ITUPublications
Recommandations

Union internationale des télécommunications
Secteur de la normalisation

Recommandation

# UIT-T X.1280 (03/2024)

SÉRIE X: Réseaux de données, communication entre systèmes ouverts et sécurité

Sécurité du cyberespace – Gestion des identités (IDM) et authentification

# Cadre pour l'authentification de serveurs hors bande à l'aide de dispositifs mobiles

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**Réseaux de données, communication entre systèmes ouverts et sécurité**

| | |
|---|---|
| RÉSEAUX PUBLICS DE DONNÉES | X.1-X.199 |
| INTERCONNEXION DES SYSTÈMES OUVERTS | X.200-X.299 |
| INTERFONCTIONNEMENT DES RÉSEAUX | X.300-X.399 |
| SYSTÈMES DE MESSAGERIE | X.400-X.499 |
| ANNUAIRE | X.500-X.599 |
| RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES | X.600-X.699 |
| GESTION OSI | X.700-X.799 |
| SÉCURITÉ | X.800-X.849 |
| APPLICATIONS OSI | X.850-X.899 |
| TRAITEMENT RÉPARTI OUVERT | X.900-X.999 |
| SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX | X.1000-X.1099 |
| APPLICATIONS ET SERVICES SÉCURISÉS (I) | X.1100-X.1199 |
| SÉCURITÉ DU CYBERESPACE | X.1200-X.1299 |
| Cybersécurité | X.1200-X.1229 |
| Lutte contre le pollupostage | X.1230-X.1249 |
| **Identity management (IdM) and Authentication** | **X.1250-X.1299** |
| APPLICATIONS ET SERVICES SÉCURISÉS (II) | X.1300-X.1499 |
| ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | X.1500-X.1599 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | X.1600-X.1699 |
| COMMUNICATIONS QUANTIQUES | X.1700-X.1729 |
| SÉCURITÉ DES DONNÉES | X.1750-X.1799 |
| INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY | X.1800-X.1839 |
| METAVERSE AND DIGITAL TWIN SECURITY | X.2000-X.2199 |
| SOFTWARE SUPPLY CHAIN SECURITY | X.2150-X.2199 |
| ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY | X.2200-X.2249 |

*Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.*

# Recommandation UIT-T X.1280

## Cadre pour l'authentification de serveurs hors bande à l'aide de dispositifs mobiles


### Résumé

Dans les normes technologiques d'authentification, la résistance à l'usurpation d'identité du vérificateur est considérée comme une exigence du plus haut niveau d'assurance d'authentification. Cependant, les technologies d'authentification existantes se concentrent sur l'authentification de l'utilisateur et il n'est pas possible de vérifier explicitement les fournisseurs de services.

La Recommandation UIT-T X.1280 fournit un cadre pour l'authentification de serveur hors bande à l'aide de dispositifs mobiles, qui résout la vulnérabilité liée à l'usurpation d'identité du vérificateur et la limitation de la dépendance à l'égard du terminal de l'utilisateur des authentificateurs existants. Il permet à un utilisateur de fournir des informations d'authentification après avoir vérifié le fournisseur de services de manière explicite et indépendante dans le processus d'authentification de l'utilisateur sur tous les terminaux de l'utilisateur.



### Historique*

| Édition | Recommandation | Approbation | Commission d'études | ID unique |
|---|---|---|---|---|
| 1.0 | UIT-T X.1280 | 01-03-2024 | 17 | 11.1002/1000/15661 |

### Mots clés

Authentification, authentificateur, partie se fiant à l'information, vérification, vérificateur, résistance à l'usurpation d'identité du vérificateur.


* Pour accéder à la Recommandation, reporter cet URL https://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique.

## 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.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

À la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

## TABLE DES MATIÈRES

# Recommandation UIT-T X.1280

## Cadre pour l'authentification de serveurs hors bande à l'aide de dispositifs mobiles

### 1 Domaine d'application

La présente Recommandation fournit un cadre pour l'authentification hors bande des serveurs à l'aide de dispositifs mobiles, y compris par ce qui suit:

- définit le modèle d'authentification du serveur hors bande et la procédure d'authentification;
- définit des critères et des lignes directrices pour la génération d'informations d'authentification du serveur à l'aide de dispositifs mobiles;
- définit les menaces et les exigences en matière de sécurité dans le modèle d'authentification du serveur hors bande;
- décrit les cas d'utilisation du modèle d'authentification du serveur hors bande; et
- décrit la relation avec d'autres technologies d'authentification.

La présente Recommandation n'aborde pas les questions liées à l'authentification de l'utilisateur, à la réglementation et à la protection de la vie privée.

### 2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations ou autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références indiquées ci-après. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

Aucune.

### 3 Définitions

#### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants, définis ailleurs:

**3.1.1 authentification** [b-ISO/IEC 18014-2]: fourniture d'une assurance sur l'identité déclarée d'une entité.

**3.1.2 fournisseur de services d'identification (CSP)** [b-UIT-T X.1254]: acteur de confiance qui délivre ou gère des informations d'identification.

**3.1.3 partie dépendante (RP)** [b-UIT-T X.1254]: acteur qui s'appuie sur une affirmation ou une revendication d'identité.

**3.1.4 vérification** [b-ISO/IEC 29115]: processus de vérification des informations en comparant les informations fournies avec des informations précédemment corroborées.

**3.1.5 vérificateur** [b-ISO/IEC 29115]: acteur qui corrobore les informations relatives à l'identité.

#### 3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

**3.2.1 authentification du serveur**: processus de vérification de l'authenticité du fournisseur de services par comparaison des informations d'authentification du serveur générées par le vérificateur et l'authentificateur de serveur hors bande d'un utilisateur.

**3.2.2 informations d'authentification du serveur**: code d'authentification généré à l'aide d'un algorithme de mot de passe à usage unique (OTP) dans le vérificateur et le serveur d'authentification hors bande de l'utilisateur.

**3.2.3 authentification de l'utilisateur hors bande**: processus de vérification de l'authenticité d'un utilisateur à l'aide d'un autre canal de communication distinct de celui utilisé pour se connecter ou effectuer une transaction.

**3.2.4 authentification du serveur hors bande**: processus de vérification de l'authenticité d'un serveur à l'aide d'un autre canal de communication distinct de celui utilisé pour se connecter ou effectuer une transaction.

## 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ATM distributeur automatique de billets (*automated teller machine*)

CSP fournisseur de services d'accréditation (*credential service provider*)

CTAP protocole client-authentificateur (*client to authenticator protocol*)

DNS système de nom de domaine (*domain name system*)

FIDO identité rapide en ligne (*fast identity online*)

IA intelligence artificielle

ICP infrastructure à clé publique

ID identification

IdP fournisseur d'identité (*identity provider*)

IP protocole internet (*internet protocol*)

OAuth authentification d'ouverture (*open authentication*)

OTP mot de passe à usage unique (*one-time password*)

PAM modules d'authentification enfichables (*pluggable authentication modules*)

PIN numéro d'identification personnel (*personal identification number*)

QR réponse rapide (*quick response*)

RP partie utilisatrice

SAML langage de balisage d'assertion de sécurité (*security assertion markup language*)

SMS service de messages courts (*short message service*)

SSL couche de sockets sécurisés (*secure socket layer*)

U2F universel à deux facteurs (*universal two factor*)

## 5 Conventions

La présente Recommandation applique les formes verbales suivantes pour l'expression des dispositions:

a) le terme "**doit**" indique une exigence;

b) le terme "**devrait**" indique une recommandation;

c) la mention "**peut**" indique une autorisation;

d) le mot "**peut**" indique une possibilité ou une capacité.

## 6 Introduction

Dans l'authentification traditionnelle, seul le serveur authentifie l'utilisateur et ce dernier est vulnérable aux cyberattaques telles que le phishing et le détournement de domaine.

L'authentification du serveur basée sur l'infrastructure à clé publique (ICP) est adéquate pour l'utilisateur lorsqu'il utilise des applications basées sur un navigateur avec une barre d'adresse. L'authentification basée sur l'ICP est également réalisée indépendamment du processus d'authentification de l'utilisateur, ce qui permet à l'utilisateur d'être facilement ignoré.

La présente recommandation fournit un cadre pour l'authentification hors bande du serveur à l'aide de dispositifs mobiles, conçu pour authentifier le serveur par l'utilisateur en premier lieu et aider l'utilisateur à s'engager explicitement dans l'authentification du serveur dans le cadre du processus d'authentification de l'utilisateur. Dans le cadre de l'authentification de l'utilisateur, tous les processus y afférents peuvent être appliqués ensemble.

L'authentification du serveur hors bande peut être utilisée par des applications basées sur un navigateur et par de nombreux types d'applications et de systèmes d'exploitation.

L'authentification hors bande du serveur est réalisée en vérifiant les informations d'authentification du serveur par l'utilisateur, puis en vérifiant les informations d'authentification de l'utilisateur par le serveur, ce qui permet au vérificateur de résister à l'usurpation d'identité.

Grâce à l'authentification hors bande du serveur, les fournisseurs de services et les utilisateurs bénéficient des avantages suivants:

1) Authentification centrée sur l'utilisateur: au lieu de demander à l'utilisateur de se souvenir et de saisir ses informations d'authentification complexes, le serveur présente ses informations d'authentification de sorte que l'utilisateur authentifie le serveur. Les utilisateurs sont libérés du fardeau de la gestion des justificatifs d'identité en changeant le rôle de l'utilisateur, qui passe de la saisie des informations d'authentification de l'utilisateur à la vérification des informations d'authentification du serveur. La Figure 1 illustre l'authentification centrée sur l'utilisateur.

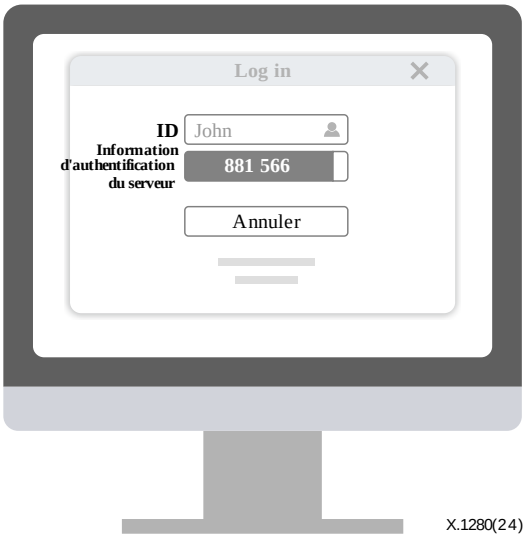


**Figure 1 – Authentification centrée sur l'utilisateur**

2) Authentification mutuelle: l'utilisateur vérifie l'authenticité du serveur à l'aide des informations d'authentification du serveur générées par le serveur et l'authentificateur de serveur hors bande, respectivement. Le serveur vérifie l'authenticité de l'utilisateur à l'aide des informations d'authentification de l'utilisateur envoyées après que l'utilisateur a confirmé deux correspondances d'informations d'authentification du serveur. La Figure 2 illustre l'authentification mutuelle.

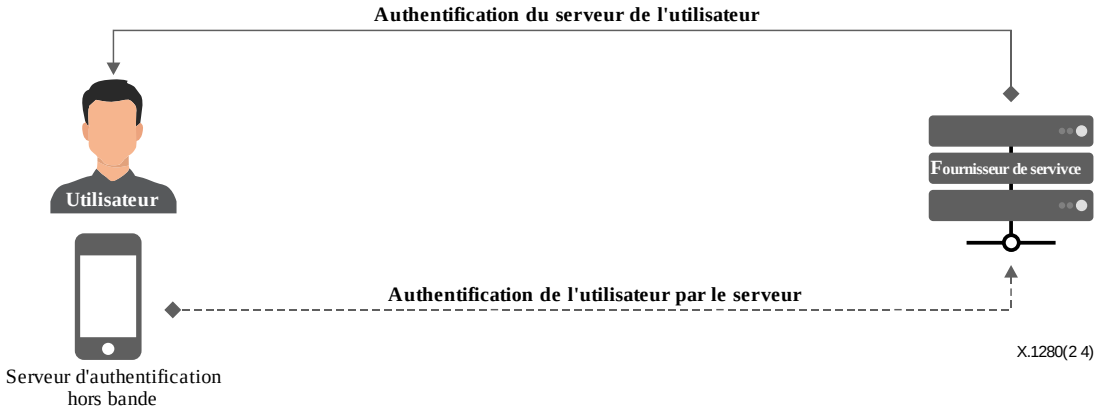


**Figure 2 – Authentification mutuelle**

3) Authentification unifiée: même si des terminaux supplémentaires sont ajoutés, tels que des ordinateurs, des smartphones, des distributeurs automatiques de billets (ATM) et des haut-parleurs à Intelligence artificielle (IA), les méthodes d'authentification peuvent être unifiées puisque les serveurs présentent leurs informations d'authentification à l'utilisateur au lieu de lui demander d'entrer diverses informations d'authentification. La Figure 3 illustre l'authentification unifiée.

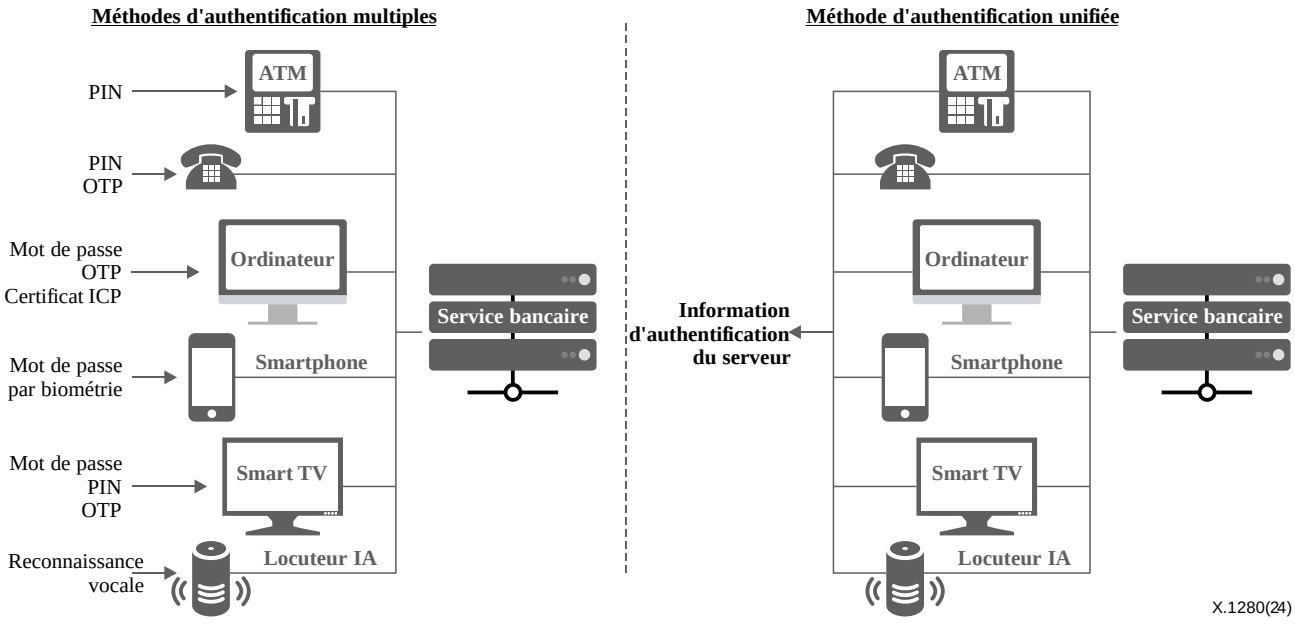


**Figure 3 – Authentification unifiée (par exemple, service bancaire)**

## 7 Cadre pour l'authentification des serveurs hors bande

Les rôles et les composants du modèle d'authentification pour le cadre d'authentification serveur hors bande, qui permet l'authentification mutuelle entre l'utilisateur et le serveur, sont définis dans la présente section. Le flux principal consiste à vérifier les informations d'authentification du serveur

par l'utilisateur d'abord, puis à vérifier les informations d'authentification de l'utilisateur par le serveur.

## 7.1 Rôles et composantes

Le Tableau 1 présente la liste des rôles et des composants du cadre d'authentification du serveur hors bande.

**Tableau 1 – Rôles et composants du modèle d'authentification du serveur hors bande**

| Nom | Description |
|---|---|
| Vérificateur | Un vérificateur génère des informations d'authentification du serveur en réponse à la demande de l'utilisateur. Les informations sont envoyées à la partie utilisatrice à l'information pour être présentées à l'utilisateur. Il envoie le décalage pour générer les informations d'authentification du serveur à l'authentificateur de serveur hors bande pour générer les informations d'authentification du serveur à présenter à l'utilisateur. |
| Partie utilisatrice | Une partie utilisatrice à l'information présente à l'utilisateur les informations d'authentification du serveur générées et envoyées par le vérificateur. |
| Utilisateur | Un utilisateur reçoit des services de la part de parties utilisatrices et de vérificateurs. |
| Terminal utilisateur | Un terminal utilisateur affiche les informations d'authentification du serveur par le biais d'applications. Les terminaux utilisateurs sont par exemple des ordinateurs, des smartphones, des guichets automatiques et des haut-parleurs d'intelligence artificielle. |
| Authentificateur de serveur hors bande | Un authentificateur de serveur hors bande génère des informations d'authentification de serveur en utilisant le décalage envoyé par le vérificateur. |

## 7.2 Informations sur l'authentification du serveur

Les informations d'authentification du serveur sont un code à plusieurs chiffres utilisé lorsque l'utilisateur authentifie le serveur. Il est généré à l'aide d'un mot de passe à usage unique (OTP) de défi et de réponse, à la demande de l'utilisateur. Des valeurs de défi dynamiques et une clé de vérification sont utilisées pour calculer et générer des informations d'authentification du serveur. Les valeurs de défi dynamique et la clé de vérification sont définies dans la section 8.

Si les informations d'authentification du serveur générées par le serveur correspondent aux informations d'authentification du serveur générées par l'authentificateur de serveur hors bande de l'utilisateur, l'authenticité du serveur est vérifiée.

## 7.3 Modèle d'authentification

Le flux principal de l'authentification du serveur hors bande est que l'utilisateur s'authentifie d'abord auprès du serveur en comparant les informations d'authentification du serveur générées par le vérificateur et l'authentificateur du serveur hors bande. Une fois que l'utilisateur a authentifié le serveur, l'authentificateur génère des informations d'authentification de l'utilisateur et les envoie au vérificateur. Le vérificateur authentifie l'utilisateur à l'aide des informations d'authentification de l'utilisateur.

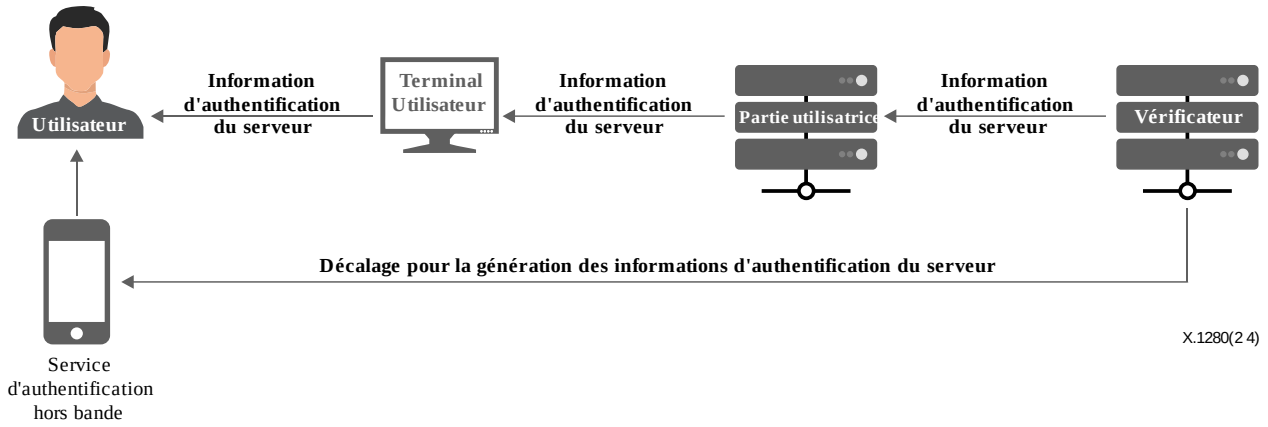


**Figure 4 – Vue d'ensemble de l'authentification du serveur hors bande à l'aide d'appareils mobiles**

Pour lancer l'authentification du serveur hors bande à l'aide d'appareils mobiles, l'utilisateur doit taper son identifiant sur le terminal de l'utilisateur doté d'un écran. Une fois que l'utilisateur a saisi l'identifiant sur le terminal de l'utilisateur, la partie utilisatrice présente à l'utilisateur, d'abord sur le terminal de l'utilisateur, les informations d'authentification du serveur générées par le vérificateur. L'utilisateur les compare ensuite aux informations d'authentification du serveur générées par l'authentificateur de serveur hors bande de l'utilisateur.

## 8 Procédures d'authentification du serveur hors bande

### 8.1 Installation et enregistrement d'un authentificateur de serveur hors bande

À l'étape d'installation et d'enregistrement de l'authentificateur du serveur hors bande, l'utilisateur installe l'application d'authentification sur le téléphone intelligent et l'enregistre dans le vérificateur.

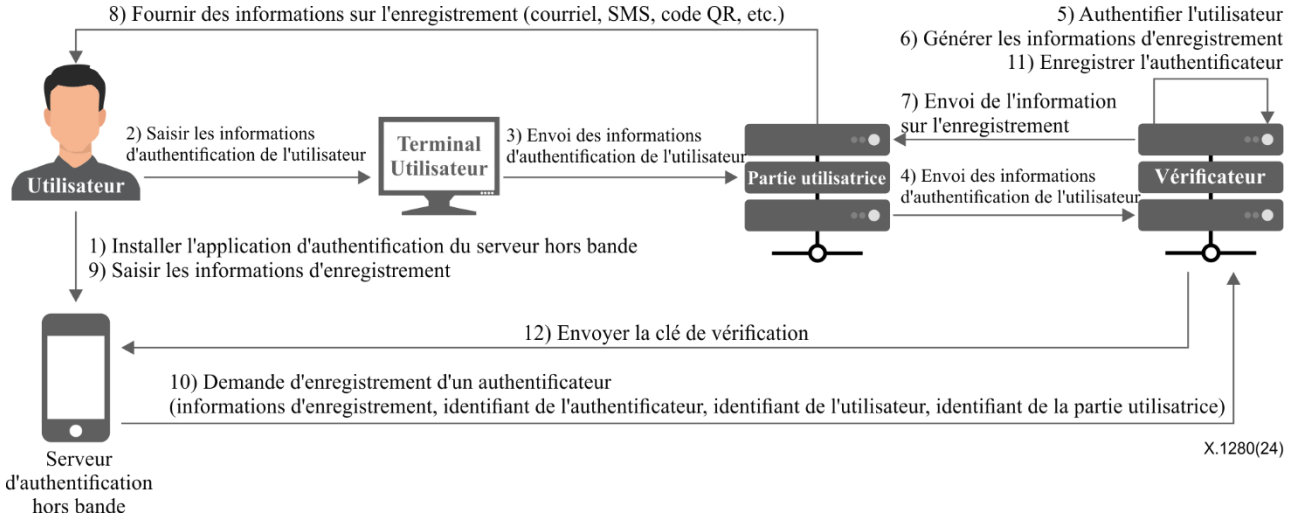


**Figure 5 – Déroulement de l'installation et de l'enregistrement de l'authentificateur du serveur hors bande**

La Figure 5 identifie les données nécessaires à l'étape d'installation et d'enregistrement de l'authentificateur du serveur hors bande et montre le flux. L'explication du flux est la suivante:

1) L'utilisateur installe l'application d'authentification du serveur hors bande sur le smartphone.

2) L'utilisateur saisit les informations d'authentification de l'utilisateur via le terminal de l'utilisateur pour s'authentifier en tant qu'utilisateur légitime par une méthode fiable, telle que

la connexion, la vérification du courrier électronique ou l'identification du téléphone portable, conformément à la politique de la partie utilisatrice.

3) Les informations d'authentification de l'utilisateur saisies dans le terminal de l'utilisateur sont envoyées à la partie utilisatrice.

4) La partie utilisatrice envoie les informations d'authentification de l'utilisateur au vérificateur.

5) Le vérificateur authentifie l'utilisateur.

6) Le vérificateur génère des informations d'enregistrement correspondant à l'utilisateur authentifié.

7) Le vérificateur envoie les informations d'enregistrement générées, y compris l'identifiant de l'utilisateur de la partie utilisatrice et l'identifiant de la partie utilisatrice, à la partie utilisatrice.

8) La partie utilisatrice fournit à l'utilisateur les informations d'enregistrement en utilisant des méthodes fiables, telles que le courrier électronique, le message texte, le code de réponse rapide (QR), etc.

9) L'utilisateur saisit les informations d'enregistrement de l'authentificateur dans l'authentificateur installé dans le smartphone.

10) L'authentificateur envoie les informations d'enregistrement, l'identifiant de l'authentificateur, l'identifiant de l'utilisateur et l'identifiant de la partie utilisatrice au vérificateur.

11) Le vérificateur vérifie les informations d'enregistrement et enregistre l'authentificateur avec l'identificateur d'authentificateur, l'identificateur d'utilisateur et l'identificateur de partie utilisatrice.

12) Après avoir enregistré l'authentificateur, le vérificateur envoie la clé de vérification correspondante à l'authentificateur.

La procédure d'enregistrement hors bande de l'authentificateur du serveur doit être assurée et exécutée en appliquant le protocole SSL (secure socket layer) à l'aide de certificats UIT-T X.509 pour sécuriser la communication entre l'authentificateur et le vérificateur.

Dans le cas où l'authentificateur du serveur hors bande ne peut être utilisé en raison d'une perte ou d'une détérioration, le vérificateur peut permettre à l'utilisateur d'enregistrer plus d'un authentificateur de serveur hors bande en tant qu'authentificateur de secours.

## 8.2 Demande d'authentification du serveur

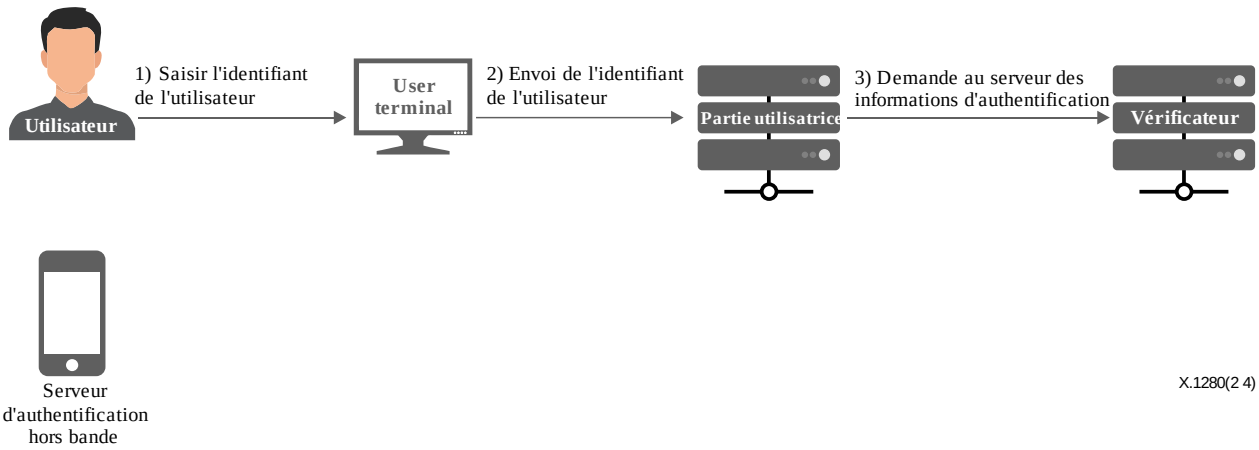


**Figure 6 – Flux de la demande d'authentification du serveur**

La Figure 6 identifie les données nécessaires à l'étape de la demande d'authentification du serveur et montre le flux. L'explication du flux est la suivante:

1) L'utilisateur du terminal se connecte à la partie utilisatrice, puis saisit son identifiant.

2) Le numéro d'identification de l'utilisateur saisi dans le terminal de l'utilisateur est envoyé à la partie utilisatrice.

3) La partie utilisatrice demande au vérificateur des informations sur l'authentification du serveur.

## 8.3 Génération et présentation des informations d'authentification du serveur

Lors de l'étape de génération et de présentation des informations d'authentification du serveur, le vérificateur génère les informations d'authentification du serveur correspondant à l'identifiant de l'utilisateur après avoir reçu la demande d'authentification du serveur de la part de la partie utilisatrice. Le vérificateur envoie ensuite les informations d'authentification du serveur à la partie utilisatrice pour qu'elle soit affichée sur l'écran du terminal de l'utilisateur. Le vérificateur envoie également le décalage à l'authentificateur du serveur hors bande de l'utilisateur. L'authentificateur utilise le décalage reçu pour générer des informations d'authentification du serveur et présente les informations d'authentification du serveur générées.

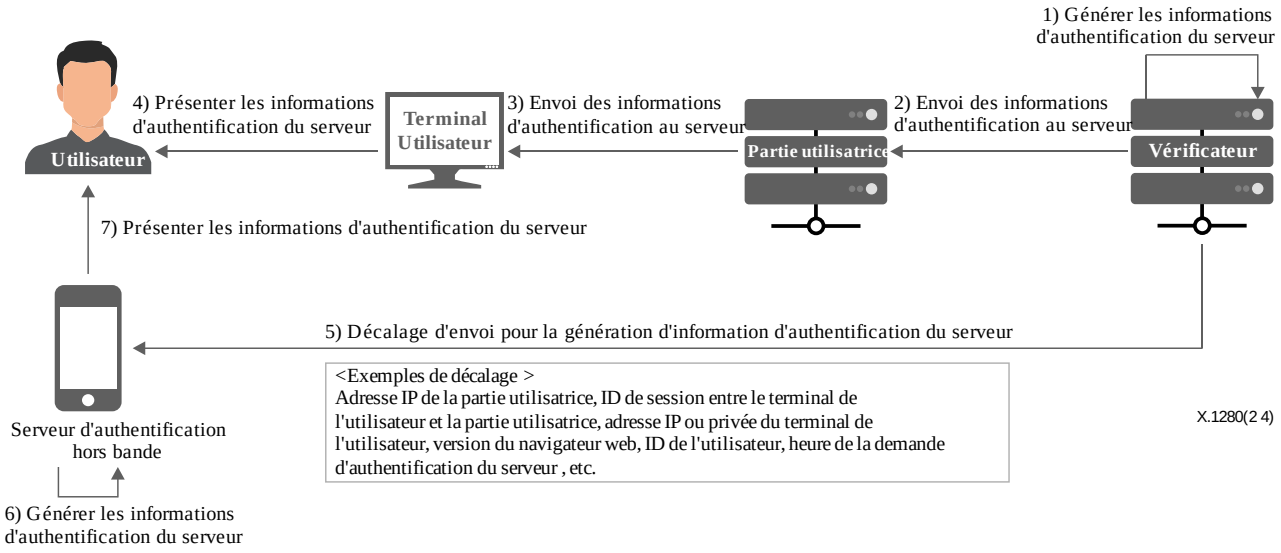


**Figure 7 – Flux de génération et de présentation des informations d'authentification du serveur**

La Figure 7 identifie les données nécessaires à l'étape de génération et de présentation des informations d'authentification du serveur et montre le flux. L'explication du flux est la suivante:

1) Le vérificateur génère des informations d'authentification du serveur une fois que la demande d'authentification du serveur est reçue, y compris l'identifiant de l'utilisateur et le décalage de la partie utilisatrice. Le vérificateur calcule et génère les informations d'authentification du serveur avec la clé de vérification, que le vérificateur et l'authentificateur hors bande de l'utilisateur ont reçue et stockée au cours de l'étape d'installation et d'enregistrement de l'authentificateur hors bande du serveur, et le décalage.

2) Le vérificateur envoie les informations d'authentification du serveur générées à la partie utilisatrice.

3) La partie utilisatrice envoie les informations d'authentification du serveur reçues au terminal de l'utilisateur.

4) La partie utilisatrice présente les informations d'authentification du serveur à l'utilisateur par l'intermédiaire du terminal de l'utilisateur.

5) Le vérificateur envoie également le décalage pour générer les informations d'authentification du serveur à l'authentificateur de serveur hors bande de l'utilisateur.

6) L'authentificateur du serveur hors bande de l'utilisateur calcule et génère des informations d'authentification du serveur avec la clé de vérification, que le vérificateur et l'authentificateur hors bande de l'utilisateur ont reçue et stockée au cours de l'étape d'installation et d'enregistrement de l'authentificateur du serveur hors bande et du décalage.

7) L'authentificateur de serveur hors bande présente également à l'utilisateur les informations d'authentification du serveur qu'il a lui-même générées.

Le décalage doit inclure l'adresse IP du serveur de la partie utilisatrice, l'identifiant de session entre le terminal de l'utilisateur et le serveur de la partie utilisatrice, l'adresse IP publique du terminal de l'utilisateur, l'adresse IP privée du terminal de l'utilisateur, la version du navigateur web du terminal de l'utilisateur, l'identifiant de l'utilisateur et l'heure de la demande d'authentification du serveur de l'utilisateur.

Les informations d'authentification du serveur doivent être calculées et générées à l'aide de la clé de vérification et du décalage, puis converties en une valeur facile à lire pour les utilisateurs. La valeur doit être au moins un nombre à 6 chiffres ou une chaîne de caractères. La valeur doit être affichée dans le terminal de l'utilisateur et dans l'authentificateur du serveur hors bande. En outre, les informations d'authentification du serveur doivent avoir une durée de validité appropriée en fonction du type de services en ligne et doivent indiquer visuellement la durée de validité restante sous différentes formes dans la zone d'affichage des informations d'authentification du serveur, comme illustré à la Figure 8.

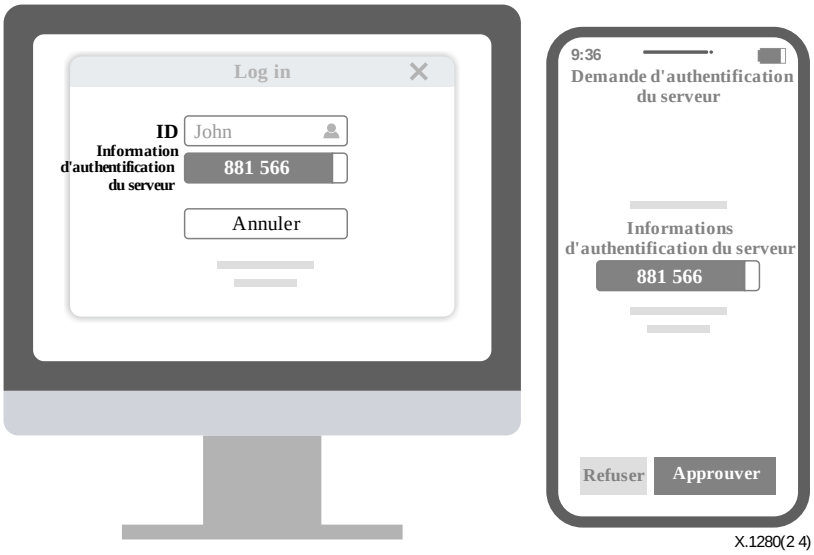


**Figure 8 – Exemple de présentation des informations d'authentification du serveur**

Au lieu de comparer les informations d'authentification de l'utilisateur, la partie utilisatrice peut afficher un code QR, qui comprend les informations d'authentification du serveur pour que l'authentificateur du serveur hors bande lise et vérifie le code. L'authentificateur affiche alors des informations compréhensibles pour l'utilisateur afin qu'il puisse vérifier si le serveur est authentique.

## 8.4 Authentification de l'utilisateur

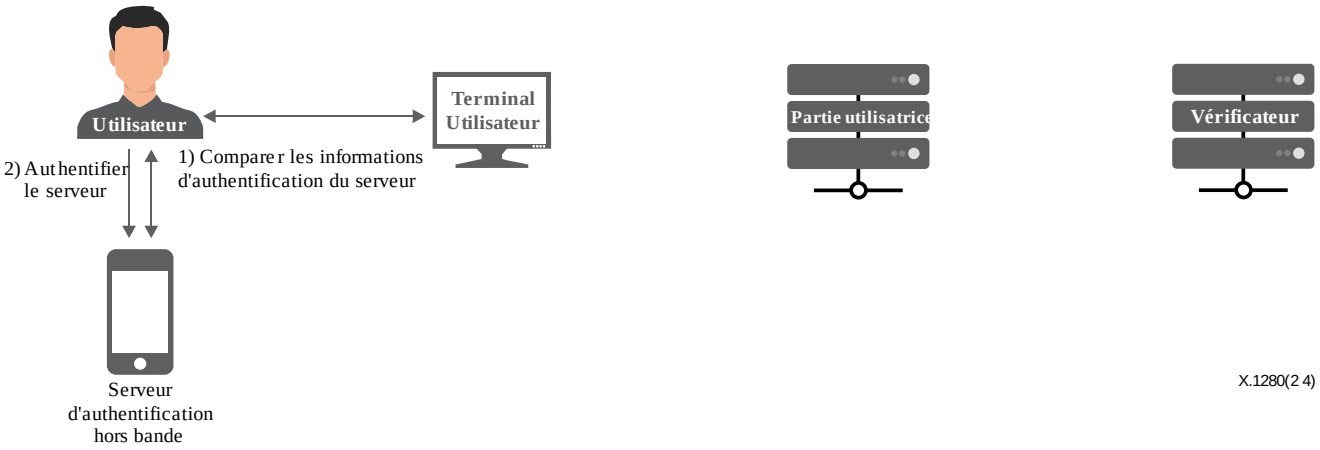


**Figure 9 – Déroulement de l'authentification du serveur**

La Figure 9 identifie les données nécessaires à l'étape d'authentification du serveur et montre le flux. L'explication du flux est la suivante:

1) L'utilisateur compare et vérifie visuellement les informations d'authentification du serveur présentées à la fois dans le terminal et dans l'authentificateur de serveur hors bande.

2) L'utilisateur authentifie le serveur en sélectionnant l'approbation dans l'authentificateur hors bande de l'utilisateur.

## 8.5 Authentification de l'utilisateur et fourniture de services

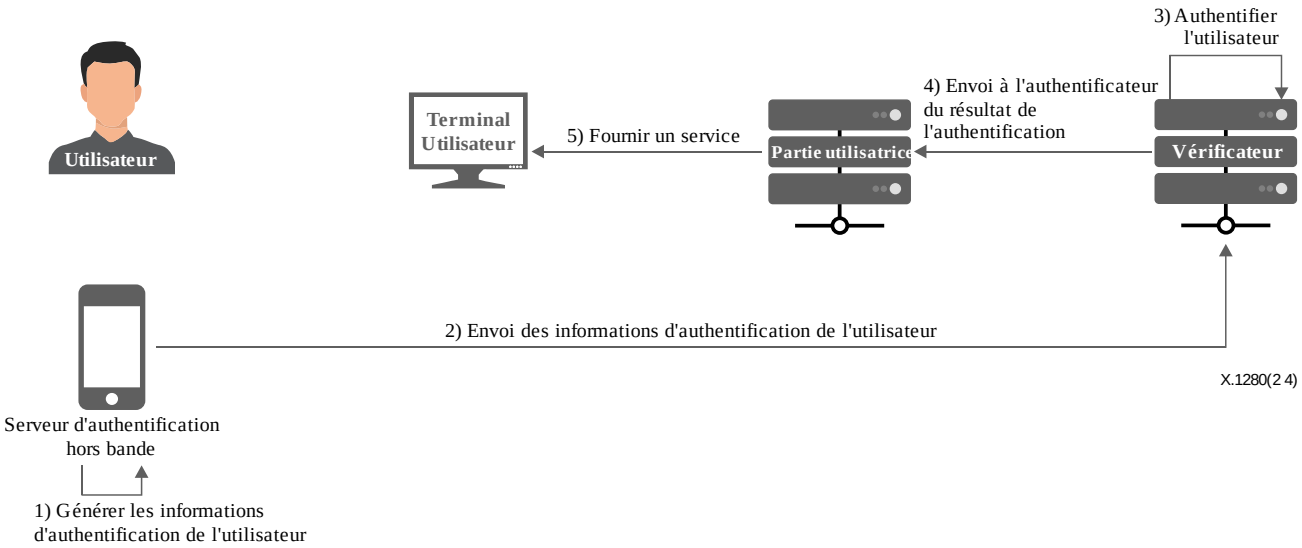


**Figure 10 – Flux de l'authentification de l'utilisateur et de la fourniture de services**

La Figure 10 identifie les données nécessaires à l'étape d'authentification de l'utilisateur et de fourniture de services et montre le flux. L'explication du flux est la suivante:

1) Lorsque l'utilisateur authentifie le serveur dans l'authentificateur de serveur hors bande de l'utilisateur, l'authentificateur génère les informations d'authentification dynamique de l'utilisateur, telles qu'un mot de passe à usage unique. Afin de confirmer l'utilisation légitime de l'authentificateur par l'utilisateur, ce dernier peut être identifié à l'aide d'informations

biométriques telles que son visage, ses empreintes digitales ou son numéro d'identification personnel (PIN) sur le smartphone.

2) Le serveur d'authentification hors bande de l'utilisateur envoie les informations d'authentification de l'utilisateur au vérificateur.

3) Le vérificateur authentifie l'utilisateur en vérifiant les informations d'authentification reçues.

4) Le vérificateur envoie le résultat de l'authentification de l'utilisateur à la partie utilisatrice.

5) La partie utilisatrice fournit le service en fonction du résultat de l'authentification de l'utilisateur reçu du vérificateur.

Au lieu d'utiliser des informations d'authentification dynamique de l'utilisateur, il est possible d'utiliser une authentification forte basée sur l'ICP, telle que l'ICP et la FIDO (identité rapide en ligne). La valeur de défi requise pour l'authentification de l'utilisateur basée sur l'ICP peut être reçue en même temps que l'étape de génération et de présentation des informations d'authentification du serveur, ou le décalage reçu peut être utilisé comme valeur de défi.

# 9 Menaces et exigences en matière de sécurité

## 9.1 Menaces pour la sécurité

Dans le présent paragraphe, les menaces potentielles pour la sécurité qui peuvent découler du modèle d'authentification du serveur hors bande sont identifiées.

### 9.1.1 Prestataire de services en ligne frauduleux

Un attaquant fait accéder un utilisateur à un fournisseur de services en ligne frauduleux et l'incite à saisir son mot de passe pour qu'il soit volé au lieu d'utiliser l'authentificateur de serveur hors bande.

### 9.1.2 Impossible d'utiliser l'authentificateur de serveur hors bande

Si un utilisateur n'est pas en mesure d'utiliser son authentificateur de serveur hors bande en raison de la perte ou de la détérioration de l'authentificateur, il peut ne pas être en mesure d'accéder au service en ligne car il peut oublier le mot de passe de l'utilisateur actuel ou ne pas être en mesure d'utiliser une autre méthode d'authentification.

### 9.1.3 Utilisation non autorisée d'un authentificateur de serveur hors bande

Un attaquant peut utiliser l'authentificateur de serveur hors bande d'un utilisateur, par exemple en le volant.

### 9.1.4 Attaques à distance contre un authentificateur de serveur hors bande

Un pirate peut effectuer l'authentification à distance en installant un logiciel malveillant sur le smartphone sur lequel est installé le serveur d'authentification hors bande de l'utilisateur.

### 9.1.5 Fausse demande d'authentification du serveur

Lorsqu'un utilisateur utilise un service en ligne qui fournit une authentification de serveur hors bande, au moment où l'utilisateur essaie d'authentifier le serveur en comparant et en vérifiant les informations d'authentification du serveur, un attaquant envoie une fausse demande d'authentification de serveur à l'authentificateur hors bande de l'utilisateur en saisissant l'identifiant de l'utilisateur dans un terminal différent pour inciter l'utilisateur à effectuer une mauvaise authentification.

## 9.2 Exigences de sécurité

Dans le présent paragraphe, les exigences de sécurité sont décrites en réponse aux menaces de sécurité potentielles qui peuvent découler du modèle d'authentification du serveur hors bande. La relation entre chaque menace pour la sécurité et chaque exigence en matière de sécurité est décrite à l'Appendice I.

### 9.2.1 Restriction de l'authentification par mot de passe de l'utilisateur

Afin d'empêcher les utilisateurs qui ont enregistré un authentificateur de serveur hors bande de se faire voler leur mot de passe ou de le divulguer, la méthode d'authentification par mot de passe de l'utilisateur peut être restreinte, et seule l'authentification de l'utilisateur par l'authentificateur de serveur hors bande peut être autorisée.

### 9.2.2 Méthodes supplémentaires pour libérer l'authentificateur de serveur hors bande et réinitialiser le mot de passe de l'utilisateur

Des méthodes supplémentaires doivent être prévues pour libérer l'authentificateur de serveur hors bande enregistré et réinitialiser le mot de passe de l'utilisateur par le biais d'une authentification distincte de l'utilisateur, telle que la vérification de l'identité, la vérification du courrier électronique et les questions de sécurité.

### 9.2.3 Méthodes d'authentification supplémentaires dans l'authentificateur de serveur hors bande

Lors de l'authentification du serveur par l'authentificateur, une méthode d'authentification supplémentaire peut être fournie pour vérifier que l'utilisateur est légitime, telle que l'authentification par code PIN ou biométrique par le smartphone sur lequel l'authentificateur de serveur hors bande est installé.

### 9.2.4 Contrôle simultané des demandes d'authentification du serveur

Une fois que les informations d'authentification du serveur sont affichées par l'authentificateur de serveur hors bande, les nouvelles demandes d'authentification du serveur doivent être bloquées ou mises en file d'attente jusqu'à ce que l'utilisateur ait terminé l'authentification du serveur.

# Annexe A

## Procédure supplémentaire pour l'authentification du serveur hors bande

(Cette annexe fait partie intégrante de la présente Recommandation.)

### A.1 Renouvellement automatique du mot de passe de l'utilisateur

Lors de l'étape de renouvellement automatique du mot de passe de l'utilisateur, le fournisseur de services en ligne renouvelle automatiquement le mot de passe du compte de l'utilisateur après que la partie utilisatrice a fourni un service à l'utilisateur par le biais d'une authentification de serveur hors bande. Les fournisseurs de services en ligne peuvent maintenir le concept de mots de passe utilisateur afin de minimiser les changements apportés aux structures et fonctions de données existantes, tout en renforçant la sécurité des mots de passe utilisateur.

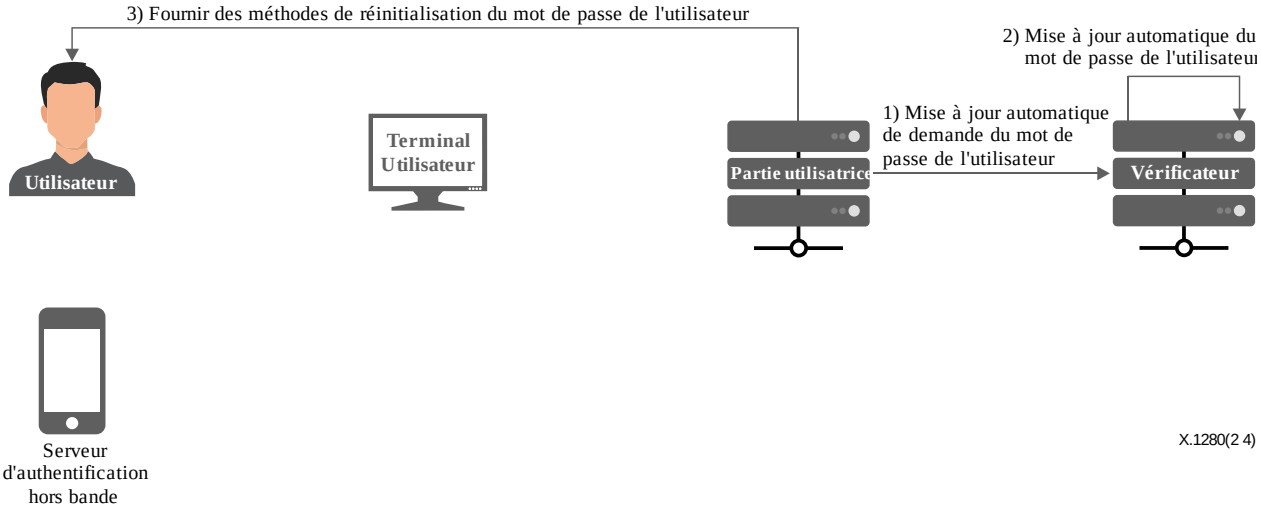


**Figure A.1 – Déroulement du renouvellement automatique du mot de passe de l'utilisateur**

La Figure A.1 identifie les données nécessaires à l'étape de renouvellement automatique du mot de passe de l'utilisateur et montre le flux. Ce flux suppose que le vérificateur effectue le renouvellement automatique du mot de passe de l'utilisateur, qui peut être effectué soit par la partie utilisatrice, soit par le vérificateur. L'explication du flux est la suivante:

1) Une fois que la partie a fourni un service à l'utilisateur après l'authentification du serveur hors bande, une demande de renouvellement du mot de passe de l'utilisateur est envoyée au vérificateur.

2) Le vérificateur remplace le mot de passe de l'utilisateur par une valeur générée de manière aléatoire avec une règle complexe.

3) S'il est impossible d'utiliser l'authentificateur de serveur hors bande enregistré par l'utilisateur en raison d'une perte, etc., la partie utilisatrice fournit une méthode pour libérer l'authentificateur et réinitialiser le mot de passe de l'utilisateur par le biais d'une authentification séparée, de sorte que l'utilisateur puisse utiliser le service avec le mot de passe de l'utilisateur réinitialisé.

L'utilisateur peut gérer son mot de passe sans le modifier régulièrement et rester à l'abri des fuites de mot de passe.

# Appendice I

## Relation entre les exigences de sécurité et les menaces

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Dans le présent appendice, la relation entre les menaces potentielles pour la sécurité qui peuvent découler du modèle d'authentification du serveur hors bande et les exigences en matière de sécurité est définie dans le Tableau I.1.

**Tableau I.1 – Relation entre les exigences de sécurité et les menaces**

| **Exigences de sécurité** | **Menaces pour la sécurité** | | | | |
|---|---|---|---|---|---|
| | Service en ligne frauduleux | Impossible d'utiliser l'authentificateur de serveur hors bande | Utilisation non autorisée d'un authentificateur de serveur hors bande | Attaques à distance contre un authentificateur de serveur hors bande | Fausse demande d'authentification du serveur |
| Restriction de l'authentification par mot de passe de l'utilisateur | **O** | – | – | – | – |
| Méthodes d'authentification supplémentaires | – | **O** | – | – | – |
| Méthodes supplémentaires d'authentification des utilisateurs | – | – | **O** | **O** | – |
| Contrôle simultané des demandes d'authentification du serveur | – | – | – | – | **O** |

# Appendice II

## Cas d'utilisation du modèle d'authentification du serveur hors bande

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

### II.1 Sites web et applications

Les sites web, les applications web et diverses applications qui n'utilisent pas de navigateur web peuvent résoudre les limites de l'authentification de serveur basée sur l'ICP en appliquant le modèle d'authentification de serveur hors bande.

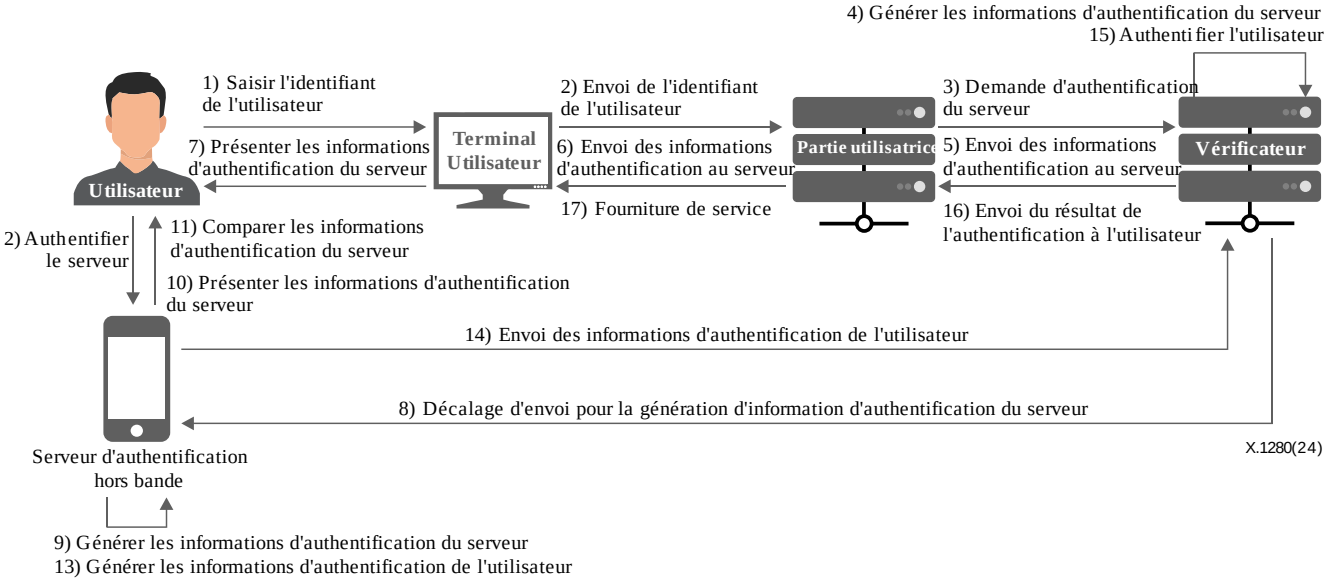


**Figure II.1 – Flux de l'authentification du serveur hors bande pour les sites web et les applications**

La Figure II.1 présente le flux d'authentification du serveur hors bande pour les sites web et les applications.

Même dans le cas de sites web d'entreprise et d'applications web utilisant un système de nom de domaine privé (DNS) qui ne peuvent obtenir un certificat ICP par l'intermédiaire d'une autorité de certification, d'applications basées sur l'adresse IP et d'applications qui n'utilisent pas de navigateur web, l'utilisateur peut procéder à l'authentification en toute sécurité après avoir clairement vérifié les fournisseurs de services en ligne au préalable.

### II.2 IdP

Les fournisseurs d'identité (IdP) qui proposent les services OAuth 2.0 et SAML (Security Assertion Markup Language) peuvent appliquer le modèle d'authentification de serveur hors bande pour garantir la sécurité des comptes d'utilisateurs pour tous les services en ligne qui leur sont connectés.

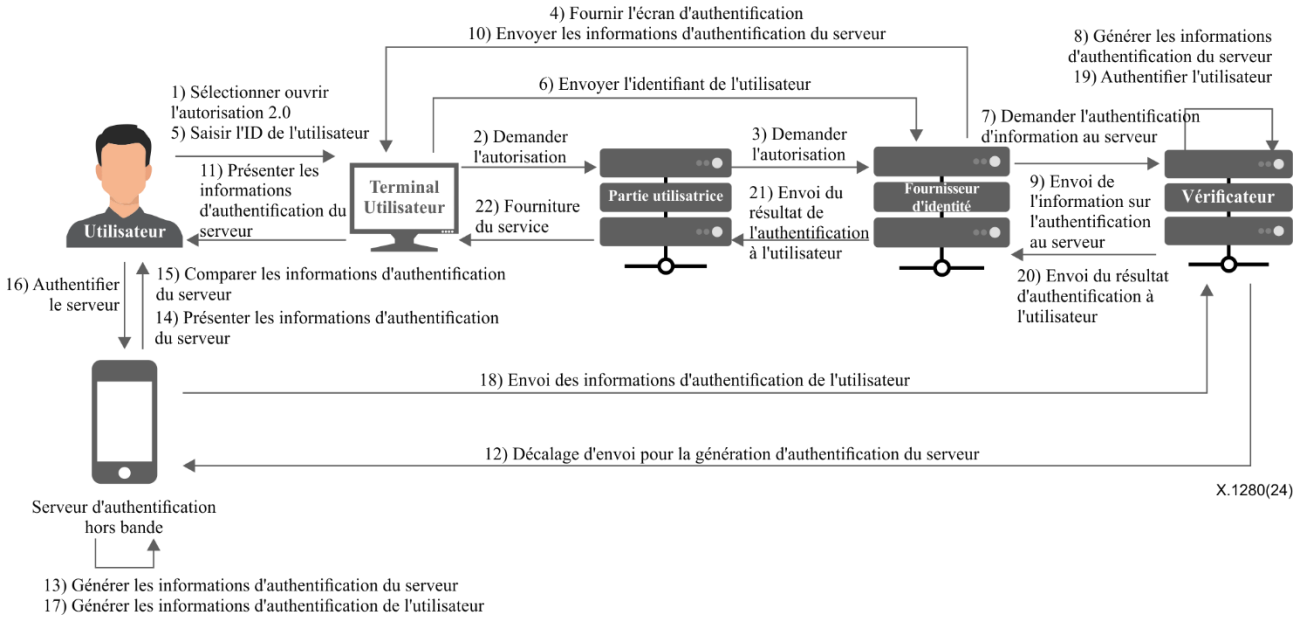


**Figure II.2 – Flux d'authentification du serveur hors bande pour les IdP**

La Figure II.2 présente le flux d'authentification du serveur hors bande pour les IdP.

Si les informations d'authentification de l'utilisateur du fournisseur d'identité sont divulguées à la suite d'une cyberattaque qui a usurpé l'identité de l'écran d'authentification du fournisseur d'identité, les comptes de tous les fournisseurs de services enregistrés par l'utilisateur peuvent être menacés. Les IdP peuvent s'affranchir du phishing et du détournement de domaine en ajoutant l'authentification du serveur hors bande.

## II.3 Systèmes d'exploitation

Les systèmes d'exploitation Windows et Linux peuvent appliquer le modèle d'authentification du serveur hors bande pour renforcer la sécurité du compte local du système d'exploitation.

Pour appliquer le modèle d'authentification au système d'exploitation Windows, il est nécessaire d'installer et de configurer un client de fournisseur d'informations d'identification tiers qui peut contrôler les informations d'identification du système d'exploitation.

Afin d'appliquer le modèle d'authentification aux systèmes d'exploitation basés sur Linux, il est nécessaire d'installer et de configurer des modules d'authentification enfichables (PAM).

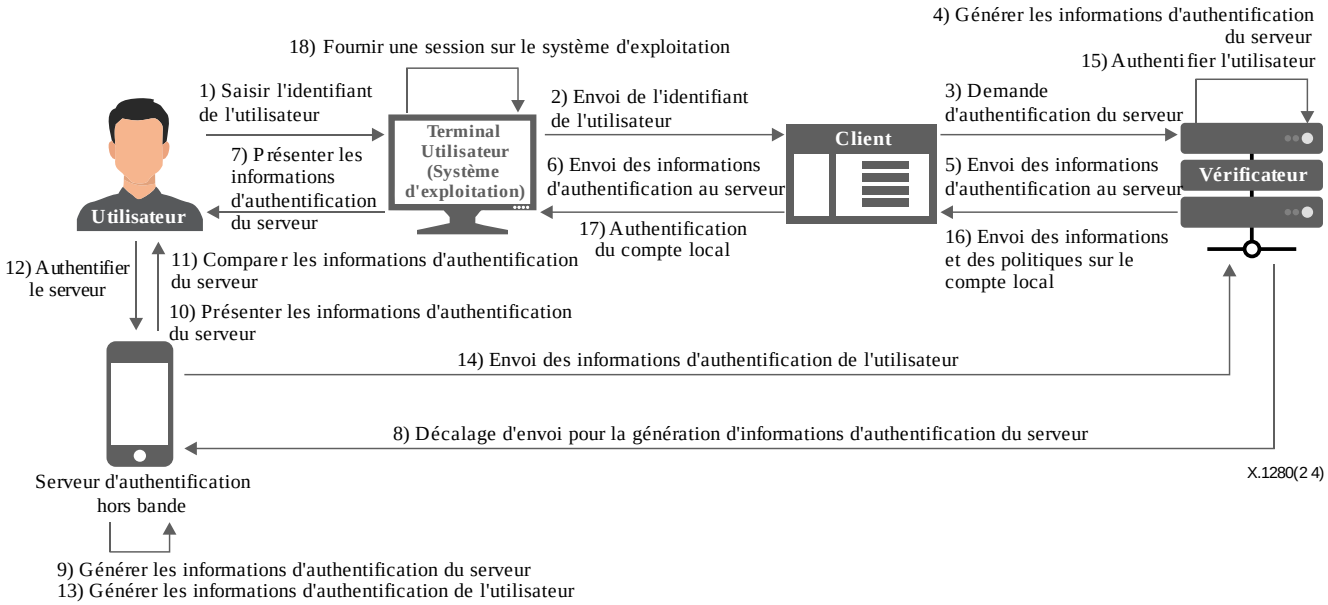


**Figure II.3 – Flux d'authentification du serveur hors bande pour les systèmes d'exploitation**

La Figure II.3 présente le flux d'authentification du serveur hors bande pour les systèmes d'exploitation.

Les utilisateurs peuvent clairement vérifier que le système d'exploitation auquel ils tentent d'accéder est correct, et il est possible d'éviter les incidents causés par l'écriture des informations d'accès sur un papier ou leur partage avec d'autres utilisateurs, même si le système d'exploitation fonctionne sur le cloud.

En outre, si le renouvellement automatique du mot de passe de l'utilisateur, une étape supplémentaire de la procédure d'authentification hors bande du serveur, est appliqué, les politiques de changement de mot de passe pour les comptes locaux peuvent être gérées plus facilement et en toute sécurité.

Après avoir saisi l'identifiant utilisateur, l'utilisateur peut utiliser le système d'exploitation après avoir vérifié les informations d'authentification du serveur affichées sur l'écran de connexion du système d'exploitation et l'authentificateur de serveur hors bande. L'utilisateur n'a pas besoin de taper un mot de passe ou d'utiliser un fichier clé pour accéder aux systèmes d'exploitation.

En outre, si le renouvellement automatique du mot de passe de l'utilisateur, une étape supplémentaire de la procédure d'authentification hors bande du serveur, est appliqué au client, le compte du système d'exploitation peut être géré plus facilement et en toute sécurité en changeant automatiquement le mot de passe du compte local du système d'exploitation.

# Appendice III

## Relations avec d'autres technologies d'authentification

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

Les technologies d'authentification sont une technologie fondamentale qui maintient la confiance entre les utilisateurs et les fournisseurs de services en ligne à l'ère numérique. Diverses technologies d'authentification, telles que OTP, FIDO et l'authentification mobile push, ont été développées et largement utilisées, en vue d'une authentification sûre, rentable et pratique. En conséquence, différents niveaux d'assurance d'authentification ont été classés pour les nouvelles technologies d'authentification dans les [b-UIT-T X.1254], [b-ISO/IEC 29115] et [b-NIST SP 800-63-3].

Les technologies d'authentification ayant été améliorées et normalisées, la résistance à l'usurpation d'identité du vérificateur est très demandée, de même que l'authenticité de l'utilisateur. Les technologies d'authentification qui répondent à cette exigence sont classées au niveau le plus élevé.

Cependant, comme les technologies d'authentification existantes n'authentifient que les utilisateurs, il y a des limites à la fourniture des seules informations d'authentification de l'utilisateur aux fournisseurs de services sans que les utilisateurs les vérifient explicitement pour la résistance à l'usurpation d'identité du vérificateur.

Les technologies existantes d'authentification des utilisateurs peuvent être principalement divisées en deux catégories: l'authentification en bande qui fournit des informations d'authentification par le biais du canal de communication principal entre les serveurs du fournisseur de services et les utilisateurs, et l'authentification hors bande qui fournit des informations d'authentification par le biais d'un canal de communication distinct.

Les technologies d'authentification en bande sont résistantes à l'usurpation d'identité du vérificateur, mais elles ne sont pas pratiques et ne sont pas rentables. Les technologies d'authentification hors bande sont pratiques et rentables, mais elles sont vulnérables à l'usurpation d'identité du vérificateur.

La Figure III.1 illustre le flux d'informations d'authentification pour l'authentification en bande et hors bande.

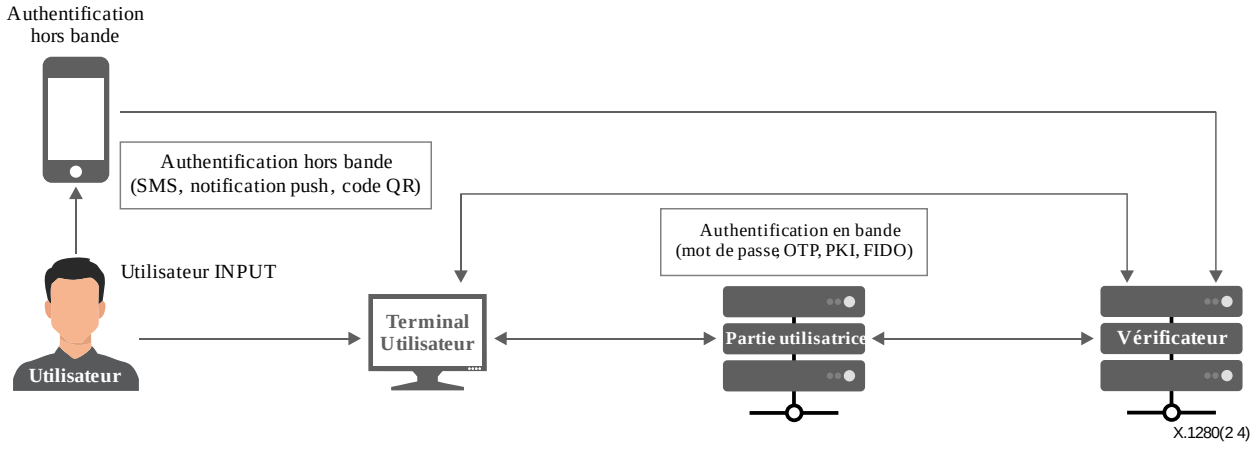


**Figure III.1 – Flux d'informations d'authentification pour l'authentification en bande et hors bande**

L'authentification en bande, telle que les technologies ICP, n'assure qu'implicitement la résistance à l'usurpation d'identité du vérificateur puisqu'elle ne fournit pas explicitement à l'utilisateur une méthode de vérification du fournisseur de services. Si un serveur ou une application est modifié, il doit réidentifier l'utilisateur et réémettre le certificat sur le terminal de l'utilisateur. En particulier,

FIDO est une technologie d'authentification intra-bande typique car l'authentificateur communique avec le serveur d'authentification via le terminal actuellement connecté à la partie utilisatrice, même si le facteur deux universel (U2F) et le protocole client-authentificateur (CTAP) semblent être un authentificateur externe indépendant du terminal. De ce fait, si deux terminaux ou plus sont utilisés à la maison ou au travail, l'utilisateur doit réenregistrer le service dans l'authentificateur FIDO de chaque terminal. De plus, même si vous utilisez un authentificateur CTAP, un authentificateur externe de FIDO2, il doit être enregistré ou reconnecté à chaque terminal. Par conséquent, les technologies d'authentification en bande basées sur l'ICP dépendent du terminal sans vérification explicite du fournisseur de services.

L'authentification hors bande, telle que la notification mobile push, est une technologie d'authentification qui vérifie la possession par l'utilisateur d'un authentificateur, qui n'a pas besoin de réidentifier l'utilisateur et de réémettre le certificat même en cas de changement de serveur ou d'application. Cependant, si l'utilisateur est déjà connecté à un serveur frauduleux sans savoir où il s'est connecté, il ne peut pas résister à l'usurpation d'identité du vérificateur, comme l'illustre la Figure III.2.

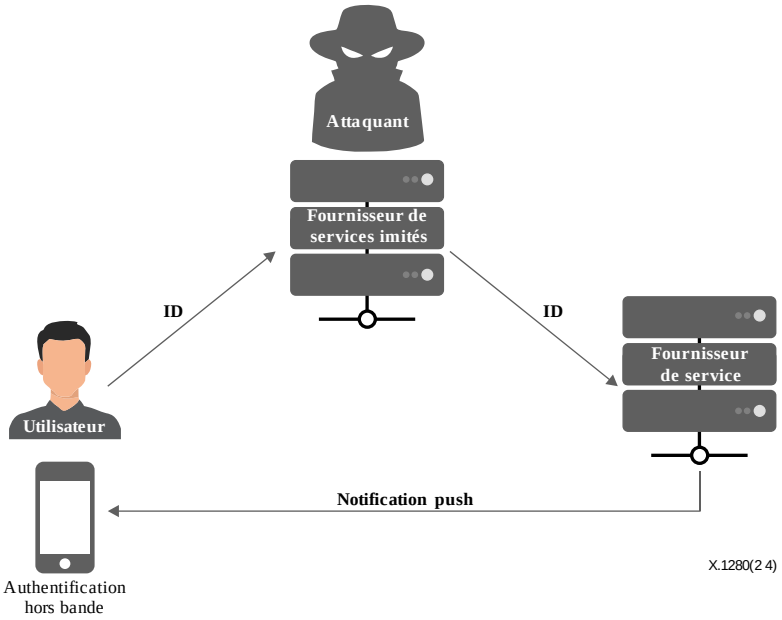


**Figure III.2 – Vulnérabilité de l'authentification hors bande de l'utilisateur face à un fournisseur de services dont l'identité a été usurpée**

Indépendamment des technologies d'authentification de l'utilisateur, il existe une technologie d'authentification du serveur web que l'utilisateur peut utiliser pour vérifier le fournisseur de services en contrôlant le certificat UIT-T X.509 connu sous la forme d'un symbole de cadenas sur le navigateur, mais cette technologie n'est pas alignée sur le processus d'authentification de l'utilisateur, de sorte que les utilisateurs peuvent trouver difficile de vérifier le certificat à chaque fois, et les utilisateurs qui ne sont pas familiers avec les technologies peuvent même ne pas vérifier le certificat. En outre, il est vulnérable aux attaques d'ingénierie sociale utilisant des noms de domaine similaires et n'est pas en mesure de vérifier les services en ligne utilisant un serveur DNS privé, les services en ligne basés sur l'adresse IP et les services en ligne non basés sur un navigateur.

Par conséquent, un cadre pour l'authentification du serveur hors bande peut être nécessaire pour surmonter la vulnérabilité liée à l'usurpation d'identité du vérificateur qui peut se produire lors de l'utilisation de technologies d'authentification de l'utilisateur hors bande et la limitation de la dépendance du terminal de l'authentificateur héritée de l'utilisation de technologies d'authentification de l'utilisateur en bande basées sur l'ICP.

# Bibliographie


[b-UIT-T X.509] Recommandation UIT-T X.509 (2019) *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[b-UIT-T X.1254] Recommandation UIT-T X.1254 (2020), *Infrastructure d'assurance de l'authentification des entités*.

[b-UIT-T X.1277] Recommandation UIT-T X.1277 (2018), *Cadre d'authentification universel*.

[b-UIT-T X.1278] Recommandation UIT-T X.1278 (2018), *Protocole client-authentificateur/cadre universel à deux facteurs*.

[b-ISO/IEC 29115] ISO/IEC 29115:2013, *Technologies de l'information – Techniques de sécurité – Cadre d'assurance de l'authentification d'entité*.

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2021, *Sécurité de l'information – Services d'horodatage – Partie 2: Mécanismes produisant des jetons indépendants*.

[b-NIST SP 800-63-3] NIST SP 800-63-3:2017, *Digital Identity Guidelines*.

# SÉRIES DES RECOMMANDATIONS UIT-T

| | |
|---|---|
| Série A | Organisation du travail de l'UIT-T |
| Série D | Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC |
| Série E | Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains |
| Série F | Services de télécommunication non téléphoniques |
| Série G | Systèmes et supports de transmission, systèmes et réseaux numériques |
| Série H | Systèmes audiovisuels et multimédias |
| Série I | Réseau numérique à intégration de services |
| Série J | Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias |
| Série K | Protection contre les perturbations |
| Série L | Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures |
| Série M | Gestion des télécommunications y compris le RGT et maintenance des réseaux |
| Série N | Maintenance: circuits internationaux de transmission radiophonique et télévisuelle |
| Série O | Spécifications des appareils de mesure |
| Série P | Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux |
| Série Q | Commutation et signalisation et mesures et tests associés |
| Série R | Transmission télégraphique |
| Série S | Equipements terminaux de télégraphie |
| Série T | Terminaux des services télématiques |
| Série U | Commutation télégraphique |
| Série V | Communications de données sur le réseau téléphonique |
| **Série X** | **Réseaux de données, communication entre systèmes ouverts et sécurité** |
| Série Y | Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes |
| Série Z | Langages et aspects généraux logiciels des systèmes de télécommunication |

Publié en Suisse
Genève, 2024