

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1035

(02/2007)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION
ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité des télécommunications

**Protocole d'échange de clés avec
authentification par mot de passe**

Recommandation UIT-T X.1035

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

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.379
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.889
Applications génériques de l'ASN.1	X.890–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.1035

Protocole d'échange de clés avec authentification par mot de passe

Résumé

La Recommandation UIT-T X.1035 contient un protocole qui permet une authentification mutuelle de deux parties lorsque celles-ci élaborent une clé de chiffrement symétrique via un échange de Diffie-Hellman. Le recours à l'échange de Diffie-Hellman garantit la *confidentialité totale vers l'avant* (propriété d'un protocole de création de clés qui garantit que la compromission d'une clé de session ou d'une clé privée de longue durée après une session donnée n'entraîne pas la compromission d'une session antérieure). Avec la méthode d'authentification proposée, l'échange est protégé contre "*l'attaque de l'intercepteur*". Cette authentification repose sur un secret partagé au préalable (par exemple, un mot de passe), qui est protégé (c'est-à-dire qui n'est pas révélé à un intrus), ce qui écarte le risque d'attaque "par dictionnaire" hors connexion. Ce protocole peut donc être utilisé pour des applications très diverses associées à des secrets partagés au préalable reposant sur un mot de passe qui peut être faible.

Source

La Recommandation UIT-T X.1035 a été approuvée le 13 février 2007 par la Commission d'études 17 (2005-2008) 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 développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2007

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	Définitions 1
4	Abréviations et acronymes 1
5	Conventions 1
6	Description du protocole..... 2
7	Considérations relatives à la sécurité..... 3
	Bibliographie..... 5

Introduction

Il est bien connu que, bien qu'il assure la *confidentialité totale vers l'avant*, l'échange de clés de *Diffie-Hellman* est exposé à l'attaque *de l'intercepteur*. Plusieurs méthodes permettent de limiter ces attaques. Certaines reposent sur le chiffrement de clés publiques, tandis que d'autres sont fondées sur des secrets partagés (mots de passe). La présente Recommandation contient un protocole de ce second type.

En particulier, la méthode d'authentification proposée permet de protéger l'échange contre l'attaque *de l'intercepteur*. L'authentification repose sur un secret potentiellement faible partagé au préalable qui est caché (c'est-à-dire, qui n'est pas révélé) à un intrus, ce qui écarte le risque d'attaque par dictionnaire hors connexion. Ce protocole peut donc être utilisé pour des applications très diverses pour lesquelles des secrets partagés au préalable (par exemple des mots de passe) sont utilisés.

Le protocole d'échange de clés avec authentification par mot de passe présente les avantages suivants:

- assure un échange de clés fortes avec des mots de passe faibles;
- permet de déjouer les attaques de l'intercepteur;
- permet une authentification mutuelle explicite;
- garantit la confidentialité totale vers l'avant.

Les documents énumérés dans la bibliographie contiennent des informations supplémentaires sur ce protocole.

Recommandation UIT-T X.1035

Protocole d'échange de clés avec authentification par mot de passe

1 Domaine d'application

La présente Recommandation décrit le protocole d'échange de clés avec authentification par mot de passe qui respecte les prescriptions suivantes:

- permet une authentification mutuelle sur la base d'un mot de passe partagé au préalable;
- assure une protection contre l'attaque de l'intercepteur et l'attaque par dictionnaire hors connexion.

La présente Recommandation contient également des lignes directrices concernant le choix des paramètres pour l'échange de clés de Diffie-Hellman.

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 de Recommandation.

[TIA 683-D] Norme TIA-683-D (2006), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

3 Définitions

Aucune.

4 Abréviations et acronymes

La présente recommandation utilise les abréviations et acronymes suivants:

PAK	échange de clés avec authentification par mot de passe (<i>password-authenticated key exchange</i>)
PW	mot de passe (<i>password</i>)
SHA	algorithme de hachage sécurisé (<i>secure hash algorithm</i>)
WLAN	réseau régional radioélectrique (<i>wireless local area network</i>)

5 Conventions

Les conventions ci-après sont utilisées dans la présente Recommandation:

- $a \bmod b$ désigne le plus petit reste non négatif lorsque a est divisé par b ;
- $H_i(u)$ désigne une fonction de hachage convenue (par exemple, basée sur l'algorithme de hachage sécurisé n° 1 *SHA-1*) calculée sur une chaîne u , où $i = 1, 2, 3, \dots$ les différentes fonctions $H_i()$ se comportent comme des fonctions aléatoires indépendantes. Il est recommandé d'utiliser des fonctions aléatoires différentes dans le protocole d'échange de clés avec authentification par mot de passe afin d'accroître la sécurité de celui-ci;

- $s|t$ désigne la concaténation des chaînes s et t .

6 Description du protocole

Pour la concordance de clés de Diffie-Hellman, l'expéditeur et le destinataire d'un message doivent créer leurs propres nombres aléatoires secrets et échanger leurs nombres respectifs élevés à une certaine puissance. En élevant la valeur échangée à la puissance correspondant à leurs nombres aléatoires secrets, les deux parties peuvent calculer la même clé de Diffie-Hellman secrète partagée.

Dans le cadre du protocole d'échange de clés avec authentification par mot de passe, deux parties, A et B , communiquent et partagent un mot de passe secret PW . On choisit les constantes globales de Diffie-Hellman connues de tous, un nombre premier p et un générateur g en prenant garde que les conditions suivantes soient respectées:

- 1) pour être *sûr*, un nombre premier p doit être suffisamment grand pour qu'il soit impossible de calculer le logarithme discret;
- 2) les puissances de g modulo p couvrent tous les $p-1$ entiers compris entre 1 et $p-1$.

Au départ, A choisit un exposant secret R_A et calcule $g^{R_A} \bmod p$; B choisit un exposant secret R_B et calcule $g^{R_B} \bmod p$. Par souci d'efficacité, des exposants courts pourraient être utilisés pour R_A et R_B , sous réserve qu'ils aient une longueur minimale donnée. Dans les étapes qui suivent, toutes les opérations de multiplication devraient se faire avec mod p , de sorte que toutes les valeurs échangées entre les parties qui communiquent ne soient pas supérieures à p . Par conséquent, toutes les opérations de division devraient elles aussi être effectuées avec mod p .

Ensuite

- 1) A entame l'échange en choisissant un exposant R_A aléatoire et en envoyant la grandeur $X = H_1(A|B|PW) \cdot (g^{R_A} \bmod p)$ à B ;
- 2) Lorsqu'il reçoit cette grandeur, B vérifie que X n'est pas égale à zéro puis la divise par $H_1(A|B|PW)$ afin de retrouver $g^{R_A} \bmod p$. B choisit ensuite un exposant R_B aléatoire et calcule $S_1 = H_3(A|B|PW | \frac{X}{H_1(A|B|PW)} | g^{R_B} \bmod p | \left\{ \left(\frac{X}{H_1(A|B|PW)} \right)^{R_B} \bmod p \right\})$ et $Y = H_2(A|B|PW) \cdot (g^{R_B} \bmod p)$. B envoie à A un message contenant les deux grandeurs S_1 et Y .
- 3) Lorsqu'il a reçu ce message et après avoir vérifié que Y n'est pas égale à zéro, A peut authentifier B en retrouvant ce que devrait être $g^{R_B} \bmod p$ et en calculant S_1 lui-même. Si le résultat est égal à la valeur reçue, A calcule la clé $K = H_5(A|B|PW | g^{R_A} \bmod p | \frac{Y}{H_2(A|B|PW)} | \left\{ \left(\frac{Y}{H_2(A|B|PW)} \right)^{R_A} \bmod p \right\})$. Pour s'authentifier et achever l'échange, A calcule également la grandeur $S_2 = H_4(A|B|PW | g^{R_A} \bmod p | \frac{Y}{H_2(A|B|PW)} | \left\{ \left(\frac{Y}{H_2(A|B|PW)} \right)^{R_A} \bmod p \right\})$ et l'envoi à B .

- 4) B authentifie A en calculant S_2 lui-même et en comparant la valeur à celle reçue de A . Si ces deux valeurs sont identiques, B calcule lui aussi la clé

$$K = H_5(A | B | PW | \frac{X}{H_1(A | B | PW)} | g^{R_B} \text{ mod } p | \left\{ \left(\frac{X}{H_1(A | B | PW)} \right)^{R_B} \text{ mod } p \right\}).$$

Si l'une des vérifications mentionnées ci-dessus ne donne pas le résultat escompté, le protocole s'arrête. Sinon, les deux parties se sont mutuellement authentifiées et ont créé la clé.

Les étapes indiquées ci-dessus sont récapitulées dans la Figure 1, où P désigne $A|B|PW$ ($P = A|B|PW$) et où certaines formules ont été simplifiées.

Partie A		Partie B
$X = H_1(P) \cdot (g^{R_A} \text{ mod } p)$	\xrightarrow{X}	Vérifier que la valeur reçue n'est pas égale à 0 $\frac{H_1(P) \cdot (g^{R_A} \text{ mod } p)}{H_1(P)} = g^{R_A} \text{ mod } p$
$S_1 = H_3(P g^{R_A} \text{ mod } p g^{R_B} \text{ mod } p g^{R_A R_B} \text{ mod } p)$ Calcule S_1 et vérifie qu'elle est égale à la valeur reçue de B pour S_1	$\xleftarrow{S_1, Y}$	$S_1 = H_3(P g^{R_A} \text{ mod } p g^{R_B} \text{ mod } p g^{R_A R_B} \text{ mod } p)$ $Y = H_2(P) \cdot (g^{R_B} \text{ mod } p)$
$S_2 = H_4(P g^{R_A} \text{ mod } p g^{R_B} \text{ mod } p g^{R_A R_B} \text{ mod } p)$	$\xrightarrow{S_2}$	$S_2 = H_4(P g^{R_A} \text{ mod } p g^{R_B} \text{ mod } p g^{R_A R_B} \text{ mod } p)$ Calcule S_2 et vérifie qu'elle est égale à la valeur reçue de A pour S_2
$K = H_5(P g^{R_A} \text{ mod } p g^{R_B} \text{ mod } p g^{R_A R_B} \text{ mod } p)$		$K = H_5(P g^{R_A} \text{ mod } p g^{R_B} \text{ mod } p g^{R_A R_B} \text{ mod } p)$

Figure 1 – Description du protocole d'échange de clés avec authentification par mot de passe

7 Considérations relatives à la sécurité

Le présent paragraphe porte sur les aspects liés à la sécurité du protocole d'échange de clés avec authentification par mot de passe. En particulier, il contient des lignes directrices concernant le choix des paramètres de Diffie-Hellman.

Seules les valeurs des paramètres p et g convenues au préalable devraient être utilisées dans le cadre du protocole d'échange de clés avec authentification par mot de passe. Cette précaution est nécessaire pour se prémunir contre un intrus qui enverrait des valeurs p et g erronées et tromperait ainsi l'autre partie avec une élévation à la mauvaise puissance pour l'échange Diffie-Hellman. L'utilisation de paramètres p et g qui ne sont pas conformes aux prescriptions décrites dans la présente Recommandation risque d'entraîner la compromission du mot de passe. La norme [TIA-683-D] contient une valeur de 1024 bits adaptée pour p et une valeur appropriée pour g .

En outre, si l'on utilise des exposants courts pour les paramètres R_A et R_B de Diffie-Hellman, alors la longueur de ces exposants devrait être d'au moins 384 bits (si l'on part de l'hypothèse que des clés de session de 128 bits sont utilisées), comme le spécifie également la norme [TIA-683-D].

Les fonctions aléatoires indépendantes H_1 et H_2 devraient donner des résultats de 1152 bits chacun, si l'on part de l'hypothèse que le nombre premier p mesure 1024 bits et que la longueur des clés de session K est de 128 bits. Les fonctions aléatoires H_3 , H_4 , et H_5 devraient donner des résultats de 128 bits.

EXEMPLE: l'utilisation de la fonction de hachage SHA-1 contenue dans [b-FIPS 180-2] pourrait être recommandée pour l'instanciation des fonctions aléatoires $H_i()$ telles qu'elle est décrite dans [b-TIA 1050]. Il conviendrait cependant de noter que le National Institute of Standards and Technology (NIST) encourage l'utilisation de l'algorithme SHA-256 comme étant une solution plus sûre que l'algorithme SHA-1.

Bibliographie

- [b-TIA 1050] TIA 1050-100, Project Number 3-0174-000, *Wireless Local Area Network (WLAN) Interworking*.
- [b-FIPS 180-2] NIST Federal Information Processing Standards, Publication FIPS 180-2 (2002), *Secure Hash Standard*.
- [b-EUROCRYPT] BOYKO (V.), MACKENZIE (P.), PATEL (S.): Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman, EUROCRYPT 2000.
- [b-IEEE P1363.2] IEEE P1363.2 (Sept. 2006), *Standard Specifications for Password-Based Public-Key Cryptographic Techniques*.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
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	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
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 et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication