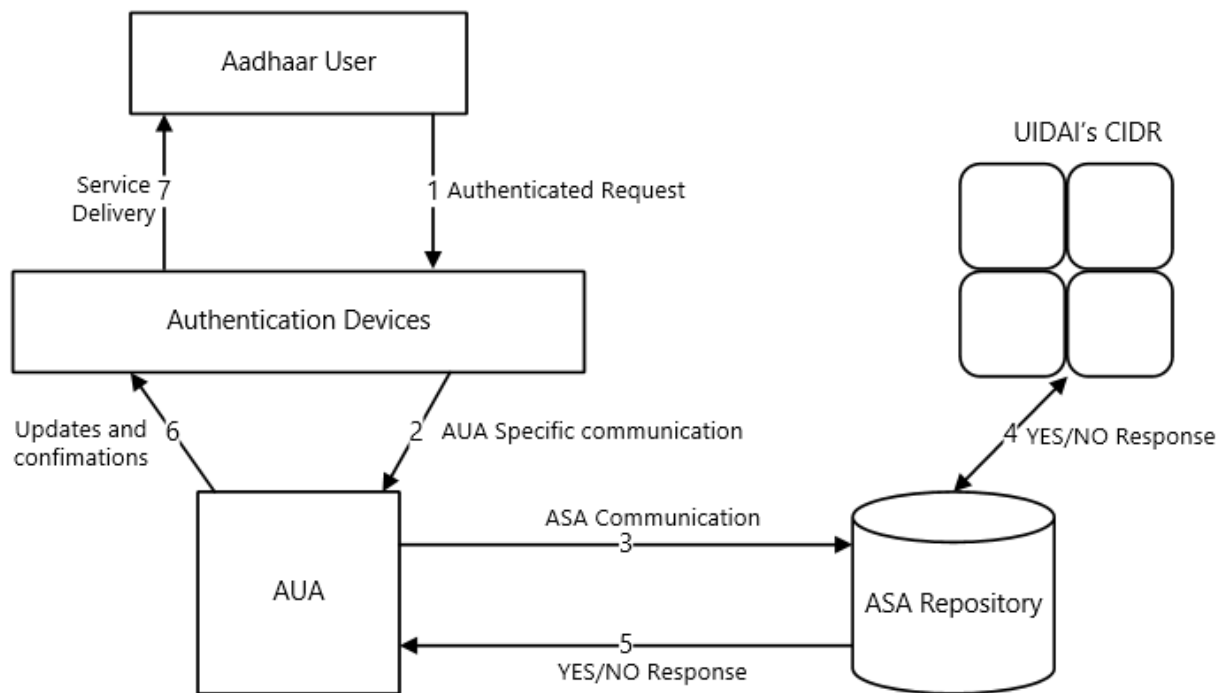


Figure 36 – Processus technique des services d'authentification et d'e-KYC

Voici les principales étapes du processus d'authentification Aadhaar telles qu'illustrées dans la figure 36 ci-dessus:

- Le titulaire de la carte Aadhaar envoie la demande d'authentification par l'intermédiaire de son appareil.
- Le logiciel d'application chargé de l'authentification Aadhaar installé sur l'appareil chiffre et envoie les données au serveur de l'AUA.
- Celui-ci, après validation, ajoute les en-têtes nécessaires (wrapper XML spécifique à l'AUA avec clé de licence, signature, etc.) et transmet la demande au référentiel central de données d'identités de l'UIDAI par le biais du serveur de l'ASA.
- Le serveur d'authentification Aadhaar répond par oui ou non en fonction de la correspondance des paramètres d'entrée.
- Selon la réponse du serveur d'authentification Aadhaar, l'AUA ou la sous-AUA effectue la transaction et le titulaire de la carte Aadhaar reçoit le service.

Fonctions de sécurité supplémentaires des services d'authentification et de KYC:

- Afin de renforcer la sécurité de l'écosystème d'authentification Aadhaar, en vertu des règlements 14(n) et 19(o) de 2016 de la réglementation relative au système d'authentification Aadhaar, il a été décidé qu'il est obligatoire d'utiliser un module matériel de sécurité (HSM) pour signer numériquement le fichier XML d'authentification et déchiffrer les données du processus d'e-KYC.
- Concernant la signature numérique du fichier XML autorisé, la demande d'authentification est signée numériquement par l'entité requérante (AUA/KUA) et/ou par l'ASA utilisant le

HSM, selon l'accord mutuel convenu. Cependant, pour déchiffrer les données de réponse du processus d'e-KYC transmises par l'UIDAI, la KUA doit utiliser son propre HSM.

- Le HSM à utiliser pour signer le fichier XML d'authentification ainsi que pour déchiffrer les données du processus d'e-KYC est conforme à la norme FIPS 140-2.
- Toutes les AUA/KUA/ASA assurent la mise en place du HSM dans les services d'authentification Aadhaar.
- Pour arrêter l'utilisation de données biométriques stockées, l'UIDAI a rendu obligatoire l'utilisation d'appareils enregistrés par les AUA/KUA ainsi que les ASA. Par rapport aux appareils publics, les appareils enregistrés offrent les fonctionnalités supplémentaires suivantes:
- Identification de l'appareil: chaque appareil doit disposer d'un identifiant unique afin d'en permettre la traçabilité et l'analyse ainsi que d'améliorer la gestion des fraudes.
- Interdiction d'utiliser des données biométriques stockées: les données biométriques sont signées dans l'appareil à l'aide de la clé du fournisseur afin de garantir qu'elles sont effectivement capturées en temps réel. Le service des appareils enregistrés du fournisseur de l'appareil doit ensuite constituer le bloc de données d'identité personnelles chiffrées avant de retourner à l'application hôte.

7.2.3 Exemple: Authentification avec K-FIDO

Plusieurs méthodes d'authentification de l'utilisateur utilisées sur les portails Web, dans le cadre des transactions électroniques ainsi qu'auprès des institutions financières et des services d'administration en ligne, sont généralement prises en charge. La figure 37 présente le processus d'authentification avec K-FIDO.

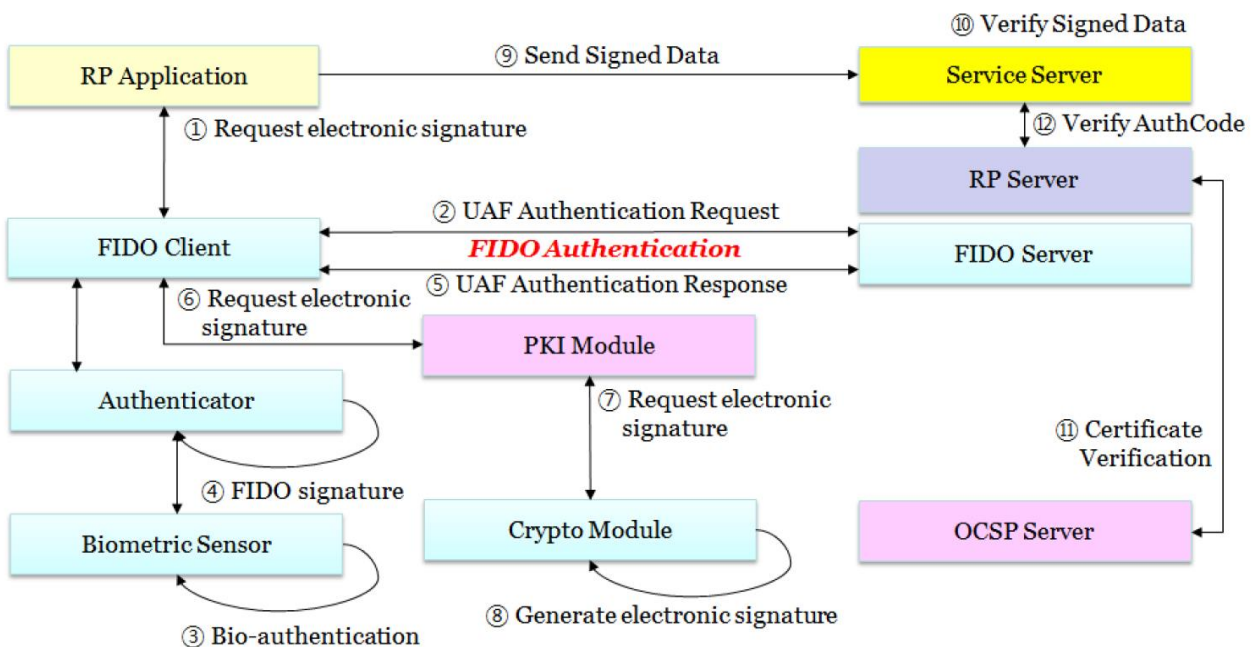


Figure 37 – Processus d'authentification du service K-FIDO

- ① L'application de la partie utilisatrice réalise une bio-authentification et demande la signature électronique d'un fournisseur de services.

- ② Le serveur FIDO envoie une demande d'authentification UAF au client FIDO.
- ③ L'utilisateur procède à sa bio-authentification auprès de l'authentificateur FIDO en suivant la même méthode que lors de l'enregistrement.
- ④ L'authentificateur FIDO génère une signature FIDO (à l'aide de la clé privée d'authentification FIDO).
- ⑤ Le client FIDO envoie la réponse d'authentification UAF au serveur FIDO. Le serveur FIDO vérifie le message d'authentification FIDO. S'il est validé, le serveur de la partie utilisatrice génère alors un code d'autorisation.
- ⑥ Le client FIDO demande au module PKI de générer une signature électronique.
- ⑦ Le module PKI demande au module cryptographique de générer une signature électronique.
- ⑧ En présence d'éléments sécurisés tels que Trustzone ou USIM, la signature électronique est générée par la clé privée depuis l'élément sécurisé. S'il s'agit toutefois de l'élément keyStore ou keyChain, la clé privée chiffrée doit alors y être déchiffrée par une clé de déchiffrement stockée et la signature électronique doit être générée par la clé privée avec le module cryptographique.
- ⑨ L'application de la partie utilisatrice envoie les données signées au serveur du service.
- ⑩ Le serveur du service vérifie les données signées.
- ⑪ Le serveur du service ou le serveur de la partie utilisatrice vérifient depuis le serveur OCSP que le certificat de l'utilisateur a été vérifié.
- ⑫ Le serveur du service vérifie le code d'autorisation du fournisseur de service FIDO. Le serveur du service envoie par la suite le résultat à l'utilisateur.

7.2.4 Exemple: Authentification du client d'un prestataire de soins de santé

Un important prestataire de soins de santé a entamé le processus pluriannuel de déploiement de sa plateforme d'authentification de nouvelle génération sur les applications mobiles et Web. Il établit ainsi de nouvelles pratiques exemplaires qui, par l'intermédiaire d'une approche à deux volets de l'authentification forte, améliorent l'accès aux soins de santé. En adoptant l'authentification FIDO sans mot de passe, en optant pour la vérification biométrique des identifiants de comptes en ligne de ses clients et au moyen d'un chiffrement à clé publique forte et inaltérable, ce prestataire a réduit sa dépendance à l'égard des "secrets partagés" vulnérables tels que les mots de passe et les codes d'accès à usage unique.

Bien que le déploiement d'une authentification forte basée sur des normes telles que la FIDO permette de résoudre de nombreux problèmes d'authentification auxquels sont confrontées les organisations en matière de sécurité et d'expérience utilisateur, les prestataires de soins de santé doivent tenir compte des risques relatifs à la perte ou au vol d'appareils. C'est pourquoi ce prestataire de soins de santé déploie la deuxième composante centrale de la plateforme d'authentification de nouvelle génération – l'authentification continue basée sur le comportement – afin de s'assurer que l'utilisateur authentifié soit le même tout au long de la session. Pour ce faire, il passe en revue plusieurs attributs de l'utilisateur (tels que la façon dont il tient son téléphone) et lui attribue un score de risque afin de déterminer le niveau d'accès qu'il peut lui accorder pendant une session. S'il détecte un risque élevé au cours d'une session, le prestataire de soins peut demander des informations supplémentaires à l'utilisateur avant de l'autoriser à poursuivre son opération depuis son appareil.

7.2.5 Exemple: SK Telecom – Mobile Connect

SK Telecom dessert 28 des 57 millions d'abonnés de la Corée du Sud; il s'agit du plus grand opérateur de réseaux mobiles du pays, et l'un des premiers à exploiter le potentiel des services d'identification. Dès 2005, il commercialise T-Auth, sa propre solution d'identité mobile, qui combine authentification mobile et mise en correspondance des attributs.

Cet opérateur s'est rendu compte qu'il pouvait tirer parti de la réglementation coréenne, qui exige des fournisseurs de contenu qu'ils vérifient que les clients qui souhaitent accéder à un type de contenu y

soient autorisés. En d'autres mots, ils sont chargés de vérifier que les clients qui souhaitent acheter du contenu ont la majorité civile. SKT a découvert que les informations relatives à ses comptes clients pouvaient aider les fournisseurs de services à satisfaire à cette exigence. L'opérateur a donc conçu T-Auth à cette fin tout en veillant à avoir le moins d'impact possible sur l'expérience utilisateur.

Le parcours utilisateur conçu par SKT limite au maximum les contraintes d'authentification. La figure 38 montre un flux d'authentification typique: le client tente d'accéder à une application du fournisseur de services et est redirigé vers l'application mobile T-Auth afin qu'il s'y authentifie; il saisit ensuite son code PIN ainsi qu'un échantillon biométrique; si l'authentification est réussie, T-Auth envoie le résultat ainsi que les données d'attribut au fournisseur de services.

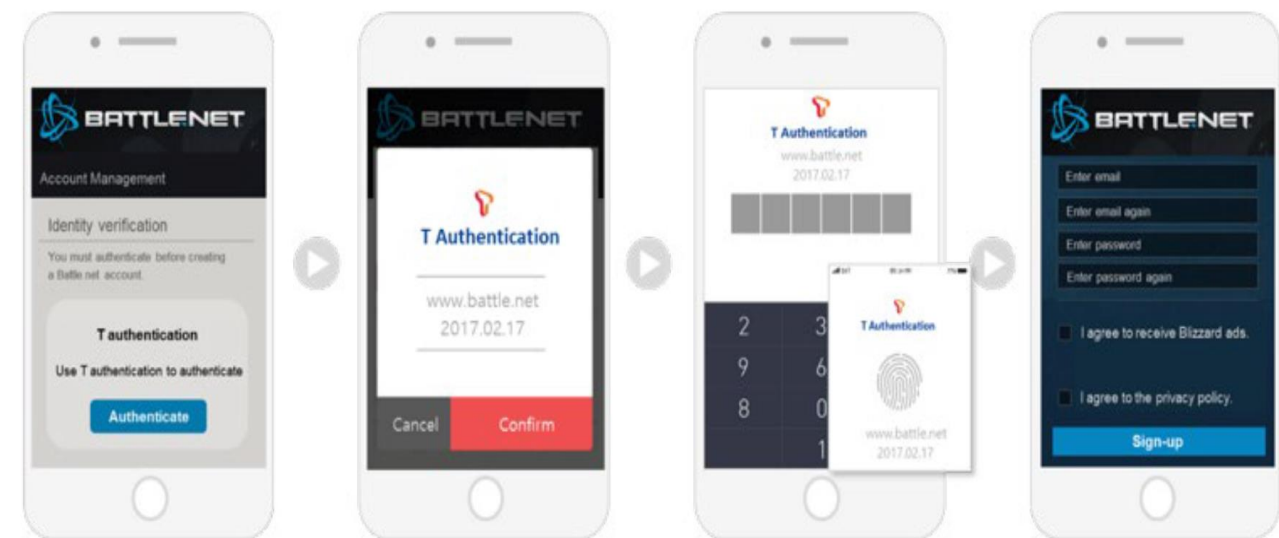


Figure 38 – Parcours d'authentification de l'utilisateur sur un compte de jeu avec T-Auth

Au début de l'année 2017, SKT s'est mise en conformité avec les spécifications de Mobile Connect, le cadre mondial d'authentification, d'autorisation et d'identification des opérateurs mobiles. T-Auth est par conséquent désormais interopérable avec les solutions d'authentification et d'identification mobiles des opérateurs non coréens.

7.2.6 Exemple: Authentification avec K-FIDO

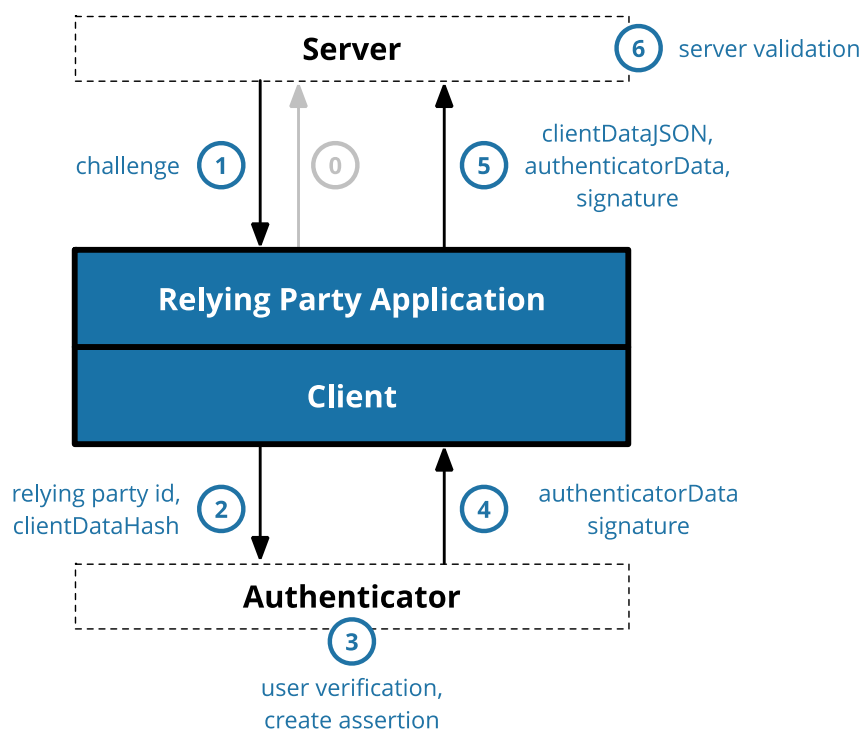


Figure 39 – Processus d'authentification de la norme FIDO

- ① **L'application demande l'authentification:** l'application émet la demande d'authentification initiale. Le protocole et le format de cette demande n'entrent pas dans le cadre de la FIDO.
- ① **Le serveur émet une demande de récusation:** le serveur envoie une demande de récusation à l'application. Le protocole de communication avec le serveur n'est pas spécifié et ne relève pas de la FIDO. En règle générale, les communications avec le serveur se font entre l'architecture REST et le protocole TLS. Elles peuvent toutefois également être effectuées par le biais de SOAP, RFC 2549 ou de tout autre protocole, à condition que le protocole soit sécurisé. Les paramètres reçus du serveur sont alors transmis à l'appel credentialGet, généralement sans qu'aucune modification, ou presque, ne soit requise.
- ② **Le client appelle authenticatorGetCredential sur l'authenticateur par l'intermédiaire du CTAP:** en interne, le client valide les paramètres et renseigne les valeurs par défaut, qui deviennent alors le clientData. Parmi ces paramètres, le plus important est l'identifiant de la partie utilisatrice. Il est enregistré dans le clientData pour que le serveur puisse le vérifier ultérieurement. Les paramètres de l'appel credentialGet sont transmis à l'authenticateur, de même qu'un hachage des clientData réalisé avec un SHA-256 (seul un hachage est envoyé, car il est possible que l'authenticateur soit associé à un lien NFC ou Bluetooth à faible bande passante; l'authenticateur va simplement apposer sa signature sur le hachage pour s'assurer qu'il n'est pas altéré).
- ③ **L'authenticateur crée une assertion:** l'authenticateur trouve pour ce service un identifiant qui correspond à celui de la partie utilisatrice, puis invite l'utilisateur à consentir à l'authentification. Si ces deux étapes sont franchies avec succès, l'authenticateur crée alors une nouvelle assertion en signant les données clientDataHash et authenticatorData avec la clé privée générée pour ce compte lors de l'appel d'enregistrement.
- ④ **L'authenticateur renvoie les données au client:** l'authenticateur renvoie les données authenticatorData ainsi que la signature de l'assertion au client.

- ⑤ **Le client crée les données finales, l'application envoie la réponse au serveur:** l'appel `authenticatorGetCredential` renvoie un identifiant `PublicKeyCredential` avec la réponse d'assertion de l'authentificateur. L'application transmet par la suite ces données au serveur à l'aide du protocole souhaité et dans le format de son choix.
- ⑥ **Le serveur valide et finalise l'authentification:** une fois le résultat de la demande d'authentification reçu, le serveur valide la réponse, par exemple:
1. En utilisant la clé publique stockée lors de la demande d'enregistrement pour valider la signature de l'authentificateur.
 2. En s'assurant que la récusation signée par l'authentificateur correspond à celle que le serveur a générée.
 3. En vérifiant que l'ID de la partie utilisatrice est celui qui est attendu pour ce service.

La spécification WebAuthn [9] comprend une liste complète des étapes de validation des assertions. Si la validation est réussie, le serveur prend note de l'authentification de l'utilisateur (par exemple, en attribuant un fanion à la session, en plaçant un cookie, etc.).

8 Conclusion

Ce rapport décrit deux des fonctions de base des DFS: l'identification initiale des clients au moment de l'inscription et l'authentification forte des clients qui souhaitent y accéder par la suite. Sans elles, il est impossible de répondre aux exigences réglementaires, de réduire les risques liés à la prestation des services ou encore, d'améliorer l'expérience des clients.

Les exemples de mise en œuvre cités rendent compte de la diversité des systèmes et des technologies employés, qui présentent tous des contraintes et des environnements différents. Ces exemples, en fonction des capacités de la clientèle, des technologies disponibles et des normes sociétales, s'appuient soit sur des autorités et des systèmes centralisés, soit sur des systèmes distribués et décentralisés. Aucune solution ne correspond aux besoins de l'ensemble de ces environnements. Les responsables de la mise en œuvre des DFS peuvent néanmoins, à condition de respecter les normes internationales ouvertes sur les technologies en la matière, bénéficier de l'expérience des communautés internationales de normalisation.

Le Groupe d'action financière recommande pour cela aux entités réglementées d'adopter une approche fondée sur le risque. Celle-ci implique d'évaluer les niveaux de garantie des systèmes d'identification numérique en matière de contrôle et d'authentification de l'identité, et de veiller à ce que ces niveaux répondent au devoir de précaution du consommateur. L'authentification forte du consommateur, basée sur au moins deux facteurs d'authentification, permet de maintenir un haut niveau de garantie conformément à la recommandation du Groupe d'action financière.

De nouvelles technologies et approches font leur apparition sur le marché. Il est essentiel de les normaliser, à la fois pour tenir compte des menaces et des risques, mais aussi pour veiller à ce que les nouvelles technologies soient compatibles avec les architectures existantes et s'y intègrent.

Annexe A – Bibliographie

- [1] UIT-T, "ITU-T FG-DFS Main Recommendations". Mars 2017 (en ligne). Disponible à l'adresse suivante: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Main-Recommendations.pdf.
- [2] UIT-T, "The Digital Financial Services Ecosystem". Mai 2016 (en ligne). Disponible à l'adresse suivante: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/FINAL%20ENDORSED%20ITU%20DFS%20Introduction%20Ecosystem%2028%20April%202016_formatted%20AM.pdf.
- [3] Groupe d'action financière, "Digital ID guidance". 20 novembre 2019 (en ligne). Disponible à l'adresse suivante: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html>.
- [4] UIT-T, "Reccomendation X.1254 Entity Authentication Framework". 7 septembre 2012 (en ligne). Disponible à l'adresse suivante: <http://handle.itu.int/11.1002/1000/11608>.
- [5] "ISO/IEC 29115:2013: Information technology — Security techniques — Entity authentication assurance framework". (En ligne). Disponible à l'adresse suivante: <https://www.iso.org/standard/45138.html>.
- [6] National Institute of Standards and Technology, "Special Publication 800-63B". National Institute of Standards and Technology, Washington (D.C.), 2017.
- [7] Alliance ID2020, "ID2020 Alliance - Committed to improving lives through digital identity". 2017 (en ligne). Disponible à l'adresse suivante: https://id2020.org/s/ID2020AllianceDoc_UPDATED.pdf. (Consulté le 27 novembre 2018).
- [8] Alliance ID2020, "ID2020 Certification Mark Application form". 2019 (en ligne). Disponible à l'adresse suivante: <https://id2020.org/technical-certification-mark>. (Consulté le 27 mai 2019).
- [9] D. Balfanz, A. Czeskis, J. Hodges, J. Jones, M. B. Jones, A. Kumar, A. Liao, R. Lindemann, E. Lundberg, V. Bharadwaj, A. Birgisson et H. Le Van Gong, "Web Authentication: An API for accessing Public Key Credentials Level 1". 20 septembre 2018 (en ligne). Disponible à l'adresse suivante: <https://w3c.github.io/webauthn/>. (consulté le 21 septembre 2018).
- [10] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant et M. Sabadello, "Decentralized Identifiers (DIDs) v0.11". 23 août 2018 (en ligne). Disponible à l'adresse suivante: <https://w3c-ccg.github.io/did-spec/>. (Consulté le 20 septembre 2018).
- [11] C. Allen, "The Path to Self-Sovereign Identity". 25 avril 2016 (en ligne). Disponible à l'adresse suivante: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>. (Consulté le 27 mars 2019).
- [12] M. Sporny et D. Longley, "Verifiable Credentials Data Model 1.0". 18 septembre 2018 (en ligne). Disponible à l'adresse suivante: <https://www.w3.org/TR/verifiable-claims-data-model/>. (Consulté le 18 septembre 2018).
- [13] Fondation Sovrin, "Sovrin Glossary v2". 27 mars 2019 (en ligne). Disponible à l'adresse suivante:

https://docs.google.com/document/d/1gfIz5TT0cNp2kxGMLFXr19x1uoZsruUe_0glHst2fZ8/edit?usp=sharing. (Consulté le 27 mai 2019).

- [14] M. Sabadello, K. Den Hartog, C. Lundkvist, C. Franz, A. Elias, A. Hughes, J. Jordan et D. Zagidulin, "Introduction to DID Auth". 26 juillet 2018 (en ligne). Disponible à l'adresse suivante: <https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/did-auth.pdf>. (Consulté le 15 mars 2019).
- [15] M. Sabadello, "A Universal Resolver for self-sovereign identifiers". 1^{er} novembre 2017 (en ligne). Disponible à l'adresse suivante: <https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c>. (Consulté le 15 mars 2019).
- [16] D. Reed, J. Law, D. Hardman et M. Lodder, "DKMS (Decentralized Key Management System) Design and Architecture". 2 avril 2018 (en ligne). Disponible à l'adresse suivante: <https://github.com/hyperledger/indy-sdk/blob/677a0439487a1b7ce64c2e62671ed3e0079cc11f/doc/design/005-dkms/DKMS%20Design%20and%20Architecture%20V3.md>. (Consulté le 15 mars 2019).
- [17] A. Offerman, "Swiss City of Zug issues Ethereum blockchain-based eIDs". Février 2018 (en ligne). Disponible à l'adresse suivante: <https://joinup.ec.europa.eu/node/700433>. (Consulté en septembre 2018).
- [18] Open Banking Limited, "Customer Experience Guidelines". Septembre 2018 (en ligne). Disponible à l'adresse suivante: <https://www.openbanking.org.uk/providers/standards/>. (Consulté en septembre 2018).
- [19] UIT-T, "ITU-T FG-DFS Executive summary". Mars 2017 (en ligne). Disponible à l'adresse suivante: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Executive-summary.pdf.
- [20] Alliance FIDO, "Frequently Asked Questions". (En ligne). Disponible à l'adresse suivante: <https://fidoalliance.org/faqs>. (Consulté le 15 juillet 2018)
- [21] Alliance FIDO, "Client To Authenticator Protocol v2.0". 27 septembre 2017 (en ligne). Disponible à l'adresse suivante: <https://fidoalliance.org/specs/fido-v2.0-ps-20170927/fido-client-to-authenticator-protocol-v2.0-ps-20170927.html>. (Consulté le 15 juillet 2018).
- [22] Alliance FIDO, "Universal Authentication Framework". 2 février 2017 (en ligne). Disponible à l'adresse suivante: <https://fidoalliance.org/specs/fido-uaf-v1.1-ps-20170202/fido-uaf-protocol-v1.1-ps-20170202.html>. (Consulté le 15 juillet 2018).
- [23] Alliance FIDO, "Universal Second Factor Overview". 11 avril 2017 (en ligne). Disponible à l'adresse suivante: <https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.html>. (Consulté le 15 juillet 2018).
- [24] S. N. Yanushkevich, "ENCM 509 Fundamental of Biometric System Design Chapter 1". (En ligne). Disponible à l'adresse suivante: <http://www.ucalgary.ca/btlab/files/btlab/ch1.pdf>. (Consulté le 15 juillet 2018).
- [25] Alliance FIDO, "Setting the Standard for Healthcare Security: Aetna Rolls out FIDO and Behavioral Authentication". 19 juillet 2017 (en ligne). Disponible à l'adresse suivante: <https://fidoalliance.org/aetna-deploys-fido-authentication>. (Consulté le 11 avril 2018).
- [26] Fondation OpenID, "OpenID Foundation Specifications". (En ligne). Disponible à l'adresse suivante: <http://openid.net/developers/specs/>. (Consulté le 7 août 2018).

- [27] Fondation OpenID, "OpenID Connect FAQ and Q&As". (En ligne). Disponible à l'adresse suivante: <http://openid.net/connect/faq/>. (Consulté le 7 août 2018).
- [28] Alliance FIDO, "FIDO Deployment Case Study K-FIDO". Septembre 2017 (en ligne). Disponible à l'adresse suivante: https://fidoalliance.org/wp-content/uploads/FIDO-Deployment-Case-Study-K-FIDO_170905.pdf. (Consulté en septembre 2018).
- [29] "Press Release". 14 septembre 2018 (en ligne). Disponible à l'adresse suivante: https://www.prnewswire.com/news-releases/id2020-alliance-launches-inaugural-pilots-welcomes-new-partners-at-annual-summit-300713089.html?tc=eml_cleartime. (Consulté le 27 novembre 2018).
- [30] "Press Release". 14 septembre 2018 (en ligne). Disponible à l'adresse suivante: <http://www.globenewswire.com/news-release/2018/09/14/1571269/0/en/Everest-ID2020-and-the-Government-of-Indonesia-TNP2K-Secretariat-Announce-Innovative-Identity-and-Blockchain-Pilot-Solution-to-Enhance-the-National-LPG-Subsidy-Program.html>. (Consulté le 27 novembre 2018).
- [31] Global System Mobile Association, "Mobile Connect - Operator cooperation in South Korea has created a successful identity solution". 2017 (en ligne). Disponible à l'adresse suivante: https://www.gsma.com/identity/wp-content/uploads/.../mc_skt_case_08_17_v.1b.pdf. (Consulté le 13 septembre 2018).
- [32] Alliance FIDO, "FIDO & PSD2: Meeting the needs for Strong Customer Authentication". 2017 (en ligne). Disponible à l'adresse suivante: <https://fidoalliance.org/wp-content/uploads/FIDO-PSD2-white-paper-FINAL.pdf>. (Consulté le 20 septembre 2018).
- [33] Autorité bancaire européenne, "Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)". 2017 (en ligne). Disponible à l'adresse suivante: <https://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf>. (Consulté le 12 septembre 2018).
- [34] Kiva, "Kiva, Sierra Leone and U.N. agencies partner to implement 'credit bureau of the future'". 2018 (en ligne). Disponible à l'adresse suivante: <https://www.kiva.org/blog/kiva-sierra-leone-and-un-agencies-partner-to-implement-credit-bureau-of-the-future>. (Consulté le 27 mai 2019).
- [35] Kiva, "Kiva Protocol FAQ". 2019 (en ligne). Disponible à l'adresse suivante: <https://pages.kiva.org/kiva-protocol-faq>. (Consulté le 27 mai 2019).

Annexe B – Conseils aux fournisseurs de DFS

Les fournisseurs de DFS sont à l'écoute des usagers, dont ils gèrent la plupart des aspects de l'expérience utilisateur. Y accorder une attention particulière, ainsi qu'à leurs parcours, peut accroître la confiance qu'ils accordent au système et augmenter la sécurité opérationnelle. Le secteur des banques ouvertes a publié des lignes directrices sur l'expérience client [18] qui décrivent les "principes d'expérience" élaborés en vue d'aider les concepteurs dans leur travail.

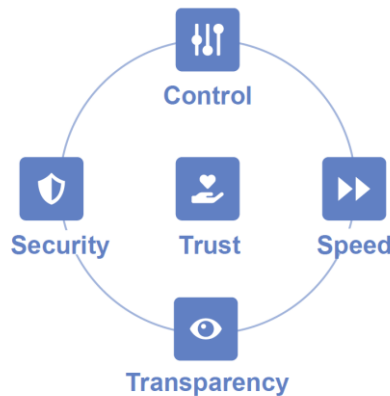


Figure 40 – Principes d'expérience relatifs à l'engagement des utilisateurs dans les services bancaires ouverts

- Contrôle: Les usagers, afin de se sentir en confiance, doivent disposer des outils appropriés ainsi que d'informations précises au bon moment.
- Rapidité: La rapidité doit être adaptée à chaque client et à chaque interaction. La rapidité n'est pas toujours le critère le plus déterminant.
- Transparence: Les choix et les actions doivent être réalisés en toute transparence, et les informations relatives à leurs conséquences doivent être communiquées.
- Sécurité: La fraude et la confidentialité des données sont au cœur des préoccupations des utilisateurs des DFS. Les messages et les informations communiquées sur les mesures de sécurité doivent être clairs et concis.
- Confiance: Le sentiment de confiance du client dépend du respect des principes de contrôle, de rapidité, de transparence et de sécurité.

Annexe C – Conseils aux fournisseurs de systèmes d'authentification

Les organismes de normalisation des systèmes d'authentification publient des documents d'orientation à l'attention de leurs fournisseurs afin d'en faciliter la mise en œuvre. Les documents d'orientation relatifs aux normes citées dans ce rapport sont les suivants:

Groupe du NIST sur les identités de confiance:

<https://www.nist.gov/itl/tig/projects/special-publication-800-63>

Orientations en matière de mise en œuvre

- "Le NIST travaillera avec la communauté dans le but de préparer des documents d'orientation en accord avec les lignes directrices sur l'identité numérique. Ceux-ci devront livrer aux responsables de la mise en œuvre des recommandations facilement applicables afin de les aider à satisfaire aux exigences en la matière."

Alliance FIDO:

<https://fidoalliance.org/white-papers/>

- *FIDO Alliance White Paper: Enterprise Adoption Best Practices - Managing FIDO Credential Lifecycle for Enterprises (avril 2018):*
"Ce livre blanc fournit des conseils aux professionnels de l'informatique et de la sécurité sur la gestion des identifiants d'authentification FIDO tout au long de leur cycle de vie."
- *FIDO Alliance White Paper: How FIDO Standards Meet PSD2's Regulatory Technical Standards Requirements on Strong Customer Authentication (décembre 2018):*
"Ce document livre un examen détaillé des exigences de sécurité énumérées dans les normes techniques de réglementation relatives à l'authentification forte du client et à des normes ouvertes communes et sécurisées de communication dans le cadre de la DSP2 (les RTS) et décrit la façon dont les normes FIDO satisfont à ces exigences."
- *FIDO Alliance White Paper: FIDO & PSD2 – Providing for a Satisfactory Customer Journey (septembre 2018):*
"Ce livre blanc passe en revue les différents modèles d'authentification qui pourraient s'appliquer dans le cadre des interactions entre un fournisseur tiers et un fournisseur de services de paiement pour les comptes. Pour chacun de ces modèles, il propose d'adopter les normes FIDO dans afin de simplifier l'expérience utilisateur d'une manière qui puisse satisfaire aux exigences de la DSP2 en matière d'authentification forte des clients."
- *FIDO Alliance White Paper: Enterprise Adoption Best Practices - Integrating FIDO & Federation Protocols (décembre 2017):*
"Ce livre blanc décrit la façon dont les normes FIDO complètent les protocoles de fédération. Il indique également la procédure qu'il convient de suivre pour les intégrer et ainsi prendre en charge l'authentification à plusieurs facteurs fondée sur les normes FIDO et remplacer ou compléter les méthodes d'authentification traditionnelles dans les environnements de fédération."

Système bancaire ouvert:

<https://www.openbanking.org.uk/providers/standards/>

Customer Experience Guidelines

- "Ce document fournit des lignes directrices sur l'expérience client ainsi que des exemples de parcours de clients aux fournisseurs tiers et aux fournisseurs de comptes sur la base d'exigences réglementaires et de travaux de recherches approfondies sur les clients. Il vise à encourager l'adoption de produits et de services compatibles avec les systèmes bancaires ouverts."

Mobile Connect de la GSMA:

https://www.gsma.com/identity/wp-content/uploads/2019/03/mc_mwc_platforms_booklet2_web_02_19-1.pdf

GSMA Platforms & Operations services, février 2019

- "La GSMA met à disposition des opérateurs de réseaux mobiles et des fournisseurs de services un ensemble de plateformes et de services techniques déployables sur Mobile Connect.
- Portail Interoperability Testsuite: vérifiez si votre produit Mobile Connect est conforme à la spécification Mobile Connect.
- API Exchange: rejoignez d'autres opérateurs de réseaux mobiles au sein d'un écosystème Mobile Connect afin d'offrir un accès transparent et interopérateurs aux fournisseurs de services.
- Developer Portal (avec Sandbox et SDK): une documentation et des outils complets qui facilitent l'intégration de Mobile Connect dans vos applications.
- Operator Management Console: un portail auquel les opérateurs peuvent accéder en libre-service afin de consulter les rapports existants et de gérer leurs opérations de gestion avec la GSMA.
- Service Desk: un point de contact unique pour toutes les demandes concernant Mobile Connect.
- Monitoring & Incident Management: vérifiez l'état de vos composants Mobile Connect ainsi que le statut de tout incident les affectant."

https://www.gsma.com/identity/wp-content/uploads/2018/02/Mobile-strong-customer-authentication-under-PSD2_March2018-FINAL.pdf

Mobile strong customer authentication under PSD2: comparisons and considerations

- "Ce document examine les principales solutions d'authentification forte mobile généralement disponibles au sein de l'Union européenne au moment de sa rédaction. Bien que de nombreuses solutions propriétaires et nationales répondent efficacement aux exigences de la DSP2, nous avons porté notre attention sur celles qui sont généralement disponibles dans l'Union européenne. Les profils présentés dans ce document rendent uniquement compte des considérations de haut niveau que les fournisseurs de services de paiement devront garder à l'esprit lors de la mise en œuvre de la SCA mobile. L'objectif des fournisseurs de services de paiement pour les comptes est d'éviter les points uniques de défaillance et de proposer diverses solutions d'authentification à leurs utilisateurs de services de paiement; les solutions retenues par ce document peuvent donc être combinées et mises en œuvre de manière complémentaire."

<https://developer.mobileconnect.io/step-by-step-guide>

- "La mise en œuvre de Mobile Connect implique d'interagir avec un certain nombre de services et de technologies. Cette section présente de façon détaillée chacune des étapes à suivre."