Groupe de travail Réseau
Request for Comments : 4683
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

J. Park, KISA
J. Lee, KISA
H. Lee, KISA
S. Park, BCQRE
T. Polk, NIST
septembre 2006

Méthode d'identification de sujet (SIM) d'infrastructure de clé publique X.509 sur Internet

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Protocoles officiels de l'Internet" (STD 1) pour voir l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent document définit la méthode d'identification de sujet (SIM, *Subject Identification Method*) pour inclure un identifiant sensible à la confidentialité dans l'extension subjectAltName *(nom de remplacement du sujet)* d'un certificat. La SIM est une caractéristique facultative qui peut être utilisée par les consommateurs d'assertions pour déterminer si le sujet d'un certain certificat est aussi la personne correspondant à un certain identifiant sensible.

Table des matières

1. Introduction

Une autorité de certification (CA, *Certification Authority*) produit des certificats de clé publique X.509 pour lier une clé publique à un sujet. Le sujet est spécifié par un ou plusieurs noms de sujet dans les champs "subject" ou "subjectAltName" d'un certificat. Le champ "subject" contient un nom distinctif structuré hiérarchiquement. Le champ "subjectAltName" peut contenir une adresse de messagerie électronique, une adresse IP, ou d'autres formes de nom qui correspondent au sujet.

Pour chaque CA particulière, un nom de sujet correspond à une personne, appareil, groupe, ou rôle unique. La CA ne va pas sciemment produire des certificats à plusieurs entités sous le même nom de sujet. C'est-à-dire, pour un producteur de certificat particulier, tous les certificats actuellement valides qui affirment le même nom de sujet sont liés à la même entité.

Lorsque le sujet est une personne, le nom qui est spécifié dans le champ Sujet du certificat peut refléter le nom des entités individuelles et affiliées (par exemple, leur appartenance à une entreprise). En réalité, il y a cependant des individus ou entreprises qui ont le même nom ou des noms similaires. Il peut être difficile à un consommateur d'assertions (par exemple, une personne ou application) d'associer le certificat à une personne ou organisation spécifique sur la seule base du nom de sujet. Cette ambiguïté pose un problème à de nombreuses applications.

Dans certains cas, les applications ou les consommateurs d'assertions ont besoin de s'assurer que le sujet des certificats produits par des CA différentes sont en fait la même entité. Cette exigence peut être satisfaite en incluant un "identifiant permanent" dans tous les certificats produits au même sujet, qui est unique à travers plusieurs CA. En comparant l'identifiant permanent, le consommateur d'assertions peut identifier les certificats provenant des différentes CA qui sont liées au même sujet. Cette solution est définie dans la [RFC4043].

Dans de nombreux cas, l'identifiant d'une personne ou entreprise (par exemple, un numéro de sécurité sociale) est considéré comme une donnée sensible, privée, ou personnelle. Un tel identifiant ne peut pas simplement être inclus au titre du champ Sujet, car sa divulgation peut amener des abus. Donc, les identifiants sensibles à la confidentialité de cette sorte ne devraient pas être inclus dans les certificats sous forme de texte en clair.

Par ailleurs, un tel identifiant n'est en fait pas un secret. Les gens choisissent de divulguer ces identifiants pour certaines classes de transactions. Par exemple, une personne peut divulguer un numéro de sécurité sociale pour ouvrir un compte en banque ou obtenir un prêt. Ceci est normalement corroboré par la présentation d'accréditifs physiques (par exemple, un permis de conduire) qui confirme le nom ou l'adresse de la personne.

Pour prendre en charge de telles applications dans un environnement en ligne, les consommateurs d'assertions ont besoin de déterminer si le sujet d'un certificat particulier est aussi la personne qui correspond à un identifiant sensible particulier. Idéalement, les applications se serviraient des accréditifs électroniques des demandeurs (par exemple, le certificat de clé publique X.509) pour corroborer cet identifiant, mais le champ Sujet d'un certificat ne fournit souvent pas des informations suffisantes.

Pour répondre à ces demandes, la présente spécification définit la méthode d'identification de sujet (SIM, *Subject Identification Method*) et le format d'informations de sujet protégées à confidentialité améliorée (PEPSI, *Privacy-Enhanced Protected Subject Information*) pour inclure un identifiant sensible à la confidentialité dans un certificat. Bien que d'autres solutions pour lier des identifiants sensibles à la confidentialité à un certificat pourraient être développées, la méthode spécifiée dans le présent document a des propriétés particulièrement attrayantes. La présente spécification étend les pratiques et mécanismes courants de PKI pour permettre d'inclure aussi des identifiants sensibles à la confidentialité dans le certificat. Le mécanisme de SIM permet aussi au sujet de contrôler l'exposition de l'identifiant sensible ; quand le sujet choisit d'exposer l'identifiant sensible, les consommateurs d'assertions peuvent vérifier le lien. Précisément :

(1) Une infrastructure de clé publique (PKI, *Public Key Infrastructure*) dépend d'un tiers de confiance – la CA – pour lier une ou plusieurs identités à une clé publique. Les mises en œuvre traditionnelles de PKI lient les noms distinctifs X.501 à la clé publique, mais l'identité peut aussi être spécifiée en termes d'adresses de la RFC 822 ou de noms du DNS. La spécification de SIM permet que le même tiers de confiance – la CA – qui lie un nom à la clé publique inclut aussi un identifiant sensible à la confidentialité dans le certificat. Comme le consommateur d'assertions fait déjà confiance à la CA pour produire les certificats, c'est une simple extension pour couvrir aussi la vérification et le lien d'un identifiant sensible. Ce lien pourrait être établi séparément, par un autre tiers de confiance, mais cela compliquerait l'infrastructure.

(2) La présente spécification s'appuie sur les extensions standard à PKI pour atteindre de nouveaux objectifs fonctionnels avec un minimum de nouveau code. La présente spécification code l'identifiant sensible dans le champ otherName dans l'extension de nom de sujet de remplacement. Comme le champ otherName est largement utilisé, cette solution utilise un champ de certificat qui est souvent rempli et traité. (Par exemple, les mises en œuvre de connexion par une carte à

mémoire reposent généralement sur des noms codés dans ce champ.) Alors que les mises en œuvre de la présente spécification vont exiger du code spécifique de SIM, un format de remplacement augmenterait le coût sans améliorer la sécurité. De plus, cela n'a pas d'impact sur les mises en œuvre qui ne traitent pas les identifiants sensibles.

(3) En liant explicitement la clé publique à l'identifiant, la présente spécification permet au consommateur d'assertions de confirmer l'identifiant du prétendant et de confirmer que le prétendant est le sujet de cet identifiant. C'est-à-dire, la preuve de possession de la clé privée confirme que le prétendant est bien la personne dont l'identité a été confirmée par la PKI (CA ou RA) selon l'architecture).

Pour atteindre le même but dans un message séparé (par exemple, un objet signé et chiffré S/MIME) le message devrait être lié au certificat ou à une identité dans le certificat (par exemple, le nom distinctif X.501). La première solution est problématique, car les certificats expirent. La dernière solution peut causer des problèmes si les noms sont réutilisés dans l'infrastructure. Un lien explicite dans le certificat est une solution plus simple et plus fiable.

(4) La présente spécification permet au sujet de l'identifiant sensible à la confidentialité de contrôler la distribution et le niveau de sécurité appliqué à l'identifiant. L'identifiant n'est divulgué que quand le sujet choisit de le divulguer, même si le certificat est posté dans un répertoire public. En choisissant un mot de passe fort, le sujet peut s'assurer que l'identifiant est protégé contre des attaques en force brute. La présente spécification permet aux sujets de divulguer de façon sélective un identifiant lorsque ils l'estiment approprié, ce qui est cohérent avec l'utilisation courante de tels identifiants.

(5) Les certificats qui contiennent un identifiant sensible peuvent quand même être utilisés pour prendre en charge d'autres applications. Une partie qui obtient un certificat contenant un identifiant sensible, mais dont le sujet ne choisit pas de divulguer l'identifiant, doit effectuer une attaque en force brute pour obtenir l'identifiant. En choisissant un algorithme de hachage fort, cette attaque devient infaisable par le calcul. De plus, quand les certificats incluent des identifiants sensibles à la confidentialité comme décrit dans la présente spécification, chaque certificat doit être attaqué séparément. Finalement, les sujets peuvent utiliser ce mécanisme pour prouver qu'ils possèdent un certificat contenant un type particulier d'identifiant sans en fait le divulguer au consommateur d'assertions.

Cette caractéristique DOIT n'être utilisée qu'en conjonction avec des protocoles qui utilisent des signatures numériques générées en utilisant la clé privée du sujet.

De plus, le présent document définit un PEPSI chiffré (EPEPSI, *Encrypted PEPSI*) de sorte que les informations d'identifiant sensibles peuvent être échangées durant le processus de production de certificat sans divulguer l'identifiant à un espion.

Le présent document est organisé comme suit :
- la Section 3 établit les exigences de sécurité et d'utilisation ;
- la Section 4 donne une vue d'ensemble du mécanisme ;
- la Section 5 définit la syntaxe et les règles de génération ;
- la Section 6 donne des exemples de cas d'utilisation.

1.1 Mots clés

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Symboles

Les symboles cryptographiques suivants sont définis dans ce document :

H() : algorithme de hachage cryptographiquement sûr. SHA-1 [FIPS 180-1] ou une fonction de hachage plus sûre est exigé.

SII *(Sensitive Identification Information)* : informations d'identification sensibles (par exemple, numéro de sécurité sociale).

SIItype : identifiant d'objet qui identifie le type de SII.

P : un mot de passe choisi par l'utilisateur.

R : valeur de nombre aléatoire généré par une autorité d'enregistrement (RA, *Registration Authority*).

PEPSI *(Privacy-Enhanced Protected Subject Information)* : informations de sujet protégées à confidentialité améliorée. Calculé à partir de la valeur d'entrée de P, R, SIItype, SII en utilisant deux itération de H().

E() : algorithme de chiffrement pour chiffrer la valeur de PEPSI.

EPEPSI *(Encrypted PEPSI)* : PEPSI chiffré.

D() : algorithme de déchiffrement pour déchiffrer le EPEPSI.

3. Exigences

3.1 Exigences de sécurité

On fait les hypothèses suivantes sur le contexte dans lequel SIM et PEPSI sont à employer :
- Alice, détentrice d'un certificat, avec un identifiant sensible SIIa (comme son numéro de sécurité sociale)
- Bob, un consommateur d'assertions qui va demander à connaître le SIIa d'Alice
- Eve, un attaquant qui acquiert le certificat d'Alice
- Un RA à qui Alice doit divulguer son SIIa
- Une CA qui va produire le certificat d'Alice

On souhaite dessiner une SIM et un PEPSI, en utilisant un mot de passe choisi par Alice, qui ait les propriétés suivantes :
- Alice peut prouver son SII, SIIa à Bob.
- Eve a un gros facteur de travail pour déterminer le SII d'Alice à partir du certificat d'Alice, même si Alice choisit un mot des passe faible, et un très gros facteur de travail si Alice choisit un bon mot de passe.
- Même si Eve peut déterminer le SIIa, elle a un problème tout aussi dur pour trouver toutes les autres valeurs de SII à partir de tout autre PEPSI ; c'est-à-dire, il n'y a rien qu'elle puisse pré calculer qui aide son attaque des PEPSI dans d'autres certificats, et rien qu'elle apprenne d'une attaque réussie qui l'aide dans toute autre attaque.
- La CA n'apprend pas le SIIa d'Alice sauf dans le cas où la CA a besoin de valider le SII passé par la RA.
- La CA peut traiter la SIM comme une forme supplémentaire de nom dans l'extension "subjectAltName" sans traitement particulier.
- Alice ne peut pas trouver un autre SII (SIIx), et un mot de passe (P), qui lui permettrait d'utiliser son certificat pour affirmer un faux SII.

3.2 Exigences d'utilisation

En plus des propriétés de sécurité déclarées ci-dessus, on a les exigences d'utilisation suivantes :

- Quand SIM et PEPSI sont utilisées, tout traitement personnalisé se fait chez le consommateur d'assertions. Alice peut utiliser un logiciel du commerce (par exemple, un navigateur standard) sans modification, en conjonction avec un certificat contenant une valeur de SIM.

3.3 Solution

On définit SIM comme R || PEPSI, où PEPSI = H(H(P || R || SIItype || SII))

Les étapes suivantes décrivent la construction et l'utilisation de SIM :
1. Alice prend un mot de passe P, et donne P, SIItype, et SII à la RA (via un canal sûr).
2. La RA valide le SIItype et le SII ; c'est-à-dire, elle détermine que la valeur de SII est correctement associée au sujet et que le SIItype est correct.
3. La RA génère une valeur aléatoire de R.
4. La RA génère la SIM = (R || PEPSI) où PEPSI = H(H(P || R || SIItype || SII)).
5. La RA envoie la SIM à Alice par un moyen hors bande et la passe aussi à la CA.
6. Alice envoie une certRequest *(demande de certificat)* à la CA. La CA génère le certificat d'Alice en incluant la SIM comme une forme de otherName à partir de la structure GeneralName dans l'extension subjectAltName.

7. Alice envoie à Bob son certificat, ainsi que P, SIItype, et SII. Ces dernières valeurs doivent être communiquées via un canal de communication sûr, pour préserver leur confidentialité.
8. Bob peut calculer PEPSI' = H(H(P || R || SIItype || SII)) et comparer SIM' = R || PEPSI' à la valeur de SIM dans le certificat d'Alice, vérifiant par là le SII.

Si la valeur du SII d'Alice n'est pas exigée par Bob (Bob sait déjà le SII d'Alice et n'en a pas besoin) alors les étapes 7 et 8 sont comme suit :
7. Alice envoie à Bob son certificat et P. P doit être envoyé via un canal de communication sûr, pour préserver sa confidentialité.
8. Bob peut calculer PEPSI' = H(H(P || R || SIItype || SII)) et comparer SIM' = R || PEPSI' à la valeur dans la SIM, vérifiant par là le SII.

Si Alice souhaite prouver qu'elle est le sujet d'un identifiant validé par la RA, sans divulguer son identifiant à Bob, alors les étapes 7 et 8 sont comme suit :
7. Alice envoie la valeur intermédiaire H(P || R || SIItype || SII) et son certificat à Bob.
8. Bob peut obtenir R du SIM dans le certificat, puis calculer H (valeur intermédiaire) et le comparer à la valeur dans la SIM, vérifiant par là que Alice connaît P et SII.

Eve a à faire une recherche exhaustive de l'espace H(P || R || SIItype || SII) pour trouver le SII d'Alice. C'est un problème très difficile même si Alice utilise un mot de passe faible, à cause de la taille de R (comme spécifié plus loin) et un problème réellement très dur si Alice utilise un très bon mot de passe (voir la Section 8).

Même si Eve trouve les P et SII d'Alice, ou construit un dictionnaire massif des valeurs de P et SII, cela ne l'aide pas à trouver d'autres valeurs de SII, parce qu'un nouveau R est utilisé pour chaque PEPSI et SIM.

4. Procédures

4.1 SII et SIItype

L'utilisateur présente la preuve qu'un SII particulier lui a été alloué. Le SIItype est un identifiant d'objet (OID) qui définit le format et la portée de la valeur de SII. Par exemple, en Corée, un SIItype est défini comme suit :

```
-- Arc spécifique KISA
IDENTIFIANT D'OBJET id-KISA ::= {iso(1) member-body(2) korea(410) kisa(200004)}

-- OID spécifiques de KISA
IDENTIFIANT D'OBJET id-npki ::= {id-KISA 10}
IDENTIFIANT D'OBJET id-attribute ::= {id-npki 1}
IDENTIFIANT D'OBJET id-kisa-identifyData ::= {id-attribute 1}
IDENTIFIANT D'OBJET id-VID ::= {id-kisa-identifyData 10}
IDENTIFIANT D'OBJET id-SII ::= {id-VID 1}
```

Pour des communautés fermées, la valeur SIItype peut être allouée par la CA elle-même, mais il est quand même recommandé que l'OID soit enregistré.

4.2. Mot de passe choisi par l'utilisateur

L'utilisateur choisit un mot de passe comme une des valeurs d'entrées du calcul due SIM. La force du mot de passe est critique pour la protection du SII de l'utilisateur, de la façon suivante. Si un attaquant a une valeur de SII candidate, et veut déterminer si la valeur de SIM dans un certificat de sujet spécifique, P, est la seule protection pour la SIM. L'utilisateur devrait être encouragé à choisir des mots de passe qui vont être difficiles à deviner, et assez longs pour protéger contre les attaques en force brute.

Les mises en œuvre de la présente spécification DOIVENT permettre à un utilisateur de choisir des mots de passe jusqu'à 28 caractères. Les RA DEVRAIENT mettre en œuvre des règles de filtre de mot de passe pour empêcher le choix par l'utilisateur de mots de passe triviaux. Voir dans [FIPS 112] et [FIPS 180-1] les critères de sécurité pour les mots de passe et un algorithme de génération automatique de mot de passe qui peut créer de façon aléatoire des syllabes simples prononçables comme mots de passe.

4.3 Génération de nombre aléatoire

La RA génère un nombre aléatoire, R. Un nouveau R DOIT être généré pour chaque SIM. La longueur de R DOIT être la même que la longueur du résultat de l'algorithme de hachage H. Par exemple, si H est SHA-1, le nombre aléatoire DOIT être de 160 bits.

Un générateur de nombres aléatoires (RNG, *Random Number Generator*) qui satisfait les exigences définies dans [FIPS 140-2] et son utilisation sont fortement recommandés.

4.4 Génération de SIM

La SIM dans l'extension subjectAltName au sein d'un certificat identifie une entité, même si plusieurs subjectAltNames apparaissent dans un certificat. Les RA DOIVENT calculer la valeur de SIM avec les entrées désignées selon l'algorithme suivant :

SIM = R || PEPSI
où PEPSI = H(H(P || R || SIItype || SII))

Le SII est porté à la connaissance d'une RA au moment de l'adhésion de l'utilisateur. SHA-1 et SHA-256 DOIVENT tous deux être pris en charge pour la génération et la vérification des valeurs de PEPSI. La présente spécification n'empêche pas l'utilisation d'autres fonctions unilatérales de hachage, mais SHA-1 ou SHA-256 DEVRAIT être utilisé chaque fois que l'interopérabilité est en cause.

Noter qu'un canal de communication sûr DOIT être utilisé pour passer P et SII de l'entité d'extrémité à la RA, pour les protéger de la divulgation ou la modification.

La syntaxe et l'OID associé pour SIM sont aussi fournis dans les modules ASN.1 au paragraphe 5.1. Le paragraphe 5.2 décrit aussi la syntaxe de PEPSI dans les modules ASN.1.

4.5 Chiffrement de PEPSI

Il peut être exigé que la CA (pas seulement la RA) vérifie le SII avant de produire un certificat. Pour satisfaire cette exigence, la RA DEVRAIT chiffrer les SIItype, SII, et SIM et envoyer le résultat à la CA par un canal sûr. L'utilisateur DEVRAIT aussi chiffrer les mêmes valeurs et envoyer le résultat à la CA dans son message de demande de certificat. Alors, la CA compare ces deux résultats pour vérifier le SII de l'utilisateur.

Si le résultat de la RA et de l'utilisateur sont le EPEPSI. EPEPSI = E(SIItype || SII || SIM)

Quand le EPEPSI est utilisé dans une demande de certificat d'utilisateur, il est dans les regInfo des [RFC4211] et [RFC2986].

Note : des méthodes spécifiques de chiffrement/déchiffrement ne sont pas définies dans ce document. Pour la transmission de la valeur de PEPSI d'un utilisateur à la CA, le protocole de demande de certificat employé définit comment le chiffrement est effectué. Pour la transmission de ces données entre une RA et une CA, les détails de la façon d'effectuer le chiffrement sont une affaire locale.

La syntaxe et l'IOD associé pour EPEPSI sont fournis dans les modules ASN.1 au paragraphe 5.3.

4.6 Demande de certification

Comme décrit ci-dessus, un message de demande de certificat PEUT contenir la SIM. La [RFC2986] et la [RFC4211] sont des syntaxes de message largement utilisées pour les demandes de certificat.

Fondamentalement, un message PKCS n° 10 consiste en un nom distinctif, une clé publique, et un ensemble facultatif d'attributs, collectivement signés par l'entité d'extrémité. Le nom de remplacement de SIM DOIT être placé dans l'extension subjectAltName si ce format de demande de certificat est utilisé. Si une CA vérifie le SII avant de produire le certificat, la valeur de SIM dans la demande de certification DOIT être portée dans la forme EPEPSI et être fournie par le sujet.

4.7 Certification

Une CA qui produit des certificats contenant la SIM inclut la SIM comme une forme de otherName d'après la structure GeneralName dans l'extension "subjectAltName".

Dans un environnement où une CA vérifie le SII avant de produire le certificat, une CA déchiffre les valeurs de EPEPSI qu'elle reçoit de l'utilisateur et de la RA, et les compare. Elle valide ensuite que la valeur de SII est correctement liée au sujet.

SIItype, SII, SIM = D(EPEPSI)

5. Définition

5.1 Syntaxe de SIM

Cette section spécifie la syntaxe pour la forme de nom de SIM incluse dans l'extension subjectAltName. La SIM est composée de trois champs : l'identifiant protège d'algorithme de hachage, la valeur aléatoire choisie par l'autorité, et la valeur du PEPSI lui-même.

```
IDENTIFIANT D'OBJET id-pkix ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
                                  pkix(7) }

IDENTIFIANT D'OBJET id-on ::= { id-pkix 8 }
IDENTIFIANT D'OBJET id-on-SIM ::= { id-on 6 }

SIM ::= SEQUENCE {
    hashAlg         AlgorithmIdentifier,
    authorityRandom  CHAINE D'OCTETS,       -- nombre aléatoire choisi par la RA utilisé pour le calcul de PEPSI.
        pEPSI         CHAINE D'OCTETS       -- hachage de HashContent avec l'algorithme hashAlg.
   }
```

5.2 PEPSI

Cette section spécifie la syntaxe de PEPSI. Le PEPSI est généré en effectuant deux fois la même fonction de hachage. Le PEPSI est généré sur la structure ASN.1 HashContent. HashContent a quatre valeurs : le mot de passe choisi par l'utilisateur, le nombre aléatoire choisi par l'autorité, le type d'identifiant, et l'identifiant lui-même.

```
HashContent ::= SEQUENCE {
   userPassword       UTF8String,                 -- mot de passe fourni par l'utilisateur
   authorityRandom  CHAINE D'OCTETS,              -- nombre aléatoire choisi par la RA
   identifierType      IDENTIFIANT D'OBJET,       -- SIItype
   identifiant          UTF8String                -- SII
 }
```

Avant de calculer un PEPSI, les mises en œuvre conformes DOIVENT traiter le userPassword avec l'algorithme de préparation de chaîne en six étapes de la [RFC4518], avec les changements suivants :

* dans l'étape 2, Map, la transposition devra inclure le traitement des caractères qui sont couramment transposés en rien, comme spécifié à l'Appendice B.1 de la [RFC3454].
* omettre l'étape 6, suppression des caractères non significatifs.

5.3 PEPSI chiffré

Cette section décrit la syntaxe pour PEPSI chiffré. Le PEPSI chiffré a trois champs : Type d'identifiant, identifiant, et SIM.

```
EncryptedPEPSI ::= SEQUENCE {
    identifierType  IDENTIFIANT D'OBJET,        -- SIItype
    identifiant       UTF8String,               -- SII
    sIM               SIM                       -- Valeur de SIM
 }
```

Quand il est utilisé dans une demande de certificat, l'OID dans 'regInfo' de la [RFC4211] et la [RFC2986] est comme suit :

IDENTIFIANT D'OBJET id-regEPEPSI ::= { id-pkip 3 }

6. Exemple d'usage de SIM

Selon les différents environnements de sécurité, il y a trois cas d'utilisation possibles avec la SIM.
1. Quand un consommateur d'assertions n'a aucune information sur l'utilisateur de certificat.
2. Quand un consommateur d'assertions connaît déjà le SII de l'utilisateur de certificat.
3. Quand l'utilisateur de certificat ne veut pas divulguer son SII.

Pour le cas d'utilisation 1, le SII et un mot de passe choisi par l'utilisateur P (que seul l'utilisateur connaît) doivent être envoyés à un consommateur d'assertions via un canal de communication sûr ; le certificat incluant la SIM doit aussi être transmis. Le consommateur d'assertions acquiert R du certificat. Le consommateur d'assertions peut vérifier que le SII a été validé par la CA (ou RA) et est associé à l'entité qui a présenté le mot de passe et le certificat. Dans ce cas, le consommateur d'assertions apprend quel SII est lié au sujet par suite de la procédure.

Dans le cas 2, un utilisateur de certificat transmet seulement le mot de passe, P, et le certificat. Le reste de la procédure est le même que dans le cas 1, mais ici le consommateur d'assertions fournit la valeur du SII, sur la base de sa connaissance externe de cette valeur. L'objet est dans ce cas de permettre au consommateur d'assertions de vérifier que le sujet est lié au SII, probablement parce que le consommateur d'assertions identifie le sujet sur la base de ce SII.

Dans le dernier cas, l'utilisateur du certificat ne veut pas divulguer son SII à cause de soucis de confidentialité. Ici, la seule information envoyée par un sujet de certificat est la valeur intermédiaire du PEPSI, H(R || P || SIItype || SII). Cette valeur DOIT être transmise via un canal sûr, pour préserver sa confidentialité. À réception de cette valeur, le consommateur d'assertions applique la fonction de hachage à la valeur de PEPSI intermédiaire envoyée par l'utilisateur, et la confronte à la valeur de SIM du certificat de l'utilisateur. Le consommateur d'assertions n'apprend pas la valeur du SII de l'utilisateur par suite de ce traitement, mais le consommateur d'assertions peut vérifier le fait que l'utilisateur connaît le bon SII et le bon mot de passe. Cela donne au consommateur d'assertions plus d'assurance que l'utilisateur est le sujet du certificat. Noter que cette forme de vérification d'identité d'utilisateur N'est PAS à utiliser à la place des procédures standard de validation de certificats, mais plutôt en plus de ces procédures.

7. Contraintes de nom

La valeur de SIM est mémorisée comme un otherName d'un nom de sujet de remplacement ; cependant, aucune contrainte ne peut être placée sur cette forme du nom.

8. Considérations sur la sécurité

La confidentialité d'une valeur de SIM est créée par le hachage itératif des valeurs de R, P, et SII. Une valeur de SIM dépend de deux propriétés d'une fonction de hachage : le fait qu'elle ne peut pas être inversée et le fait que les collisions (en particulier avec des données formatées) sont rares. Les attaques courantes par [WANG] ne sont pas applicables aux valeurs de SIM car l'entité d'extrémité qui fournit les valeurs de SII et SIItype ne fournit pas toutes les données à hacher ; c'est-à-dire, la RA fournit la valeur R.

De plus, un très bon mot de passe est nécessaire pour protéger contre les attaques pour deviner les SIM. Du fait de la faible longueur de nombreux SII, il est possible qu'un attaquant soit capable de le deviner avec des informations partielles sur le genre, l'âge, et la date de naissance. Les valeurs de SIItype sont très limitées. Donc, il est important que les utilisateurs choisissent un très bon mot de passe pour empêcher un attaquant de déterminer si un SII deviné est approprié.

Ce protocole suppose que Bob est un consommateur d'assertions digne de confiance qui ne va pas réutiliser les informations d'Alice. Autrement, Bob pourrait "se faire passer pour" Alice si seulement la connaissance de P et du SII était utilisée pour vérifier l'identité prétendue d'un sujet. Donc, ce protocole DOIT être utilisé seulement avec les protocoles qui utilisent des signatures numériques générées en utilisant la clé privée du sujet.

Les signatures numériques sont utilisées par l'envoyeur d'un message pour démontrer sa connaissance de la clé privée correspondant à la clé publique dans un certificat, et donc pour authentifier et lier son identité à un message signé. Cependant, gérer une clé privée est vulnérable dans certaines circonstances. Il n'est pas pleinement garanti que la clé privée revendiquée soit liée au sujet d'un certificat. Donc, la SIM peut améliorer la vérification de l'identité d'utilisateur.

Chaque fois qu'un certificat doit être mis à jour, un nouveau R DEVRAIT être généré et la SIM DEVRAIT être recalculée. Répéter la valeur du SIM d'un certificat précédent permettrait à un attaquant d'identifier les certificats associés au même individu, ce qui peut être indésirable pour les besoins de la protection des données personnelles.

9. Remerciements

Jim Schaad (Soaring Hawk Consulting), Seungjoo Kim, Jaeho Yoon, Baehyo Park (KISA), Bill Burr, Morrie Dworkin (NIST), et le Internet Security Technology Forum (ISTF) ont significativement contribué au travail sur les concepts de SIM et de PEPSI et ont identifié une potentielle attaque contre la sécurité. Leurs commentaires sur l'ensemble des propriétés désirables pour le PEPSI et leurs améliorations au PEPSI ont éclairé nos travaux. Merci aussi à Russell Housley, Stephen Kent, et Denis Pinkas de leurs contributions au présent document.

10. Considérations relatives à l'IANA

Il pourra à l'avenir être demandé à l'IANA d'établir un registre des identifiants d'objets pour promouvoir l'interopérabilité dans la spécification des SII types.

11. Références

11.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2986] M. Nystrom, B. Kaliski, "PKCS n° 10 : Spécification de la syntaxe de demande de certification, version 1.7", novembre 2000. *(Information)*

[RFC3454] P. Hoffman et M. Blanchet, "Préparation de chaînes internationalisées ("stringprep")", décembre 2002. *(P.S.)*

[RFC4043] D. Pinkas, T. Gindin, "Identifiant permanent d'infrastructure de clé publique X.509 pour l'Internet", mai 2005. *(P.S.)*

[RFC4211] J. Schaad, "Format de message de demande de certificat d'infrastructure de clé publique X.509 pour l'Internet", septembre 2005. (*Remplace* RFC2511) *(P.S.)*

11.2 Références pour information

[RFC4518] K. Zeilenga, "Protocole léger d'accès à un répertoire (LDAP) : Préparation de chaîne internationalisée", juin 2006.

[FIPS 112] Federal Information Processing Standards Publication (FIPS PUB) 112, "Password Usage", 30 mai 1985.

[FIPS 180-1] Federal Information Processing Standards Publication (FIPS PUB) 180-1, "Secure Hash Standard", 17 avril 1995.

[FIPS 140-2] Federal Information Processing Standards Publication (FIPS PUB) 140-2, "Security Requirements for Cryptographic Modules", 25 mai 2001.

[WANG] Xiaoyun Wang, Yiqun Lisa Yin, et Hongbo Yu, "Finding Collisions in the Full SHA-1", Crypto'05. <http://www.infosec.sdu.edu.cn/paper/sha1-crypto-auth-new-2-yao.pdf >

Adresse des auteurs

Jongwook Park
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, 138-803
REPUBLIC OF KOREA
téléphone : 2-405-5432
mél : khopri@kisa.or.kr

Jaeil Lee
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, 138-803
REPUBLIC OF KOREA
téléphone : 2-405-5300
mél : jilee@kisa.or.kr

Hongsub Lee
Korea Information Security Agency
78, Garak-Dong, Songpa-Gu, Seoul, 138-803
REPUBLIC OF KOREA
téléphone : 2-405-5100
mél : hslee@kisa.or.kr

Sangjoon Park
BCQRE Co.,Ltd
Yuil Bldg. Dogok-dong 411-14,
Kangnam-ku, Seoul, 135-270
REPUBLIC OF KOREA
mél : sjpark@bcqre.com

Tim Polk
National Institute of Standards et Technology
100 Bureau Drive, MS 8930
Gaithersburg, MD 20899
mél : tim.polk@nist.gov

Appendice A. Syntaxe de module ASN.1 1988 "Compilable"

```
PKIXSIM {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-
sim2005(38) }

ÉTIQUETTES EXPLICITES DE DÉFINITIONS ::=

DÉBUT

-- EXPORTE TOUT

IMPORTE
AlgorithmIdentifier, AttributeTypeAndValue DE PKIX1Explicit88
{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-pkix1-explicit(18)}

-- SIM
-- OID de certificat de SIM

IDENTIFIANT D'OBJET id-pkix ::= { iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5)
                                  pkix(7) }
IDENTIFIANT D'OBJET id-on ::= { id-pkix 8 }
IDENTIFIANT D'OBJET id-on-SIM ::= { id-on 6 }

-- Syntaxe de certificat

SIM ::= SEQUENCE {
    hashAlg             AlgorithmIdentifier,
    authorityRandom  CHAINE D'OCTETS,      -- nombre aléatoire choisi par la RA utilisé pour le calcul de PEPSI.
     pEPSI               CHAINE D'OCTETS      -- hachage de HashContent avec l'algorithme hashAlg.
  }
```

```
-- PEPSI

UTF8String ::= [UNIVERSAL 12] CHAINE D'OCTETS IMPLICITE
-- Le contenu de ce type est conforme à la RFC 2279

HashContent ::= SEQUENCE {
   userPassword       UTF8String,                  -- mot de passe fourni par l'utilsateur
   authorityRandom  CHAINE D'OCTETS,               -- nombre aléatoire choisi par la RA
   identifierType     IDENTIFIANT D'OBJET,         -- SIItype
   identifiant          UTF8String                 -- SII
}

-- PEPSI chiffré
-- OID pour le type de contenu encapsulé

IDENTIFIANT D'OBJET id-regEPEPSI ::= { id-pkip 3 }

EncryptedPEPSI ::= SEQUENCE {
  identifierType  IDENTIFIANT D'OBJET,          -- SIItype
  identifiant       UTF8String,                 -- SII
  sIM               SIM                         -- Valeur du SIM
}

FIN
```

Déclaration complète de droits de reproduction