



UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1122

(04/2004)

SÉRIE X: RÉSEAUX DE DONNÉES ET
COMMUNICATION ENTRE SYSTÈMES OUVERTS
Sécurité des télécommunications

**Lignes directrices pour la réalisation de
systèmes mobiles sécurisés basés sur
l'infrastructure de clés publiques (PKI)**

Recommandation UIT-T X.1122

RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES ET COMMUNICATION ENTRE SYSTÈMES OUVERTS

RÉSEAUX PUBLICS DE DONNÉES	
Services et fonctionnalités	X.1–X.19
Interfaces	X.20–X.49
Transmission, signalisation et commutation	X.50–X.89
Aspects réseau	X.90–X.149
Maintenance	X.150–X.179
Dispositions administratives	X.180–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	
Modèle et notation	X.200–X.209
Définitions des services	X.210–X.219
Spécifications des protocoles en mode connexion	X.220–X.229
Spécifications des protocoles en mode sans connexion	X.230–X.239
Formulaires PICS	X.240–X.259
Identification des protocoles	X.260–X.269
Protocoles de sécurité	X.270–X.279
Objets gérés des couches	X.280–X.289
Tests de conformité	X.290–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	
Généralités	X.300–X.349
Systèmes de transmission de données par satellite	X.350–X.369
Réseaux à protocole Internet	X.370–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	
Réseautage	X.600–X.629
Efficacité	X.630–X.639
Qualité de service	X.640–X.649
Dénomination, adressage et enregistrement	X.650–X.679
Notation de syntaxe abstraite numéro un (ASN.1)	X.680–X.699
GESTION OSI	
Cadre général et architecture de la gestion-systèmes	X.700–X.709
Service et protocole de communication de gestion	X.710–X.719
Structure de l'information de gestion	X.720–X.729
Fonctions de gestion et fonctions ODMA	X.730–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	
Engagement, concomitance et rétablissement	X.850–X.859
Traitement transactionnel	X.860–X.879
Opérations distantes	X.880–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DES TÉLÉCOMMUNICATIONS	X.1000–

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

Recommandation UIT-T X.1122

Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI)

Résumé

Bien qu'elles constituent des technologies propres à mettre en œuvre de nombreuses fonctions de sécurité (chiffrement, signature numérique, intégrité des données, etc.) dans le cadre des communications mobiles de bout en bout, les technologies à infrastructure de clés publiques (PKI) doivent être adaptées à ce type d'utilisation. Toutefois, la méthode permettant de construire et de gérer des systèmes mobiles sécurisés fondés sur les technologies PKI n'a pas encore été définie. La présente Recommandation décrit le cadre général pour l'établissement des systèmes de ce type.

Source

La Recommandation UIT-T X.1122 a été approuvée le 29 avril 2004 par la Commission d'études 17 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) 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 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.

A 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 à acquérir 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 la base de données des brevets du TSB.

© UIT 2004

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références normatives.....	1
3	Termes et définitions	2
3.1	Définitions relatives au cadre général des clés publiques et des certificats d'attribut.....	2
3.2	Définitions relatives à l'architecture de sécurité du modèle de référence OSI.....	2
3.3	Lignes directrices concernant l'utilisation et la gestion des définitions de services tiers de confiance	2
3.4	Caractéristiques des services et dispositions applicables à l'exploitation figurant dans les définitions IMT-2000.....	2
3.5	Définitions supplémentaires	2
4	Abréviations.....	3
5	Classification des technologies PKI	3
6	Modèles de systèmes mobiles sécurisés basés sur les technologies PKI.....	4
6.1	Modèle général de systèmes mobiles sécurisés basés sur les technologies PKI.....	4
6.2	Modèle passerelle de systèmes mobiles sécurisés basés sur les technologies PKI	6
7	Opérations PKI pour communications mobiles de données de bout en bout	6
7.1	Opérations PKI liées au cycle de vie du certificat.....	6
8	Modèle d'utilisation dans les services de télécommunication	9
8.1	Fonction à assurer dans le modèle d'utilisation par la couche Session.....	9
8.2	Modèle d'utilisation au niveau application.....	13
9	Exemples de configuration de système.....	14
9.1	Exemples de configuration de système de gestion de certificat	14
9.2	Exemple de modèle d'authentification basé sur le certificat	17
10	Infrastructure de clés publiques pour communications mobiles de données de bout en bout	20
10.1	Interopérabilité avec le système existant.....	20
10.2	Utilisation de l'infrastructure de clés publiques dans le service mobile.....	21
10.3	Généralités concernant l'infrastructure de clés publiques	23
	Appendice I – Exemples de modèles de service	24
I.1	Modèles de service de gestion de certificat.....	24

Recommandation UIT-T X.1122

Lignes directrices pour la réalisation de systèmes mobiles sécurisés basés sur l'infrastructure de clés publiques (PKI)

1 Domaine d'application

La présente Recommandation indique le cadre général pour l'établissement de systèmes mobiles sécurisés fondés sur les technologies PKI. La présente Recommandation couvre les applications suivantes:

- le contrôle des certificats utilisés généralement dans les systèmes de communication;
- toutefois, la définition d'une méthode d'établissement de communication mobile en tant que modèle d'établissement doit être exclue du domaine d'application de la présente Recommandation.

2 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. 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.

- Recommandation UIT-T F.116 (2000), *Fonctionnalités de service et dispositions d'exploitation des télécommunications IMT-2000*.
- Recommandation UIT-T Q.814 (2000), *Spécification d'un agent interactif d'échange informatisé de données*.
- Recommandation UIT-T Q.1701 (1999), *Cadre général des réseaux IMT-2000*.
- Recommandation UIT-T Q.1711 (1999), *Modèle fonctionnel réseau pour les IMT-2000*.
- Recommandation UIT-T Q.1761 (2004), *Convergence des systèmes fixes et des systèmes IMT-2000 existants: principes et prescriptions*.
- Recommandation UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.
- Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT*.
- Recommandation UIT-T X.842 (2000) | ISO/CEI TR 14516:2002, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'utilisation et à la gestion des services de tiers de confiance*.
- Recommandation UIT-T X.1121 (2004), *Cadre général des technologies de la sécurité pour les communications mobiles de données de bout en bout*.

3 Termes et définitions

3.1 Définitions relatives au cadre général des clés publiques et des certificats d'attribut

Les termes suivants sont définis dans la Rec. UIT-T X.509 | ISO/CEI 9594-8:

- a) autorité d'attribut;
- b) certificat d'attribut;
- c) autorité de certification (CA, *certification authority*);
- d) liste de révocation de certificat (CRL, *certificate revocation list*);
- e) clé publique;
- f) certificat de clé publique (certificat);
- g) infrastructure de clés publiques (PKI, *public key infrastructure*).

3.2 Définitions relatives à l'architecture de sécurité du modèle de référence OSI

Les termes suivants sont définis dans la Rec. UIT-T X.800 | ISO/CEI 7498-2:

- a) information d'authentification;
- b) confidentialité;
- c) cryptographie;
- d) clé;
- e) mot de passe.

3.3 Lignes directrices concernant l'utilisation et la gestion des définitions de services tiers de confiance

Les termes suivants sont définis dans la Rec. UIT-T X.842 | ISO/CEI TR 14516:

- a) autorité d'enregistrement.

3.4 Caractéristiques des services et dispositions applicables à l'exploitation figurant dans les définitions IMT-2000

Les termes suivants sont définis dans la Rec. UIT-T F.116:

- a) module d'identité utilisateur.

3.5 Définitions supplémentaires

La présente Recommandation définit les termes suivants:

3.5.1 système mobile sécurisé: un système permettant de réaliser des communications mobiles de données de bout en bout entre un utilisateur mobile et un fournisseur de services d'application ou entre utilisateurs mobiles.

3.5.2 référentiel des certificats: base de données dans laquelle certificats, listes de révocation de certificats et différentes informations liées à l'infrastructure de clés publiques sont enregistrés et accessibles en ligne.

3.5.3 autorité de validation: autorité assurant un service en ligne de vérification de la validité d'un certificat. Elle établit un trajet de certificat à des fins de vérification, depuis un signataire vers un utilisateur désireux de confirmer la validité de la signature du signataire et confirme le fait que tous les certificats figurant sur le trajet de vérification des certificats sont fiables ou ne sont pas annulés. Elle vérifie en outre si un certificat a ou non été annulé.

4 Abréviations

La présente Recommandation utilise les abréviations suivantes:

AA	autorité d'attribut (<i>attribute authority</i>)
ASP	fournisseur de services d'application (<i>application service provider</i>)
CA	autorité de certification (<i>certification authority</i>)
CMC	gestion des certificats sur CMS (<i>certificate management over CMS</i>)
CMP	protocole de gestion de certificat (<i>certificate management protocol</i>)
CRL	liste de révocation de certificat (<i>certificate revocation list</i>)
ID	identificateur
PIN	numéro d'identification personnel (<i>personal identification number</i>)
PKI	infrastructure de clés publiques (<i>public-key infrastructure</i>)
POP	preuve de détention (<i>proof of possession</i>)
RA	autorité d'enregistrement (<i>registration authority</i>)
RSA	algorithme de clé publique RSA (<i>RSA public key algorithm</i>)
TLS	sécurité de couche Transport (<i>transport layer security</i>)
UIM	module d'identité d'utilisateur (<i>user identity module</i>)
VA	autorité de validation (<i>validation authority</i>)

5 Classification des technologies PKI

Les technologies de sécurité fondées sur l'infrastructure de clés publiques sont appliquées à la relation entre terminaux mobiles et serveurs d'application dans le modèle général des systèmes mobiles de communication de données de bout en bout entre utilisateurs mobiles et fournisseurs de services d'application ou à la relation entre terminaux mobiles et passerelle de sécurité mobile d'une part et entre passerelle de sécurité mobile et serveur dans le modèle passerelle de communications mobiles de données de bout en bout entre utilisateurs mobiles et fournisseurs de services d'application.

Les technologies de sécurisation PKI servent à mettre en œuvre les fonctions suivantes de sécurité:

- 1) chiffrement;
- 2) échange de clés;
- 3) signature numérique;
- 4) contrôle d'accès;
- 5) intégrité des données;
- 6) échange d'authentification;
- 7) notarisation.

Tableau 1/X.1122 – Fonctions et points d'application des technologies PKI

Points d'application des technologies	Terminal mobile	Serveur d'application/ passerelle de sécurité mobile	Relation entre utilisateur mobile et terminal mobile	Relation entre terminal mobile et serveur d'application ou autres relations
Fonctions assurées par les technologies				
Chiffrement				X
Echange de clé				X
Signature numérique				X
Contrôle d'accès				X
Intégrité des données				X
Echange d'authentification				X
Notarisation				X

Bien que les technologies PKI soient fréquemment mises en œuvre dans un réseau ouvert afin d'assurer les fonctions de sécurité ci-dessus, certaines adaptations des technologies PKI doivent être réalisées en raison des caractéristiques dans le cas des communications mobiles de bout en bout (en particulier de la faible puissance de traitement et de la faible capacité de mémoire).

6 Modèles de systèmes mobiles sécurisés basés sur les technologies PKI

Comme d'autres systèmes mobiles sécurisés, les modèles de systèmes mobiles sécurisés basés sur les technologies PKI sont classés comme suit: modèle général de systèmes mobiles sécurisés basés sur les technologies PKI pour les communications entre utilisateur mobile et fournisseur de services d'application, et modèle passerelle de systèmes mobiles sécurisés basés sur les technologies PKI pour les communications entre utilisateur mobile et fournisseur de services d'application.

Toutefois, aux fins des utilisations opérationnelles des technologies PKI (par exemple, gestion du cycle de vie des certificats), certaines entités (CA, RA, VA, Référentiel, etc.) sont ajoutées aux modèles.

6.1 Modèle général de systèmes mobiles sécurisés basés sur les technologies PKI

La description du modèle général de systèmes mobiles sécurisés basés sur les technologies PKI pour les communications entre utilisateur mobile et fournisseur de services d'application est décrite dans la Figure 1.

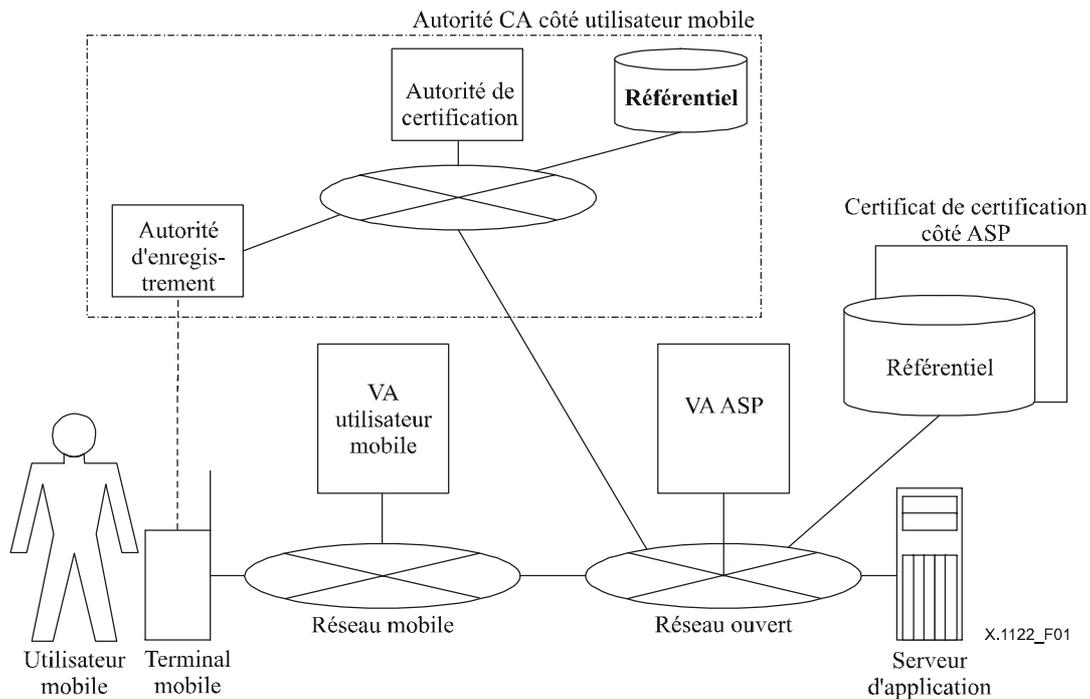


Figure 1/X.1122 – Modèle général de systèmes mobiles sécurisés basés sur les technologies PKI

Ce modèle contient des entités supplémentaires par rapport au modèle général des communications mobiles de données de bout en bout entre utilisateur mobile et fournisseur de services d'application: autorité de certification côté utilisateur mobile (comprenant l'autorité d'enregistrement et le référentiel), autorité de validation côté utilisateur mobile, autorité de certification côté fournisseur ASP et autorité de validation côté fournisseur ASP.

– *Autorité CA de certification côté utilisateur mobile*

L'autorité de certification CA côté utilisateur mobile délivre et gère les certificats d'utilisateur mobile ou de terminal mobile. Elle contient l'autorité d'enregistrement RA chargée d'identifier et d'authentifier les utilisateurs mobiles, ainsi que le référentiel dans lequel sont enregistrés les certificats et les listes de révocation de certificat des utilisateurs mobiles.

– *Autorité VA de validation des utilisateurs mobiles*

L'autorité VA de validation des utilisateurs mobiles offre à ces derniers un service en ligne de vérification de la validité des certificats reçus par les utilisateurs mobiles.

– *Autorité de certification côté fournisseur ASP*

L'autorité de certification côté fournisseur ASP établit et gère les certificats de fournisseur ASP ou les certificats de serveur d'application. Elle inclut en outre l'autorité d'enregistrement qui assure l'identification et l'authentification des fournisseurs ASP comme du référentiel qui enregistre les certificats et les listes de révocation de certificat des fournisseurs ASP.

– *Autorité VA de validation des fournisseurs ASP*

L'autorité VA des fournisseurs ASP fournit un service en ligne de vérification de la validité des certificats obtenus par les fournisseurs ASP.

6.2 Modèle passerelle de systèmes mobiles sécurisés basés sur les technologies PKI

La Figure 2 donne la description du modèle passerelle de systèmes mobiles sécurisés basés sur les technologies PKI pour les communications entre utilisateur mobile et fournisseur ASP.

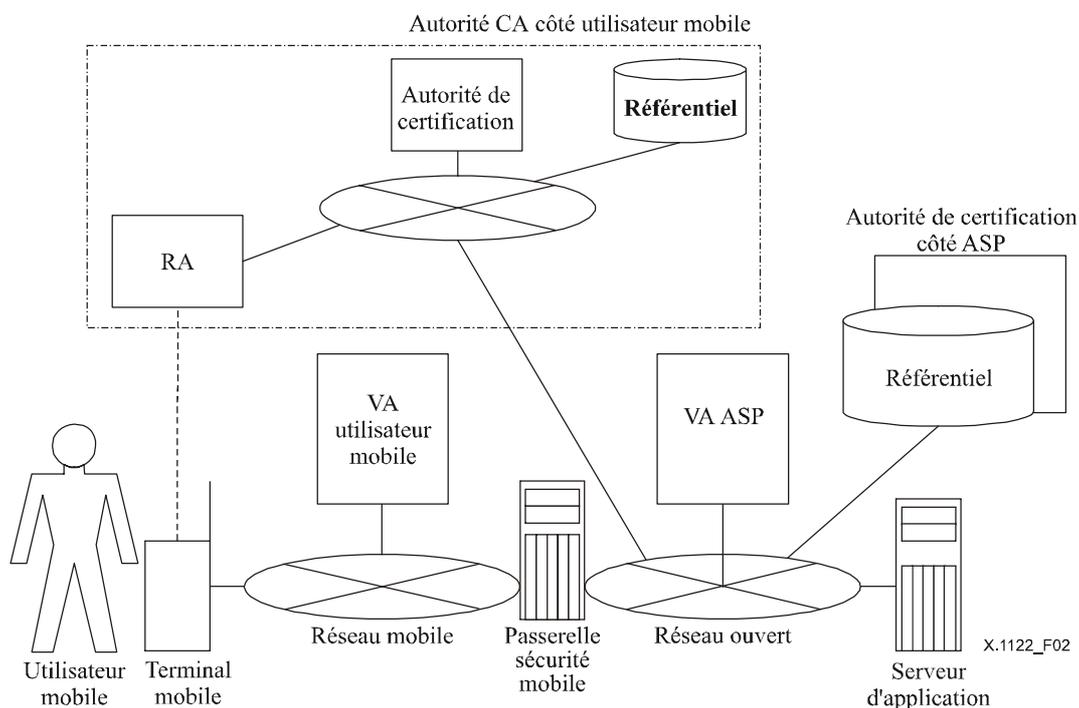


Figure 2/X.1122 – Modèle passerelle de systèmes mobiles sécurisés basés sur les technologies PKI

A l'instar du modèle général des systèmes mobiles sécurisés basés sur les technologies PKI pour les communications entre utilisateur mobile et fournisseur ASP, ce modèle contient les entités supplémentaires suivantes par rapport au modèle passerelle de communications mobiles de données de bout en bout entre utilisateur mobile et fournisseur de services d'application: autorité de certification côté utilisateur mobile (comprenant l'autorité d'enregistrement et le référentiel), autorité de validation côté utilisateur mobile, autorité de certification côté fournisseur ASP et autorité de validation côté fournisseur ASP.

7 Opérations PKI pour communications mobiles de données de bout en bout

7.1 Opérations PKI liées au cycle de vie du certificat

Le cycle de vie du certificat comporte généralement les étapes suivantes:

- 1) génération d'une paire de clés privée et publique;
- 2) demande, émission et activation du certificat;
- 3) utilisation du certificat;
- 4) rénovation du certificat;
- 5) renouvellement du certificat.

7.1.1 Génération de la paire de clés l'une privée l'autre publique

La génération d'une paire de clés (l'une privée l'autre publique), fait l'objet de différents modèles, selon l'entité génératrice des clés ou l'emplacement de leur génération.

7.1.1.1 Entité génératrice de clés.

En dépit de l'intérêt du point de vue de la sécurité du modèle comportant la génération des clés par l'utilisateur mobile, on peut envisager un modèle dans lequel l'autorité de certification génère les clés à la place de l'utilisateur mobile et enfin un modèle dans lequel cette tâche incombe à un tiers.

Avec les modèles dans lesquels le traitement des clés est assuré par un tiers, l'utilisateur peut dans un cas acheter l'appareil dans lequel les clés sont installées. (L'appareil en question peut être un terminal mobile ou un composant associé au terminal mobile); le fabricant de l'appareil assure alors la génération de la clé.

7.1.1.2 Emplacement de génération des clés.

Dans certains modèles les clés sont générées au sein de l'appareil et dans d'autres elles sont à l'extérieur, puis installées dans celui-ci.

7.1.2 Demande, émission et activation du certificat

La demande, l'émission et l'activation du certificat font l'objet de différents modèles selon que ces opérations sont effectuées en ligne ou non à chaque étape.

Dans certains cas le certificat est censé être activé dès son émission.

Le choix du modèle dépend de la personne à qui le certificat est délivré (utilisateur mobile), de l'émetteur (CA), de la nature des garanties offertes et de la finalité de son utilisation, etc.

En outre, dans un environnement mobile, les modèles sont différents selon la synchronisation des opérations suivantes:

- a) génération des clés;
- b) émission du certificat;
- c) activation du certificat;
- d) obtention de l'appareil.

7.1.2.1 Modèle dans lequel l'obtention de l'appareil suit l'activation du certificat (dans ce modèle les éléments ci-dessus interviennent dans l'ordre suivant (a)→(b)→(c)→(d))

Ce modèle correspond au cas dans lequel l'utilisateur mobile achète un appareil dans lequel les clés et le certificat ont été préalablement installés. Dans ce modèle, il est possible de vendre un appareil où a été installé au préalable un certificat dont le sujet n'est pas lié à l'utilisateur mobile (par exemple lorsque l'appareil est un terminal mobile, le numéro de téléphone ou le numéro de série électronique peut faire office de sujet, ou encore d'installer le certificat au magasin au moment de l'achat de l'appareil. Le traitement et l'installation du certificat dépendent des informations concernant l'application au moment de la demande d'un appareil). Dans ce cas, (b), (c) et (d) doivent intervenir simultanément.

7.1.2.2 Modèle dans lequel un utilisateur obtient un appareil dans lequel le certificat a déjà été émis (modèle dans lequel les éléments ci-dessus se déroulent dans l'ordre (a)→(b)→(d)→(c))

Ce modèle est pour l'essentiel identique au précédent, bien qu'il exige une procédure d'activation du certificat suite à l'obtention de l'appareil. Il convient de maintenir un court laps de temps entre (b) et (d).

7.1.2.3 Modèle dans lequel un utilisateur se procure un appareil qui enregistre uniquement les clés (modèle dans lequel les éléments ci-dessus se déroulent dans l'ordre (a)→(d)→(b)→(c))

Modèle correspondant au cas dans lequel l'utilisateur demande le certificat en ligne après avoir acheté un appareil sur lequel les clés sont installées.

7.1.2.4 Modèle dans lequel un utilisateur se procure un appareil ne comportant pas de clé ni de certificat installé (modèle dans lequel les éléments ci-dessus se déroulent dans l'ordre (d)→(a)→(b)→(c))

Dans ce modèle, l'utilisateur génère les clés et demande un certificat après acquisition de l'appareil. Ce modèle doit assurer la confidentialité de la clé privée d'un terminal mobile, lui-même doté d'une capacité de calcul, d'une mémoire de stockage et d'un temps de traitement suffisants pour générer les clés à l'intérieur de l'appareil.

7.1.3 Utilisation du certificat

7.1.3.1 Signataire

Le signataire associe son certificat au message signé et l'envoie au vérificateur. Il existe différents modèles selon la méthode d'association (par exemple joindre le certificat au message et lui associer l'emplacement du référentiel).

7.1.3.2 Vérificateur

La vérification de l'authenticité du message reçu par le signataire exige les opérations suivantes:

1) *Vérification de la validité du certificat*

Cette opération vise à vérifier l'authenticité du certificat du signataire. Concrètement, elle consiste à établir un itinéraire d'authentification du certificat et à vérifier la validité de chaque certificat sur l'itinéraire d'authentification.

Selon la méthode de vérification, on dispose de deux modèles:

a) *Modèle dans lequel le vérificateur assure lui-même la vérification*

Au moment de la vérification, le vérificateur découvre l'itinéraire d'authentification et vérifie la validité de chaque certificat sur l'itinéraire d'authentification.

Pour la vérification de chaque certificat, le vérificateur établit la validité du certificat en obtenant la liste CRL du centre d'information de l'autorité de certification ou en la demandant à l'autorité de certification qui indique en ligne ou non l'information de statut des certificats.

Il est à noter que la fréquence des relevés de liste CRL ou des demandes adressées à l'autorité de certification dépend de l'utilisation et de l'importance du certificat (en principe indispensable à chaque vérification du certificat).

b) *Modèle comportant l'utilisation d'une autorité de vérification fiable*

Une demande concernant la validité du certificat associé au message est adressée à l'autorité de vérification, celle-ci procédant à la vérification proprement dite (découverte d'un itinéraire d'authentification et vérification de la validité de chaque certificat).

Cette opération peut être omise dans différents cas notamment dans celui d'un certificat de courte durée.

2) *Vérification de la signature apposée au message*

Cette opération vise à vérifier l'authenticité de la signature apposée au message.

Dans de nombreux cas le vérificateur vérifie lui-même une signature au moyen de la clé publique contenue dans le certificat, bien que dans certains modèles l'autorité de vérification procède elle-même à cette tâche.

7.1.4 Révocation du certificat

Cette tâche vise à demander la révocation du certificat à l'autorité de certification, et permet d'annuler le certificat. Selon la méthode utilisée, on distingue deux modèles de révocation du certificat: avec demande de révocation faite respectivement en ligne et hors ligne.

7.1.5 Renouvellement du certificat

Cette tâche vise à annuler un certificat existant, à produire une nouvelle paire de clés et à recevoir un nouveau certificat émis par l'autorité de certification. En principe, la demande de révocation et l'émission d'un certificat interviennent successivement, mais il existe différents modèles selon l'ordre des opérations et selon que (les informations correspondantes) le certificat actuel est utilisé dans la demande de nouveau certificat.

8 Modèle d'utilisation dans les services de télécommunication

Le présent paragraphe indique le modèle d'utilisation auquel l'infrastructure de clés publiques permettra d'accéder.

Il existe deux types de modèles d'utilisation: un modèle d'utilisation par la couche Session et un modèle d'utilisation par la couche Application. Le premier assure les fonctions de chiffrement des communications, d'authentification et d'intégrité des données par la couche Session dans le modèle de référence ISO (par exemple sécurité de couche Transport). Par ailleurs, le modèle d'utilisation par la couche Application assure les fonctions d'intégrité et de confidentialité sur la couche Application.

Nombre des implémentations actuelles du modèle d'utilisation par la couche Session (la sécurité de la couche Transport figure parmi les utilisations les plus connues) sont conçues pour assurer un transport sécurisé de bout en bout et offrir un tunnel sécurisé entre un serveur et un client. Le client et le serveur peuvent donc se délivrer mutuellement une autorisation et l'utilisation de l'infrastructure de clés publiques permet de réaliser ces authentifications.

Le modèle d'utilisation par la couche Session est basé sur les fonctions de sécurité suivantes:

- authentification du serveur;
- authentification du client;
- chiffrement et intégrité de l'itinéraire de communication.

Le modèle d'utilisation par la couche Application est basé sur les fonctions de sécurité suivantes:

- fonction de signature numérique au niveau application (pour l'intégrité et l'authentification);
- fonction de chiffrement des données au niveau application (pour la confidentialité).

Par ailleurs, il est également possible de concevoir un modèle d'utilisation par la couche Réseau.

8.1 Fonction à assurer dans le modèle d'utilisation par la couche Session

Le modèle d'utilisation par la couche Session assure les fonctions suivantes: la fonction d'authentification du serveur, la fonction d'authentification du client et celle du chiffrement du trajet de communication et d'intégrité (en fait, cette fonction sera assurée par une combinaison de la fonction authentification du serveur et de chiffrement et d'intégrité du trajet de communication ou encore d'une combinaison de la fonction authentification de serveur, authentification du client et chiffrement et intégrité du trajet de communication). Les applications de ce modèle d'utilisation (par exemple sécurité de la couche Transport) peuvent être mises à profit dans les communications mobiles de données de bout en bout afin d'obtenir l'authentification aussi bien d'un terminal mobile que d'un serveur d'application, et d'obtenir un tunnel sécurisé entre deux points d'extrémité. Les différents rôles du certificat sont très importants dans le cadre de ce modèle d'utilisation. Il importe

par conséquent de spécifier la procédure d'émission, de révocation ou de suspension du certificat ainsi que la méthode d'authentification applicable à un utilisateur et à un serveur.

8.1.1 Authentification du serveur dans le modèle d'utilisation par la couche Session

Puisqu'on distingue deux modèles pour les systèmes mobiles sécurisés basés sur l'infrastructure de clés multiples tel qu'indiqué au § 6, il existe deux types d'authentification de serveur: dans le modèle général et dans le modèle passerelle.

Pour l'authentification de serveur dans le modèle général, le terminal mobile vérifie le serveur d'application au moyen du certificat présenté par celui-ci et de la signature numérique figurant sur le message reçu au cours d'une procédure d'échange.

L'authentification de serveur dans le modèle général comporte les opérations suivantes:

- le serveur d'application envoie son certificat et les informations d'authentification appropriées au terminal mobile;
- le terminal mobile vérifie si le certificat est émis par l'autorité de certification à laquelle le terminal mobile fait confiance;
- le terminal mobile vérifie la validité des informations d'authentification reçues au moyen de la clé publique du certificat du serveur d'application;
- simultanément, le terminal mobile détermine si le serveur d'application auquel il tente d'accéder est effectivement celui qui convient.

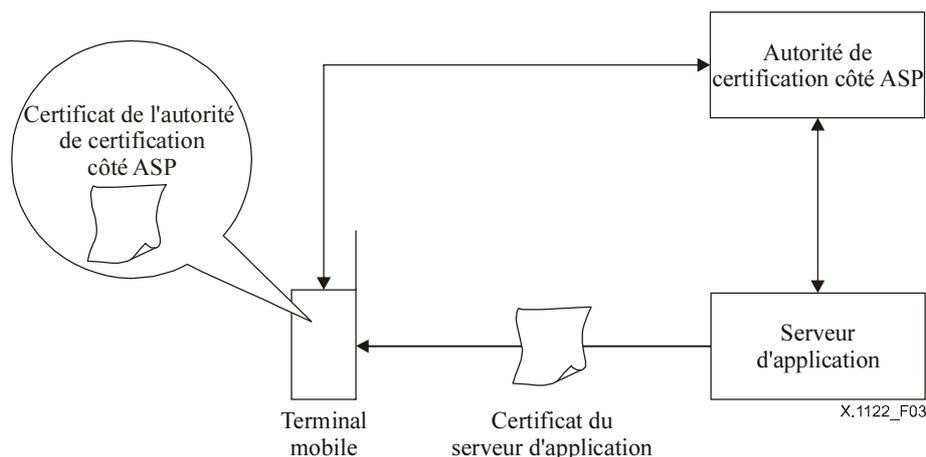


Figure 3/X.1122 – Authentification du serveur dans le modèle général

L'authentification du serveur dans le modèle passerelle réalise une authentification en deux phases entre le terminal mobile et la passerelle de sécurité mobile, et entre la passerelle de sécurité mobile et le serveur d'application.

L'authentification du serveur en deux phases comporte les opérations suivantes:

- en premier lieu, une session protégée est établie entre le terminal mobile et la passerelle de sécurité mobile, au moyen du certificat de la passerelle de sécurité mobile;
- ensuite, une session protégée est également établie entre la passerelle de sécurité mobile et le serveur d'application.

Par conséquent, selon cette authentification de serveur en deux phases, la passerelle de sécurité mobile doit pouvoir transformer correctement la session protégée entre terminal mobile et passerelle de sécurité mobile, en une session protégée entre passerelle de sécurité mobile et serveur d'application.

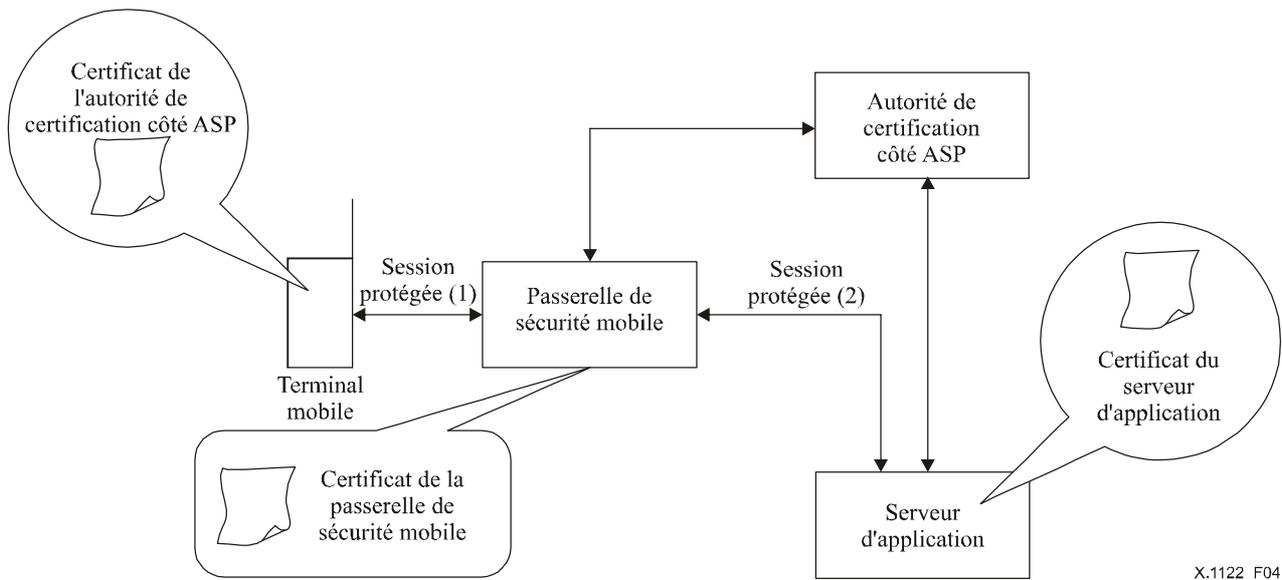


Figure 4/X.1122 – Authentification du serveur dans le modèle passerelle

8.1.2 Authentification du client dans le modèle d'utilisation par la couche Session

Pour l'authentification du client dans le modèle d'utilisation par la couche Session, le terminal mobile présente le certificat et les informations d'authentification appropriées au serveur d'application en réponse à la demande de celui-ci; le serveur d'application procède alors à l'authentification du client.

L'authentification du client dans ce modèle d'utilisation comporte les opérations suivantes:

- le terminal mobile envoie le certificat au serveur d'application;
- simultanément, le terminal mobile envoie au serveur d'application le message de vérification signé (créé au moyen de la clé privée du client);
- le serveur d'application vérifie le certificat du terminal mobile;
- de plus, le serveur d'application décrypte et vérifie le message de vérification du certificat au moyen de la clé publique contenue dans le certificat.

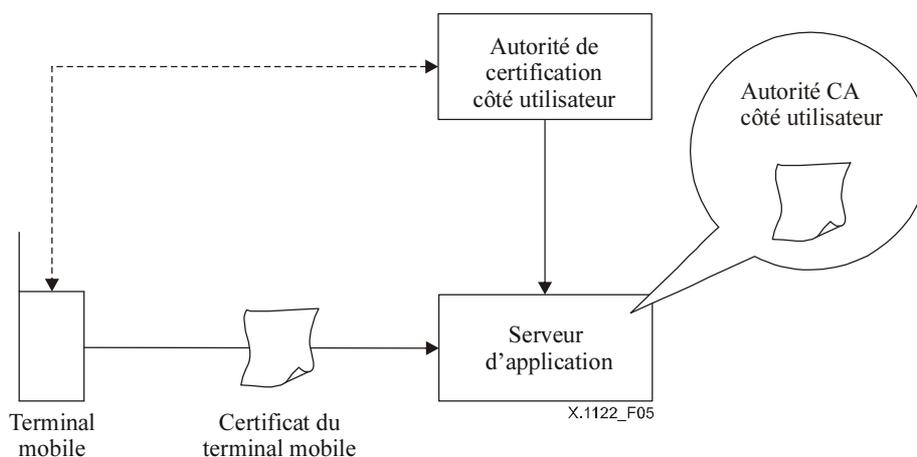
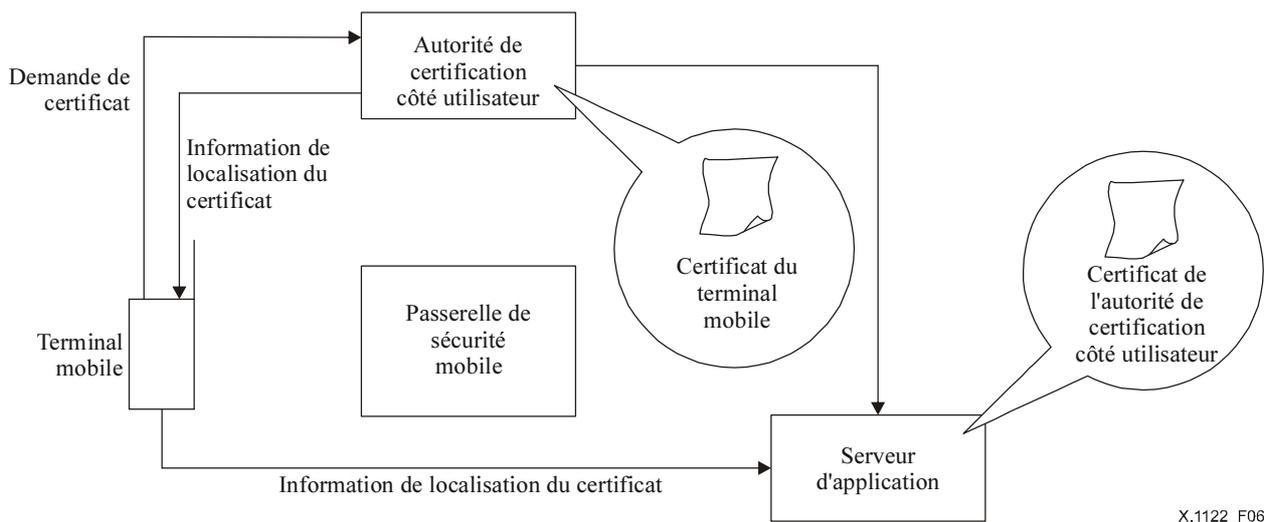


Figure 5/X.1122 – Authentification du client dans le modèle d'utilisation par la couche Session

En raison des caractéristiques des communications mobiles de données de bout en bout, certaines réalisations comportent les modifications suivantes de la procédure:

- le terminal mobile envoie à l'autorité de certification côté utilisateur (ou à son agent) une demande de certificat;
- l'autorité de certification authentifie le terminal mobile;
- l'autorité de certification produit le certificat du terminal mobile et envoie à celui-ci les données de localisation du certificat (notamment URL);
- l'autorité de certification enregistre le certificat du terminal mobile dans la zone de mémorisation;
- ensuite, le terminal mobile signe les données à signer et les envoie ainsi que la signature et les données de localisation du certificat au serveur d'application;
- le serveur d'application saisit le certificat du terminal mobile dans le référentiel au moyen des informations de localisation du certificat;
- le serveur d'application vérifie la validité du certificat du terminal mobile (si nécessaire), vérifie au moyen de sa clé publique la signature contenue dans le certificat du terminal mobile; enfin le serveur d'application authentifie le terminal mobile au moyen du certificat de ce dernier;
- une session protégée est établie entre le terminal mobile et le serveur d'application.



X.1122_F06

Figure 6/X.1122 – Authentification du client dans le modèle d'utilisation par la couche Session

8.1.3 Chiffrement et intégrité du trajet de communication dans le modèle d'utilisation par la couche Session

Le chiffrement et l'intégrité du trajet de communication dans le modèle d'utilisation par la couche Session impliquent les opérations suivantes:

- le terminal mobile transmet la série d'algorithmes de cryptographie utilisables et l'ordre de préférence correspondant au serveur d'application;
- le serveur d'application choisit l'algorithme de cryptographie dont le classement est le plus élevé parmi les algorithmes à clé commune utilisables par les deux parties;
- le serveur est authentifié afin d'éviter les utilisations frauduleuses du serveur d'application;

- le terminal mobile génère le nombre aléatoire utilisé comme valeur de départ pour la clé de session et le chiffre au moyen de la clé publique du serveur d'application dans le cas de la méthode d'échange de clés RSA, et envoie au serveur d'application la valeur de départ chiffrée de la clé de session. A partir de cette valeur de départ, serveur d'application et terminal mobile peuvent produire la clé de session commune pour les communications ultérieures;
- les communications chiffrées commencent ensuite.

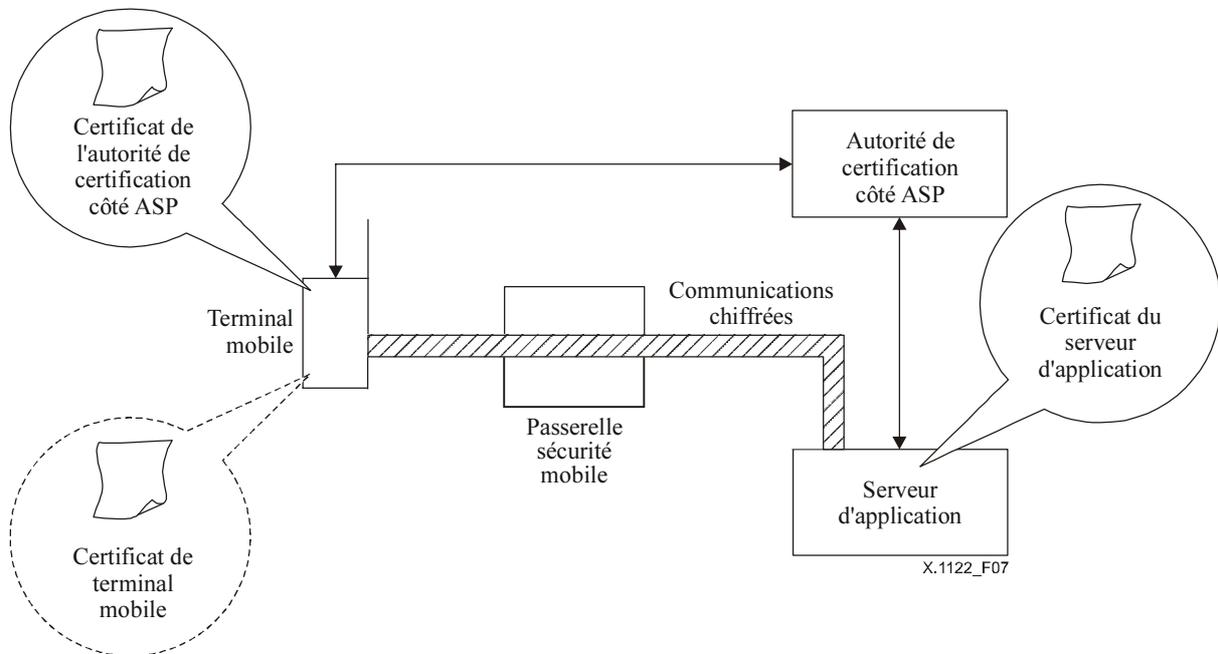


Figure 7/X.1122 – Chiffrement du trajet de communication dans le modèle d'utilisation par la couche Session

8.2 Modèle d'utilisation au niveau application

Il est possible d'utiliser l'infrastructure de clés publiques pour une fonction de chiffrement propre à une application, pour une fonction de signature numérique et pour une combinaison de l'une et l'autre, ce qui exige l'identification et la confidentialité des données proprement dites et ne peut être assuré uniquement par la sécurité sur le trajet de communication, notamment via authentification et chiffrement par la couche Session. Parmi les exemples d'implémentation de ce type de modèle figurent le chiffrement des courriers électroniques et les applications de création de compte dans le cadre du commerce électronique.

8.2.1 Fonction de signature au niveau application

Cette fonction garantit l'intégrité des données et crée une signature numérique sur le haché des données transmises à partir du terminal mobile afin de garantir qu'elles proviennent d'une personne signataire. La fonction de signature au niveau application comporte les opérations suivantes:

- introduction ou sélection des données à signer;
- traitement d'une signature numérique sur la valeur hachée des données au moyen de la clé privée enregistrée dans le terminal mobile ou dans le dispositif sécurisé associé au terminal mobile;
- présenter les données à signer, la signature numérique et le certificat contenant la clé publique correspondant à la clé privée;

- le destinataire vérifie la validité du certificat, il vérifie également la signature numérique au moyen de la clé publique contenue dans le certificat.

Cette fonction est applicable à une authentification de type demande et réponse, avec une demande (sous forme de nombre aléatoire) émise par le serveur, concernant les données à signer.

8.2.2 Fonction de chiffrement au niveau application

Le but est de fournir une fonction chiffrement au niveau application pour permettre une confidentialité sécurisée des données lorsque le chiffrement sur le trajet de communication n'est pas suffisant. La fonction de chiffrement au niveau application est réalisée par les opérations suivantes:

- production d'un nombre aléatoire utilisé comme clé commune;
- chiffrement des données avec la clé commune au moyen d'un algorithme de cryptographie symétrique;
- acquisition du certificat de la personne destinataire de la transmission;
- chiffrement de la clé commune au moyen de la clé publique contenue dans le certificat;
- envoi des données chiffrées et de la clé commune chiffrée;
- le destinataire déchiffre la clé commune chiffrée au moyen de sa propre clé privée;
- déchiffrement des données cryptées au moyen de la clé commune.

9 Exemples de configuration de système

9.1 Exemples de configuration de système de gestion de certificat

La Figure 8 illustre le cas d'un système dans lequel l'opérateur de communication émet un certificat destiné à son utilisateur. Le traitement hors ligne permet d'émettre ou d'annuler un certificat, la vérification du certificat incombant à l'autorité de vérification.

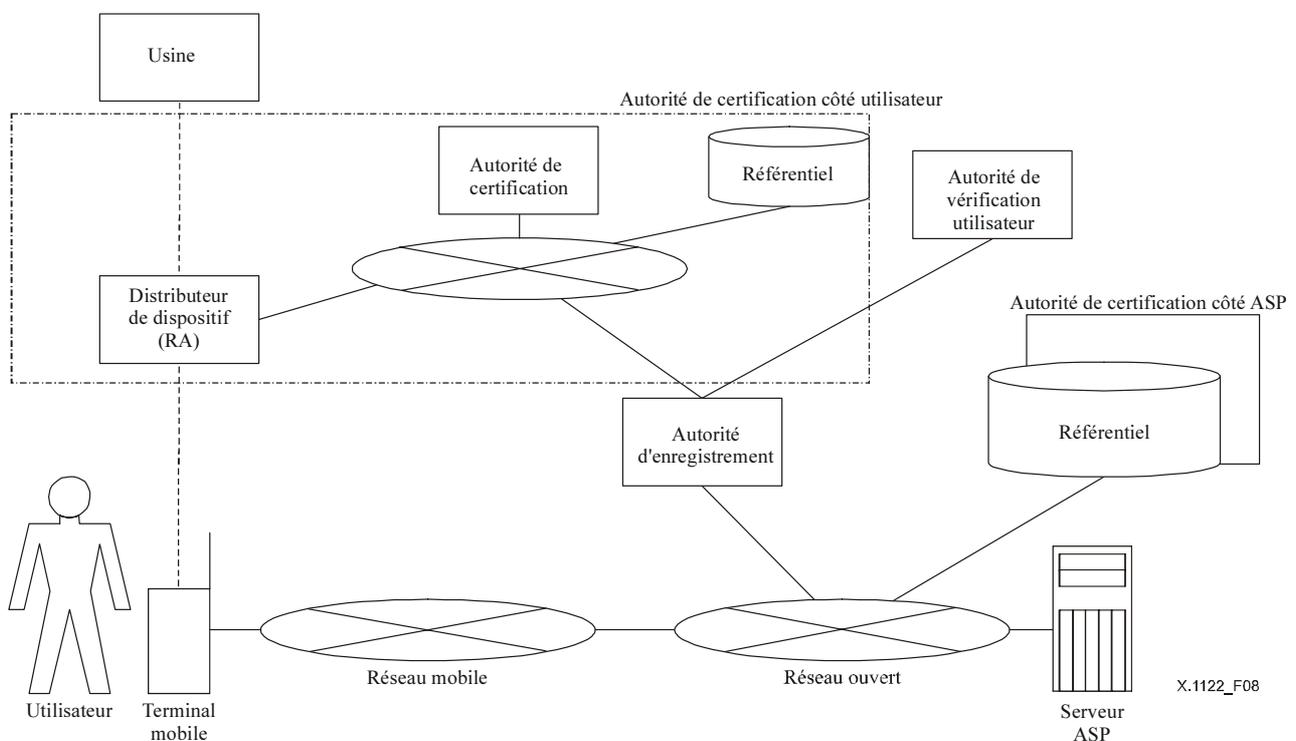


Figure 8/X.1122 – Exemple de système dans lequel l'opérateur de communication émet un certificat destiné à son utilisateur

9.1.1 Exemple d'émission de certificat

Deux exemples illustrent les conditions d'émission du certificat selon l'emplacement de génération de la clé: selon la première méthode, la clé est créée en usine, tandis que la deuxième méthode consiste à générer la clé dans le terminal mobile ou dans un jeton infraudable tel qu'un module d'identité utilisateur UIM, après acquisition du terminal mobile, lorsque le client souhaite émettre le certificat.

La preuve de la détention de la clé privée est particulièrement importante pour l'application du certificat. Le protocole de preuve de détention permet à une autorité de certification ou d'enregistrement de vérifier la validité du lien entre une entité d'extrémité et une paire de clés. Les autorités de certification/d'enregistrement sont tenues d'appliquer le certificat correspondant. Des preuves de détention spécifiques peuvent être apportées de différentes façons, selon le type de clé donnant lieu à une demande de certificat.

La Figure 9 présente un exemple de système dans lequel l'opérateur de communication émet un certificat à l'intention de son utilisateur. La clé est installée dans le dispositif à sa sortie d'usine. La demande de certificat est formulée au moment de l'achat du dispositif par l'utilisateur auprès du distributeur, lequel procède à l'installation dudit certificat. Cette opération intervient au moment de la fourniture de la preuve de détention (POP).

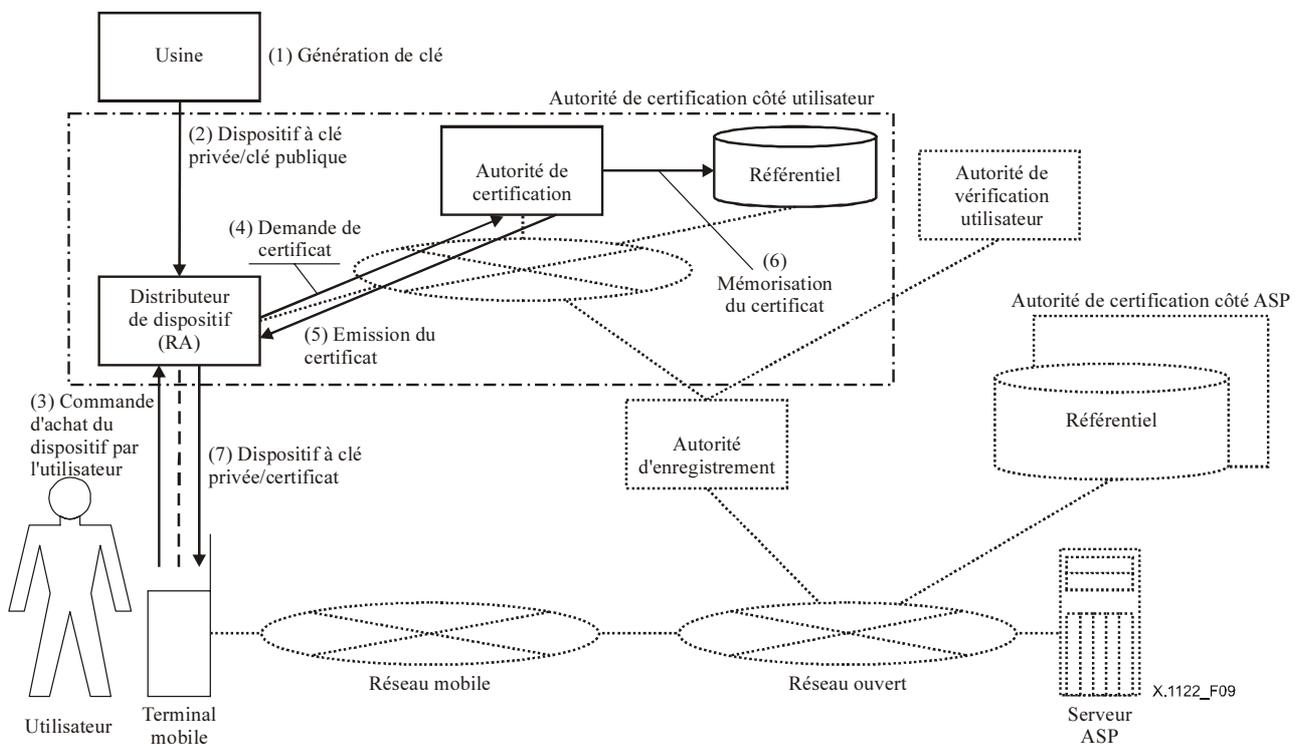


Figure 9/X.1122 – Exemple d'émission de certificat (1)

La Figure 10 donne un exemple de système dans lequel le client génère une clé et émet une demande de certificat. La demande de certificat est émise lorsque l'utilisateur souhaite l'obtenir de l'autorité de certification, le secret de la clé privée pouvant être conservé dans le terminal mobile. Avant l'exécution du protocole décrit ci-dessus, on suppose que le terminal mobile et l'autorité de certification partagent le secret commun de façon à assurer l'intégrité et l'authenticité du message échangé. Cette méthode permet de protéger le secret de la clé privée du terminal mobile.

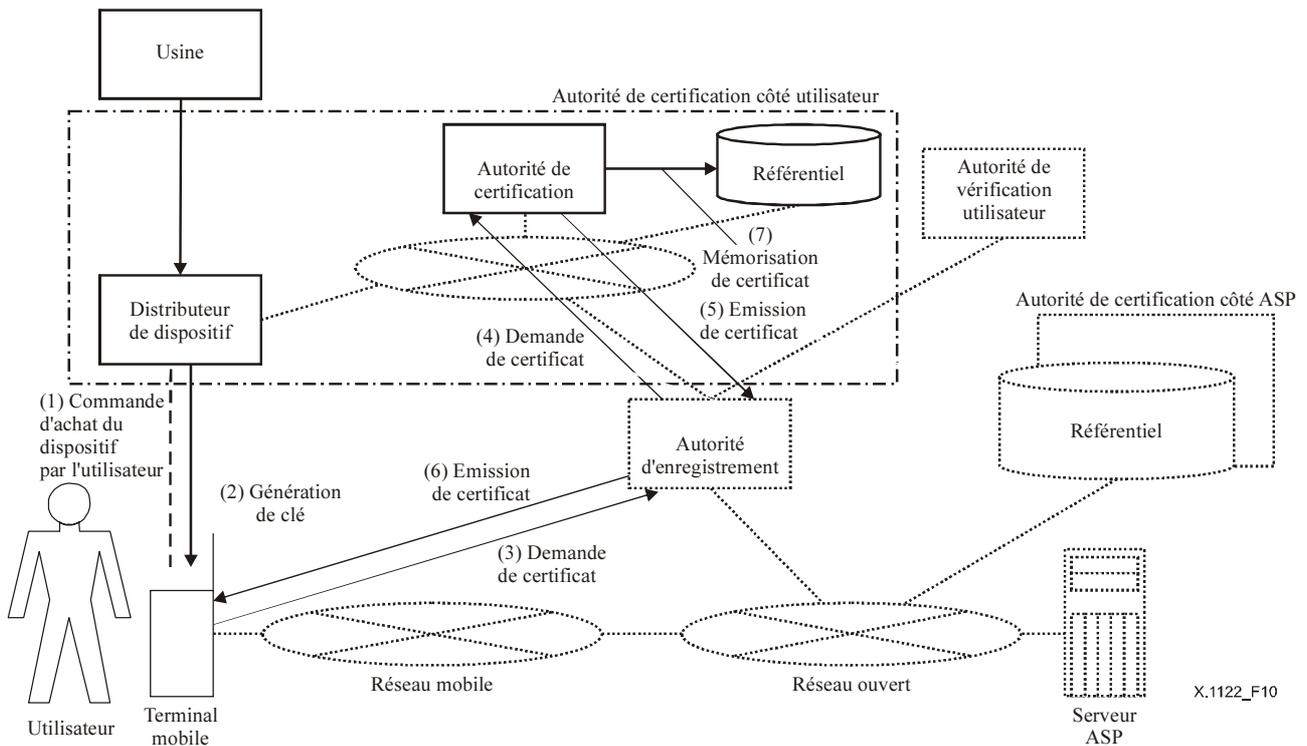


Figure 10/X.1122 – Exemple d'émission de certificat (2)

9.1.2 Exemple de vérification du certificat

En règle générale, le terminal mobile est doté d'une puissance de calcul et d'une capacité mémoire limitées, qui ne facilitent pas la mise en œuvre dans le terminal mobile du système de vérification du certificat basé sur la liste CRL. Aussi préfère-t-on utiliser l'autorité de vérification en ligne. La Figure 11 représente un exemple de vérification en ligne du certificat.

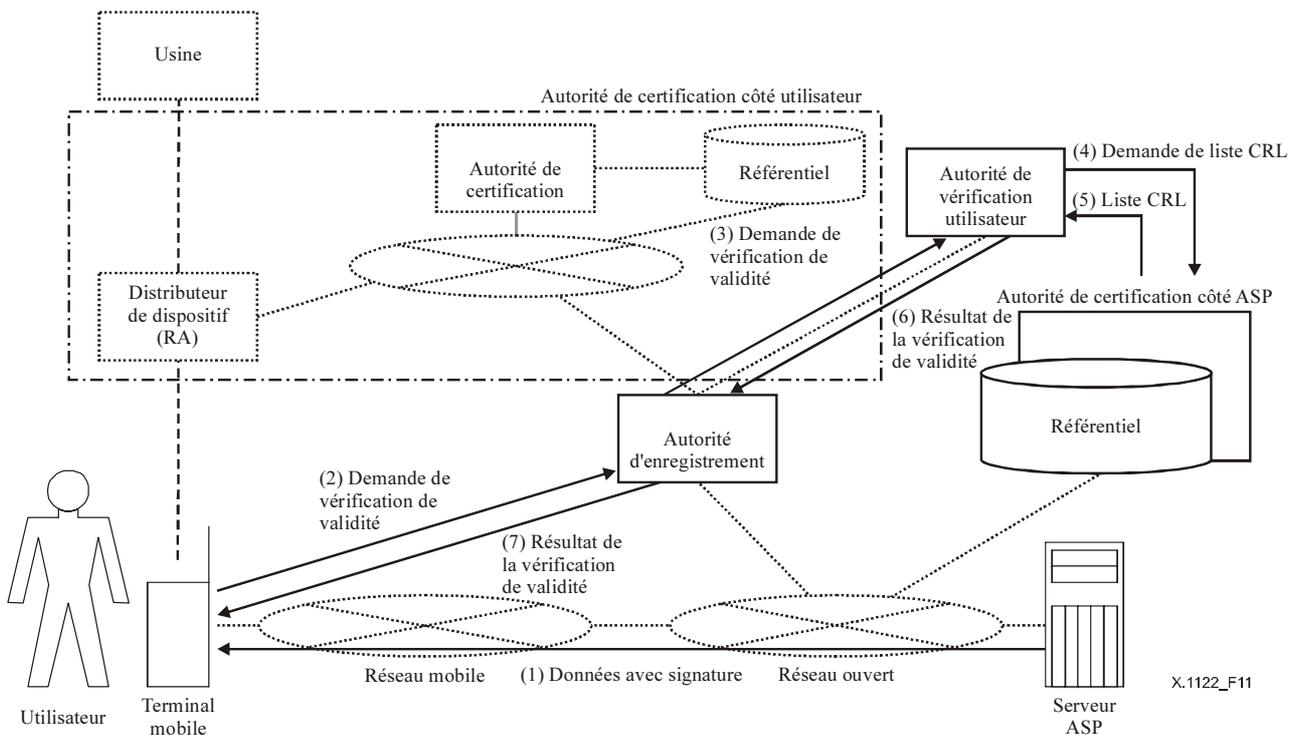


Figure 11/X.1122 – Exemple de vérification de certificat

9.2.1 Exemple de modèle d'authentification impliquant un utilisateur, un opérateur et un fournisseur de services d'application (ASP)

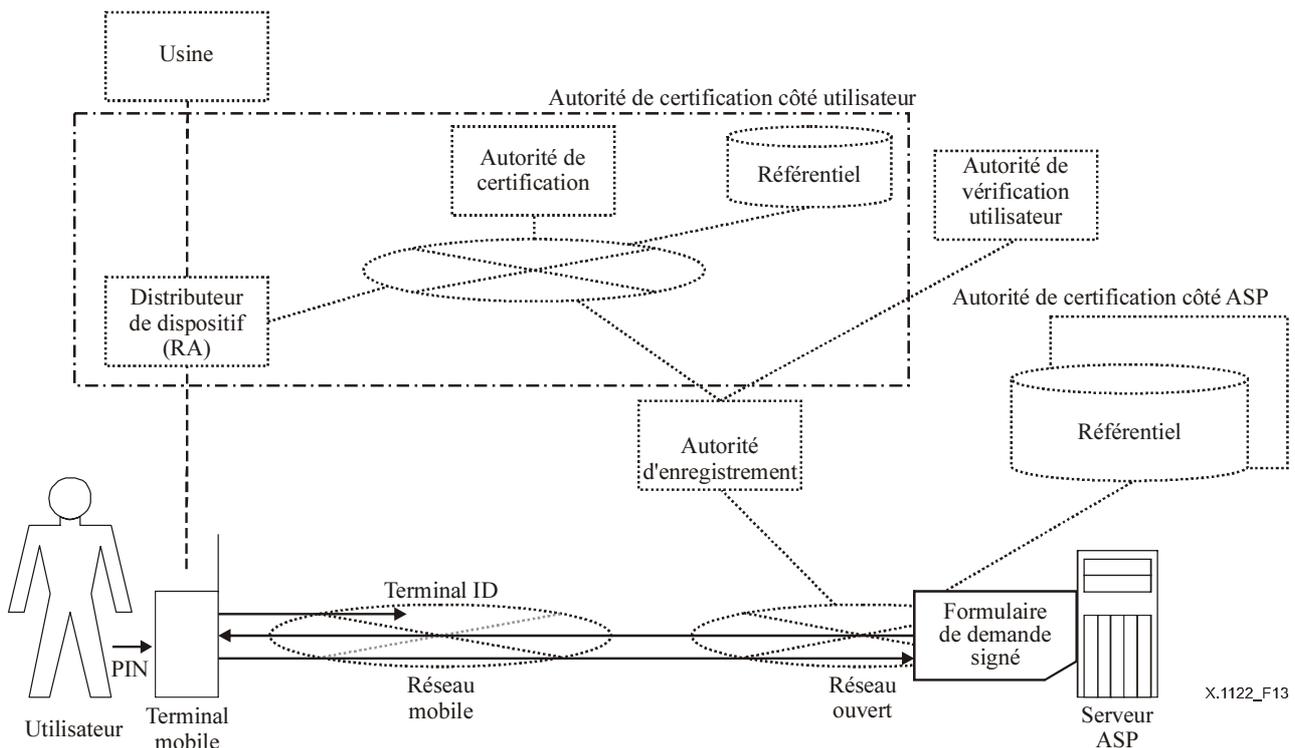


Figure 13/X.1122 – Exemple de modèle d'authentification impliquant un utilisateur, un opérateur et un fournisseur APS

9.2.1.1 Authentification d'un utilisateur de terminal mobile par l'opérateur

La présentation de l'identificateur du terminal mobile auprès de l'opérateur permet d'identifier l'utilisateur du terminal mobile en tant qu'abonné légitime.

9.2.1.2 Authentification du fournisseur ASP par l'utilisateur du terminal mobile

La vérification du certificat du fournisseur ASP permet de contrôler la fiabilité de ce dernier. A cet effet, l'utilisateur peut recevoir le certificat du fournisseur ASP proprement dit, ainsi que les données d'authentification correspondantes, telles que la signature numérique, le code d'authentification du message et les données chiffrées au moyen de la clé privée du fournisseur ASP de façon à la vérifier sur le terminal mobile de l'utilisateur. L'utilisateur peut également demander à l'autorité de vérification de vérifier le certificat reçu par l'intermédiaire de l'autorité d'enregistrement. Il peut par ailleurs spécifier l'adresse URL du certificat au lieu du certificat proprement dit. Afin d'authentifier le fournisseur ASP, l'utilisateur vérifie les données d'authentification appropriées au moyen de la clé publique correspondant à la clé publique contenue dans le certificat.

9.2.1.3 Authentification de l'utilisateur mobile par le terminal mobile (droit de l'utilisateur de carte)

Pour éviter l'usage illégitime d'un terminal mobile par un tiers – en particulier des données inscrites sur une puce (par exemple, un module d'identité utilisateur) et mémorisées sur un terminal mobile – il convient d'authentifier l'utilisateur par un numéro PIN. D'autres systèmes d'authentification de l'utilisateur, notamment par les empreintes digitales, pourraient être mis en œuvre.

De plus, il convient de prévoir un mécanisme de verrouillage pour interdire l'utilisation de la carte à puce en cas de perte ou de vol de l'appareil.

9.2.1.4 Authentification du terminal mobile (ou de l'utilisateur mobile) par le fournisseur ASP

L'utilisateur est certifié du côté ASP. Comme pour l'authentification de l'ASP par le terminal mobile, le fournisseur de service d'application peut recevoir le certificat du terminal mobile (ou celui de l'utilisateur mobile proprement dit), ainsi que les données d'authentification appropriées (par ex. signature numérique, code d'authentification des messages et données chiffrées au moyen de la clé privée de l'utilisateur), afin de les vérifier dans le cadre de l'ASP. L'ASP peut également demander à l'autorité de vérification de vérifier le certificat reçu. L'ASP peut en outre spécifier les informations de localisation du certificat au lieu du certificat proprement dit. A des fins d'authentification, l'ASP vérifie les données d'authentification appropriées au moyen de la clé publique correspondant à la clé publique contenue dans le certificat.

9.2.1.5 Légitimité de la demande

Pour déterminer si la demande provient effectivement du terminal mobile authentifié conformément au § 9.2.1.4, l'ASP vérifie la signature numérique associée à la demande. La fonction signature au niveau application peut alors être utilisée. La formule de demande peut également être chiffrée à des fins de protection du secret.

9.2.2 Exemple de modèle d'authentification utilisant une institution financière

On peut également faire appel à un modèle d'authentification utilisant les informations des cartes de crédit ou d'autres infrastructures existantes, voir Figure 14.

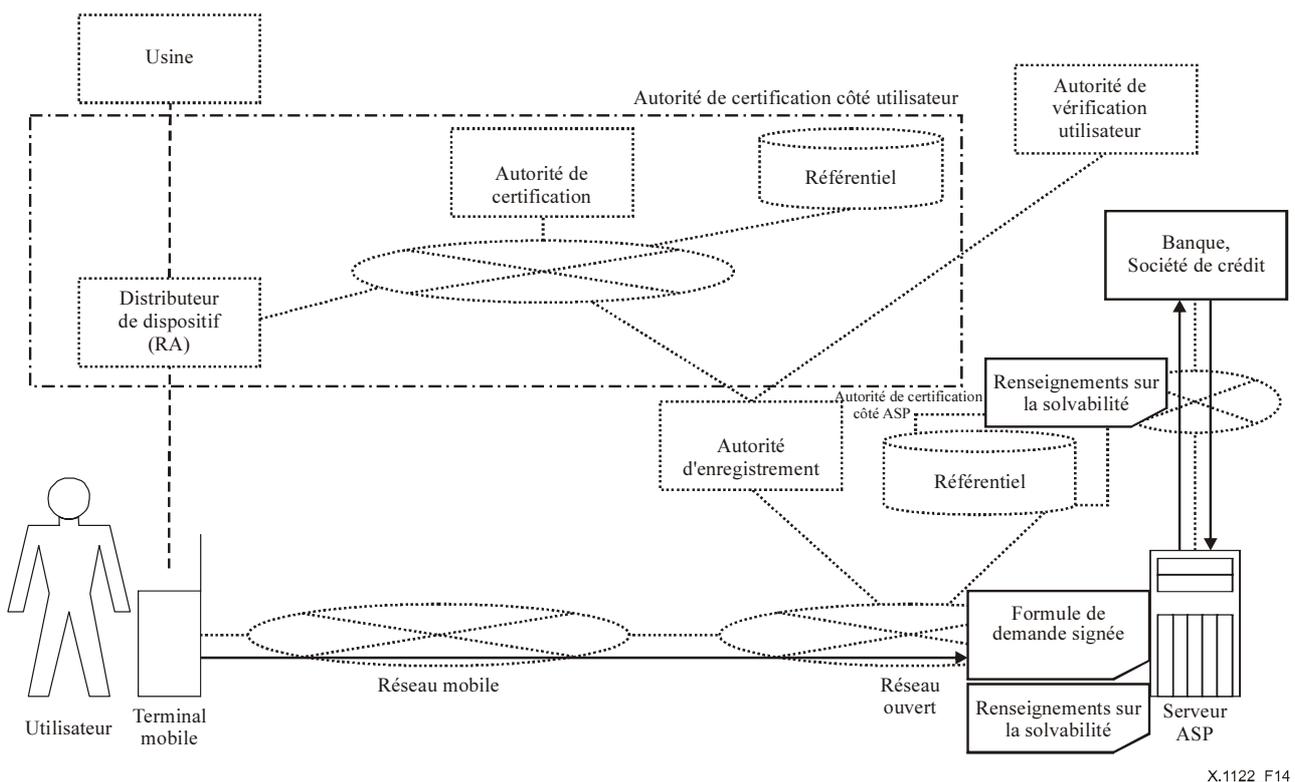


Figure 14/X.1122 – Exemple de modèle d'authentification utilisant une institution financière

9.2.2.1 Authentification de l'utilisateur par la banque ou la société émettrice de la carte de crédit

Une banque ou une société émettrice de cartes de crédit peut obtenir de l'utilisateur les informations financières (numéro de compte, numéro de carte de crédit, etc.) nécessaires à son authentification en tant que détenteur légitime de la carte.

Côté utilisateur, le numéro de carte de crédit et la date d'expiration sont déjà mémorisés sur la puce (module d'identification de l'utilisateur); aussi est-il inutile de les introduire lors de chaque authentification; une authentification de l'utilisateur au moyen du numéro PIN par exemple, est indispensable lorsque celui-ci sert à identifier sur le terminal mobile l'utilisateur légitime détenteur d'un droit d'accès aux données mémorisées.

Les informations financières peuvent également être implémentées sous forme de certificat d'attribut.

Lorsque des informations concernant des institutions financières sont transmises, elles doivent être chiffrées au moyen d'une clé de session aléatoire, elle-même chiffrée par la clé publique de l'institution financière sujet, mais non au moyen de la clé publique du fournisseur ASP.

Le résultat de la procédure d'authentification est renvoyé au fournisseur ASP par l'institution financière.

9.2.2.2 Authentification du fournisseur ASP par la banque ou la société émettrice de cartes de crédit

En cas d'utilisation d'un réseau ouvert au lieu d'un réseau de paiement existant, le fournisseur ASP doit être authentifié en tant que distributeur affilié, autorisé moyennant la présentation d'un certificat et des informations d'authentification appropriées à cet effet, établies par une banque ou une société émettrice de cartes de crédit.

9.2.2.3 Authentification du fournisseur ASP par l'utilisateur

Le fournisseur ASP doit être authentifié en tant que distributeur affilié, autorisé moyennant la présentation à l'utilisateur d'un certificat et des informations d'authentification appropriées à cet effet, établies par une banque ou une société émettrice de cartes de crédit. Par exemple, un certificat d'attribut, émis par une banque peut servir à certifier un distributeur autorisé.

10 Infrastructure de clés publiques pour communications mobiles de données de bout en bout

10.1 Interopérabilité avec le système existant

L'adaptation au service mobile du système existant fondé sur une infrastructure de clés publiques déjà créée avec le réseau ouvert, exige que les certificats relatifs au fournisseur ASP ou aux autres utilisateurs du réseau ouvert soient émis et utilisés dans (et derrière) l'ASP.

Dans ce type de cas, le terminal mobile doit pouvoir vérifier la validité des certificats existants.

En outre, si le format de certificat utilisé dans le service mobile est différent du format de certificat de l'ASP, les contraintes introduites par les capacités de débit ou de mémoire, imposent une modification du système actuel de l'ASP, pour que celui-ci puisse vérifier la validité des certificats des terminaux mobiles.

De plus, si le terminal mobile ne peut disposer d'une place suffisante pour mémoriser son certificat, il peut enregistrer l'URL du certificat au lieu du certificat proprement dit et envoyer cet URL au fournisseur ASP; celui-ci doit alors récupérer le certificat au moyen de son adresse URL.

A présent, les protocoles SSL/TLS sont largement utilisés en tant que protocoles de protection des messages (et comme protocoles d'authentification) pour les communications de données de bout en bout.

Toutefois, l'algorithme cryptographique et/ou le format de certificat utilisable pour le protocole TLS risquent de ne pas être adaptés aux capacités de traitement du terminal mobile.

Ainsi, dans les nombreux systèmes actuels qui utilisent l'infrastructure de clés publiques, l'algorithme cryptographique RSA est largement utilisé comme algorithme de signature. Toutefois, l'algorithme cryptographique RSA demande parfois une puissance de calcul supérieure à celle du terminal mobile. Dans ces conditions on préfère utiliser un algorithme cryptographique exigeant une puissance moindre ou réduite, par exemple un algorithme basé sur les courbes elliptiques. Grâce à sa rapidité supérieure à celle de l'algorithme RSA, cet algorithme permet au terminal mobile de réaliser le traitement dans un délai approprié. Toutefois l'algorithme cryptographique basé sur les courbes elliptiques n'a pas encore été adapté aux spécifications des protocoles TLS, etc.; de plus, la longueur du code de hachage risque alors de dépasser celle de la clé, ce qui peut exiger un traitement cryptographique en plusieurs étapes.

Bien que l'approche à suivre pour résoudre le problème ci-dessus consiste à introduire l'autorité de vérification, afin de vérifier une signature, il convient de s'interroger par ailleurs sur la façon de protéger les communications entre le terminal mobile et l'autorité de vérification.

La rapidité de l'algorithme cryptographique à clé commune étant nettement supérieure à celle de l'algorithme cryptographique à clés publiques, cette solution ne risque pas de poser de problème, même en cas d'adaptation au terminal mobile.

De plus, puisque les protocoles SSL/TLS échangent leurs certificats au stade de l'initialisation, il peut en résulter la nécessité d'une zone d'enregistrement mémoire supérieure à celle du terminal mobile.

Tel qu'indiqué précédemment, une méthode permettant d'adapter un protocole au moyen d'une passerelle de sécurité mobile a été proposée; toutefois, entre le fournisseur ASP et l'utilisateur il peut s'avérer nécessaire de faire appel au protocole d'authentification employé au niveau d'une couche supérieure.

10.2 Utilisation de l'infrastructure de clés publiques dans le service mobile

10.2.1 Génération de clé

10.2.1.1 Générateur de clé

En cas d'adoption d'un modèle dans lequel l'utilisateur génère une paire de clés, bien que la présence d'une fonction génération de clé soit requise à l'intérieur d'un appareil (c'est-à-dire un modèle qui génère la clé à l'intérieur de l'appareil, en tant que lieu de génération de la clé), la capacité de mémoire et la puissance de calcul risquent de poser des problèmes au niveau du terminal mobile.

Si l'on adopte un modèle dans lequel l'autorité de certification ou un tiers génère une paire de clés, il faut tenir compte de considérations pratiques et prévoir un mécanisme empêchant de compromettre la validité de la clé.

10.2.1.2 Localisation de génération de la clé

Pour des raisons de sécurité, il y a intérêt à localiser la génération d'une clé privée à l'intérieur d'un appareil; la puissance de traitement risque alors de poser un autre problème.

Si l'on adopte un modèle comportant l'installation dans l'appareil d'une clé générée à l'extérieur, il faut prévoir un mécanisme propre à éviter que la validité de la clé soit compromise.

10.2.1.3 Localisation du stockage de la clé/du certificat

En règle générale personne ne peut extraire une clé privée de l'appareil. La clé privée doit être mémorisée dans la zone protégée. Il existe deux types de zone protégée:

- zone protégée physiquement: la clé privée est enregistrée dans la zone protégée physiquement, par exemple la mémoire morte du terminal mobile ou des dispositifs externes (par ex. cartes à puce);
- zone protégée par logiciel: la clé privée est enregistrée dans la zone protégée par logiciel à l'intérieur du terminal mobile.

Il est à noter que la zone protégée par logiciel doit être une zone sécurisée, de telle sorte que seul un utilisateur légitime peut réenregistrer ou accéder à la clé privée grâce à un contrôle d'accès et/ou une protection cryptographique. Le système de chiffrement par mot de passe permet généralement d'assurer la protection cryptographique de ce type d'information.

De plus, la clé publique de l'utilisateur (certificat) ainsi que le certificat de l'autorité de certification racine sont enregistrés dans la zone protégée de l'appareil, selon l'option retenue de préférence.

10.2.2 Demande et émission de certificat

10.2.2.1 Cas de préinstallation du certificat dans l'appareil

Pour les modèles dans lesquels l'utilisateur du mobile achète le dispositif avec un certificat préinstallé, la mise à jour de la clé et du certificat présente des difficultés.

De plus, quand le certificat n'est pas associé à l'utilisateur mobile, il faut parfois, selon l'utilisation, émettre un certificat d'attribut décrivant le lien entre le certificat et l'utilisateur du mobile.

10.2.2.2 Cas de préinstallation de la clé dans l'appareil

Compte tenu de la difficulté de mettre à jour la clé, l'appareil est mis au rebut lorsque le certificat est annulé.

10.2.3 Utilisation du certificat

10.2.3.1 Cas de signature numérique du terminal mobile

Avec le protocole TLS, la méthode liant les certificats (tous les certificats depuis le certificat de l'autorité de certification racine jusqu'au certificat du signataire) au message est adoptée en tant que méthode d'association du certificat de l'autorité de certification racine au certificat du signataire.

Toutefois, si tous les certificats, depuis le certificat de l'autorité de certification racine jusqu'à celui du signataire, sont associés, il peut en résulter en cas d'association de la signature, une charge importante en raison de contraintes telles que la capacité de mémoire du terminal mobile.

Bien que la technique consistant à associer au message une adresse URL indiquant l'emplacement de stockage du certificat, celle-ci n'est pas encore prise en charge par le protocole TLS.

10.2.3.2 Cas de vérification de la signature par le terminal mobile

Les modèles comportant la vérification de la validité du certificat par le vérificateur lui-même risquent de ne pas convenir au service mobile en raison des nombreuses contraintes de puissance de calcul et de capacité de mémoire.

Pour les modèles basés sur l'utilisation d'une autorité de vérification, l'application utilisatrice du certificat doit connaître l'autorité de vérification dont elle dépend; de plus, lors des communications avec l'autorité de vérification, elle doit être en mesure de vérifier la validité de cette autorité.

Dans l'exemple indiqué au § 9.1.2, le terminal mobile accède à l'autorité de vérification par l'intermédiaire de l'autorité d'enregistrement. Dans ce cas, le terminal mobile doit être doté d'une fonction permettant de reconnaître à l'avance l'autorité d'enregistrement (RA) dont il dépend et

d'une fonction permettant de certifier (authentifier) l'exactitude des communications de l'autorité d'enregistrement RA avec l'autorité de vérification VA. Quant à l'autorité d'enregistrement RA, elle doit être dotée d'une fonction permettant de déterminer l'autorité de vérification VA dont dépend le terminal mobile, et d'une fonction permettant de certifier la validité de l'autorité de vérification avec laquelle elle communique.

10.2.4 Réflexions concernant l'autorité de certification

Les systèmes actuels qui utilisent une infrastructure de clés publiques établissent des relations fiables entre différents domaines de certification par la création d'une hiérarchie comportant plusieurs autorités de certification et par la définition de certifications croisées.

Toutefois, le contrôle de la validité des certificats de chaque autorité CA à des fins de vérification de la signature, risque de se heurter au problème de la puissance de calcul du terminal mobile.

Si l'on ne fait pas appel à une autorité de vérification, il y a intérêt à établir une structure simple d'autorités de certification.

10.3 Généralités concernant l'infrastructure de clés publiques

10.3.1 Génération de clé

10.3.1.1 Générateur de clé

Les modèles dans lesquels l'utilisateur génère les clés, permettent à un utilisateur quelconque de chercher à obtenir les clés des autres utilisateurs en recherchant les certificats correspondant à la clé publique générée, en prétendant être le propriétaire de ce certificat.

Par conséquent, avec les modèles dans lesquels l'utilisateur génère les clés, il faut adopter une clé d'une longueur suffisante compte tenu du nombre d'utilisateurs présumés.

De plus, il peut s'avérer nécessaire de mettre en œuvre certains systèmes afin de rendre plus difficile l'acquisition des certificats des autres utilisateurs.

10.3.2 Demande/émission/activation des certificats

10.3.2.1 Procédures obligatoires d'activation du certificat

Lorsque l'utilisateur suit explicitement la procédure d'activation du certificat, il faut prévoir le mécanisme qui détermine la nécessité de la procédure suivie par l'utilisateur lui-même.

Lorsqu'un certificat est activé en ligne, l'utilisateur signe les données de demande d'activation et les transmet à l'autorité d'enregistrement, etc. Lorsqu'il procède hors ligne, il est possible d'utiliser un mécanisme identique à celui de l'utilisation d'une carte de crédit (notamment appel d'un opérateur afin de demander l'activation du certificat).

10.3.2.2 Demande de certificat en ligne

Il faut alors un mécanisme propre à assurer l'intégrité et l'authenticité des communications au cours de la demande. De fait, il faut assurer la vérification par l'autorité de certification, la vérification du demandeur, la protection de l'itinéraire de communication, etc.

10.3.3 Révocation du certificat

L'adoption d'un modèle autorisant la révocation en ligne, exige la mise en œuvre d'un mécanisme propre à vérifier que le demandeur est bien l'utilisateur. En particulier, la révocation d'un certificat en raison de la perte d'une clé privée, ne peut reposer sur l'identification du demandeur par une signature numérique. Il faut donc prévoir une autre méthode (par exemple par un numéro PIN).

L'adoption d'un modèle comportant une possibilité de révocation hors ligne, peut exiger la mise en œuvre du mécanisme permettant de suspendre un certificat en ligne.

10.3.4 Renouvellement des certificats

Outre les problèmes de demande et de révocation de certificat, il importe de trouver – uniquement du point de vue de la disponibilité du système – une solution pour éviter l'oubli de la mise à jour du certificat.

10.3.5 Problèmes liés à la description du certificat

Les informations contenues dans un certificat doivent être soigneusement examinées; en effet la diffusion d'un certificat risque d'être nettement supérieure à celle envisagée par l'émetteur.

Appendice I

Exemples de modèles de service

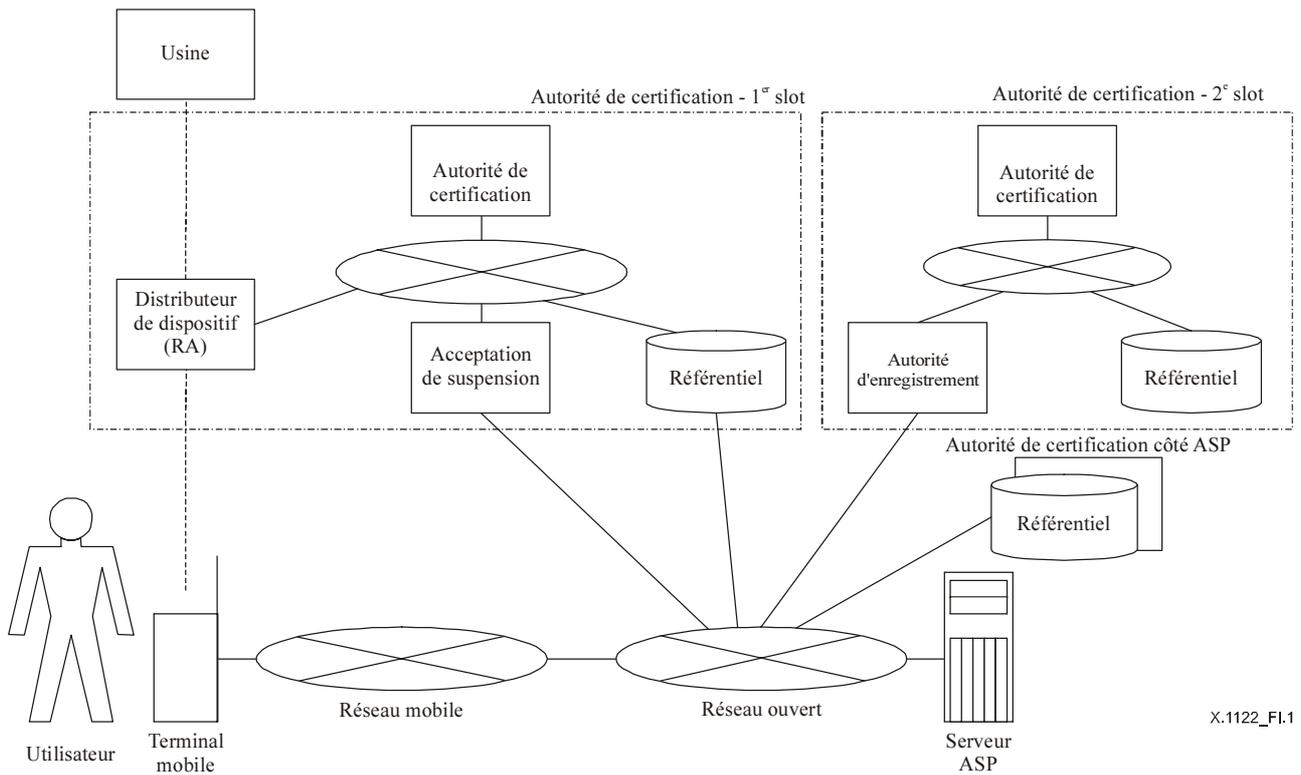
Le présent appendice décrit les modèles de service de l'infrastructure de clés publiques appliqués aux services mobiles.

I.1 Modèles de service de gestion de certificat

Le paragraphe 9 donne un exemple d'utilisation hors ligne du système, dans lequel un opérateur de télécommunication émet des certificats. Le présent appendice décrit différents modèles de service de gestion des certificats.

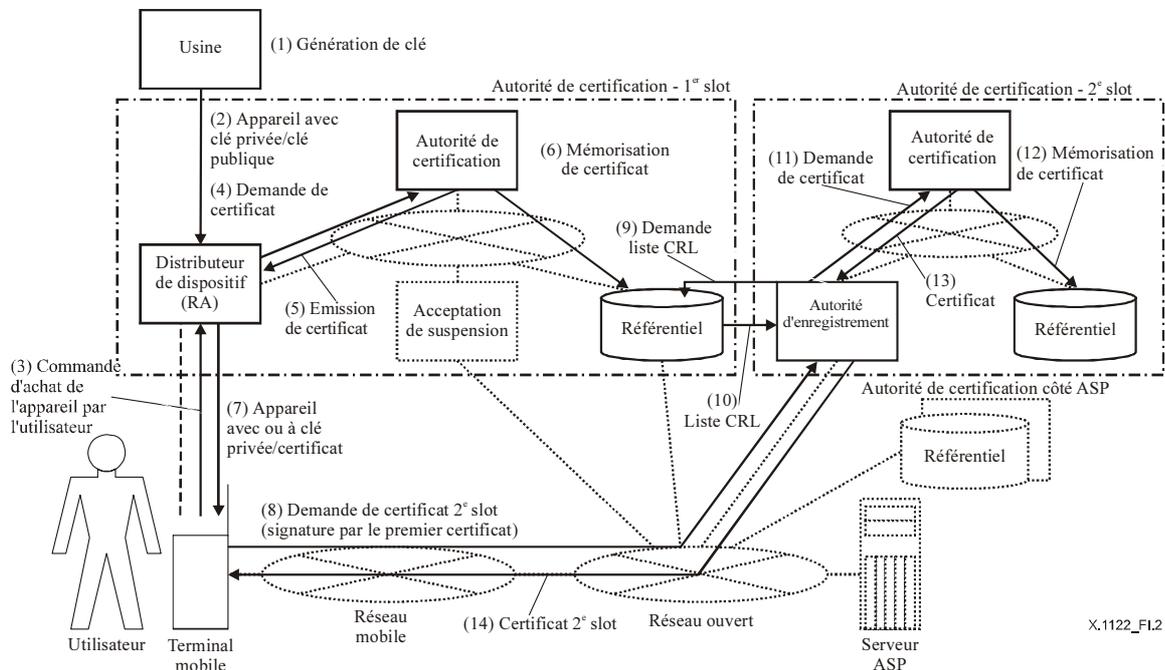
I.1.1 Exemple de système dans lequel un fournisseur ASP émet des certificats

Dans les exemples décrits dans les Figures I.1 et I.2, on distingue deux types de certificats; le premier certificat est fourni par l'autorité de certification du premier slot (voir Figure I.1) associée à un opérateur et chargée de fournir le certificat au terminal mobile pour les transports de données en session sécurisée; le deuxième certificat est fourni par l'autorité de certification du deuxième slot (voir Figure I.2) associée au fournisseur ASP et chargée de fournir au terminal mobile le certificat à utiliser pour les différentes applications. Un fournisseur ASP utilise un certificat CA émis par un opérateur de communication et de façon à pouvoir émettre son propre certificat. Afin d'émettre/révoque un certificat, le système côté opérateur (autorité de certification 1^{er} slot) utilise un traitement hors ligne, tandis que le système côté fournisseur ASP (autorité de certification 2^e slot) utilise un traitement en ligne. Cependant, pour la demande de certificat, le système du côté fournisseur ASP (autorité CA 2^e slot) utilise un certificat émis par l'opérateur (autorité CA 1^{er} slot) afin de protéger l'itinéraire de communication et d'authentifier le demandeur, puis accepte la demande en ligne.



X.1122_FI.1

Figure I.1/X.1122 – Exemple de système dans lequel un fournisseur ASP émet les certificats



X.1122_FI.2

Figure I.2/X.1122 – Exemple d'émission de certificat 2^e slot

Afin d'annuler un certificat émis par une autorité de certification de 2^e slot, l'utilisateur accède par ailleurs à l'autorité d'enregistrement par l'intermédiaire du réseau et suit la procédure de révocation.

I.1.2 Exemple de système comportant l'utilisation d'un certificat d'attribut

Dans cet exemple (voir Figure I.3) on suppose que le fournisseur ASP utilisateur du certificat émis par un opérateur de communication pour identifier un demandeur, etc., utilise par ailleurs un certificat d'attribut dans le but par exemple de réaliser un contrôle d'accès plus complexe. Lorsque l'émission d'un certificat d'attribut à l'intention d'un utilisateur fait appel à une autorité en charge des attributs, l'émission d'un certificat à l'intention d'un utilisateur incombe à une autorité de certification utilisateur.

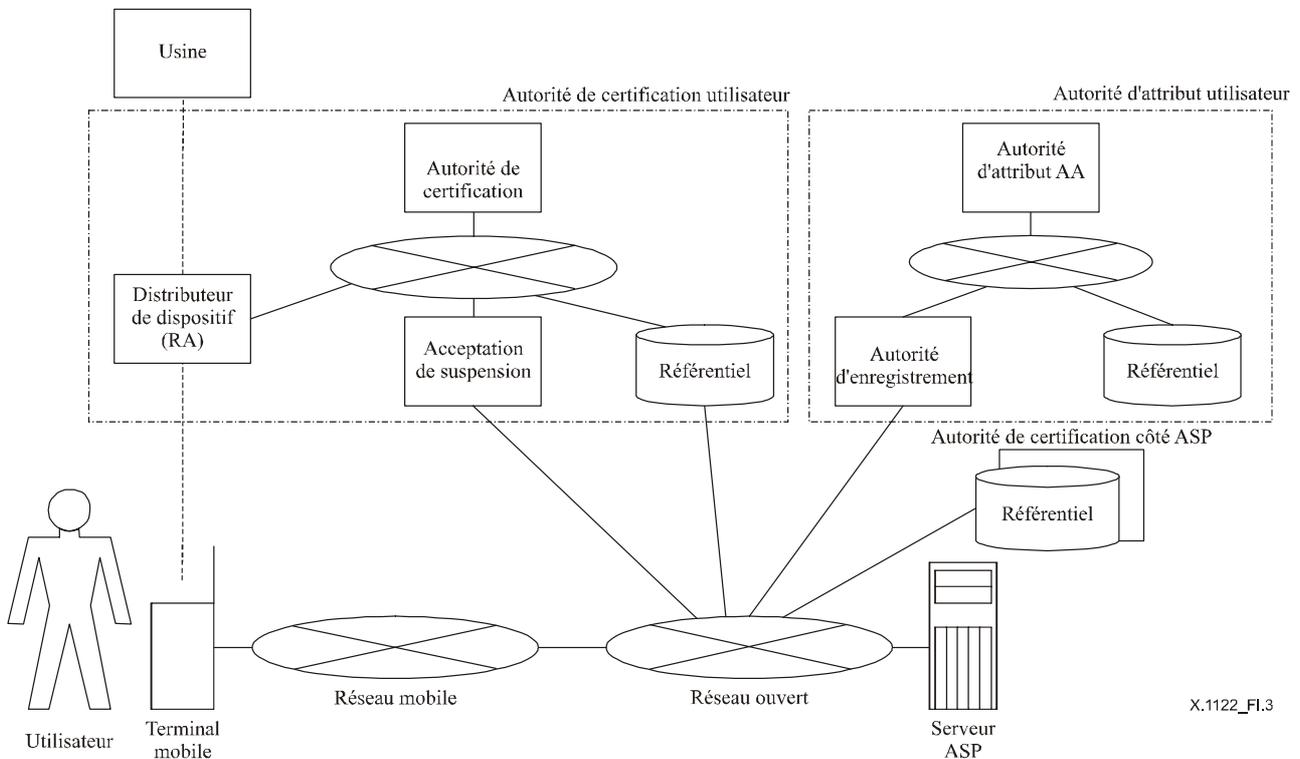


Figure I.3/X.1122 – Exemple de système comportant l'utilisation d'un certificat d'attribut

Côté opérateur (autorité de certification utilisateur) le système repose sur un traitement hors ligne pour l'émission et la révocation des certificats, et sur une autorité de vérification pour leur vérification.

Côté fournisseur ASP (autorité en charge des attributs utilisateur) le système accepte la demande en ligne d'un utilisateur, génère ensuite un certificat d'attribut en fonction des règles de demande en vigueur, puis l'associe au certificat émis par l'opérateur. Le certificat d'attribut est enregistré dans le référentiel de l'autorité en charge des attributs. (On peut également envisager un modèle dans lequel un certificat d'attribut est transmis à un utilisateur.)

Lorsqu'un fournisseur ASP reçoit des données comportant la signature de son utilisateur, il saisit dans un premier temps la liste CRL dans le référentiel de l'autorité de certification côté opérateur afin de vérifier la validité du certificat. (Le magasin vérifie en outre la signature sur les données transmises depuis l'utilisateur.) Ensuite, le fournisseur ASP acquiert un certificat d'attribut provenant de l'autorité en charge des attributs côté fournisseur ASP pour vérifier si l'utilisateur est habilité à utiliser le service, voir la Figure I.4.

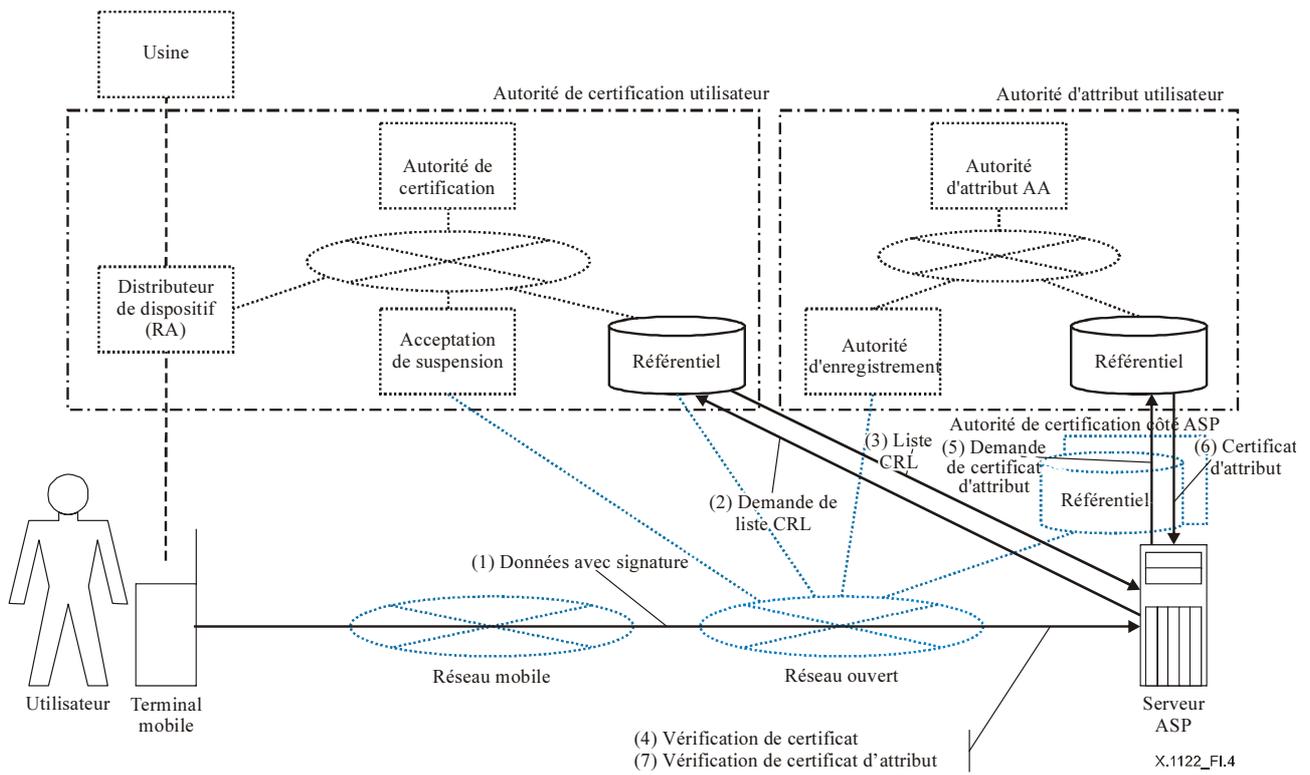


Figure I.4/X.1122 – Exemple de modèle d'authentification reposant sur des certificats d'attribut

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
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	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
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
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 et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de nouvelle génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication