Groupe de travail Réseau
Request for Comments: 5518
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

P. Hoffman, Domain Assurance Council
J. Levine, Domain Assurance Council
A. Hathcock, Alt-N Technologies
avril 2009

Protocole Caution par référence (VBR)

Résumé
Le présent document décrit le protocole de caution par référence (VBR, *Vouch By Reference*). VBR est un protocole pour ajouter la certification de tiers à la messagerie électronique. Il permet à des tiers indépendants de certifier le propriétaire d'un nom de domaine associé au message reçu.

Table des matières

1. Introduction

Caution par référence (VBR, *Vouch By Reference*) est un protocole pour ajouter une certification par un tiers à la messagerie électronique. Précisément, VBR permet à des tiers indépendants de certifier le propriétaire d'un nom de domaine associé à la messagerie reçue. VBR peut être effectué n'importe où le long du chemin de transit de la messagerie, par tout module receveur capable, soit au sein du service traitant, soit par le logiciel de l'utilisateur final.

VBR réalise cela avec un protocole en deux parties :

- Dans la première partie, un envoyeur attache des informations de VBR aux messages électroniques. Les informations de VBR disent quels services de certification de domaine l'envoyeur pense qu'ils vont se porter caution pour le trafic de messagerie associé à cet envoyeur.

- Dans la seconde partie, le receveur interroge un ou plusieurs services de certification pour obtenir des informations sur l'identité qui a été associée à un message reçu. Ce dernier protocole utilise le DNS pour distribuer les informations de certification.

Un envoyeur fournit des attestations de certification en utilisant un nouveau champ d'en-tête de message de la [RFC5322], "VBR-Info:". Ce champ d'en-tête contient les noms des services que l'envoyeur demande de cautionner, et le type particulier de contenu du message. Un service de certification par un tiers, fondé sur le DNS peut, quand il est interrogé, répondre par une liste des types de contenu de message qu'il va cautionner, comme un "message de transaction provenant de somebank.exemple" et/ou "tous les messages provenant de anotherbank.exemple".

Un prérequis pour le succès d'une opération de VBR est la validation de l'identité associée au message. VBR est fondé sur l'utilisation des noms de domaine comme identifiants, et permet plusieurs méthodes pour obtenir et valider les noms de domaine. Les méthodes de validation sont décrites à la Section 7, "Obtenir un nom de domaine utile".

L'envoyeur effectue deux étapes :
1. Ajout d'un champ d'en-tête VBR-Info à son message
2. Protège le message, comme approprié

Si un receveur utilise le résultat de la caution pour ajuster des classements comme pourriels sur la messagerie entrante, ce receveur place une grande confiance dans le fonctionnement et la puissance du service de caution. Donc, les receveurs doivent apporter un grand soin au choix de tels services. De plus, ces receveurs peuvent vouloir choisir plus d'un service de caution afin d'éviter d'avoir un seul point de défaillance pour l'établissement du classement comme pourriel.

1.1 Définitions

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. Utilisation du champ d'en-tête VBR-Info

Un envoyeur utilise VBR pour indiquer quels services de certification de domaine l'envoyeur croit qu'ils vont se porter caution pour un élément de messagerie particulier. Le service de certification utilise VBR pour déclarer pour quelles signatures il va se porter garant. Ce protocole utilise le DNS pour distribuer les informations de certification.

Un message peut avoir plusieurs champs d'en-tête VBR-Info. Cela signifie que, dans la terminologie de la RFC 5322, VBR-Info est un "champ d'en-tête trace" et DEVRAIT être ajouté au sommet des champs d'en-tête.

Le contenu du champ d'en-tête VBR-Info est une liste de trois éléments :
- Le domaine responsable
- Le type de contenu du message
- Une liste des noms de domaine des services que l'envoyeur s'attend à garantir pour cette sorte de contenu

Le domaine responsable est donné par md= suivi par un nom de domaine. Le type de contenu est donné par mc= suivi par une chaîne ; les valeurs définies de cette chaîne sont données ci-dessous. La liste des services est donnée par mv= suivi

d'une liste des noms de domaine séparés par des caractères deux-points.

La syntaxe formelle du champ d'en-tête est définie à la Section 4.

3. Processus de validation

Un receveur de message utilise VBR pour déterminer l'état de certification en suivant les étapes suivantes :
1. Extrait le domaine à certifier et le type de contenu de message.
2. Vérifie l'utilisation légitime de ce domaine en utilisant un ou plusieurs mécanismes d'authentification comme décrit ici.
3. Obtient le nom d'un service de caution de confiance, soit dans l'ensemble fourni par l'envoyeur, soit d'un ensemble défini localement de services de caution préférés.
4 Il interroge le service de caution pour déterminer si ce service se porte réellement garant pour ce type de contenu pour ce domaine.

4. Champ d'en-tête VBR-Info

Le champ d'en-tête VBR-Info a le format suivant:

VBR-Info: md=<domain>; mc=<type-string>; mv=<certifier-list>;

où <domain> est le domaine pour lequel la caution est offerte, <type-string> est le type de contenu du message, et <certifier-list> est une liste des noms de domaine de fournisseurs de certification dont l'envoyeur affirme qu'ils se portent garant pour ce message particulier. La structure de <certifier-list> est un ou plusieurs noms de domaine avec un caractère deux-points (":") entre chaque. Les éléments dans <domain>, <type-string>, et <certifier-list> ne doivent pas avoir d'espace incluse.

Par exemple, supposons que le signataire a deux compagnies qui veulent se porter garantes de ses notices de transaction : certifier-a.exemple et certifier-b.exemple. Le signataire va ajouter ce qui suit à l'en-tête de ses messages sortants.

VBR-Info: md=somebank.exemple; mc=transaction; mv=certifier-a.exemple:certifier-b.exemple;

Les trois paramètres d'en-tête dans l'en-tête VBR-Info sont tous obligatoires. En particulier, il n'y a pas de valeur par défaut pour md= domaine.

Les caractères majuscules et minuscules sont équivalents dans un champ d'en-tête VBR-Info, bien que par convention les contenus sont tous en minuscules. Pour la rétro compatibilité, les vérificateurs DOIVENT accepter les champs dans tout ordre et DEVRAIENT ignorer tous champs autres que les trois définis ici.

Si un message a plus d'un champ d'en-tête VBR-Info, les vérificateurs DEVRAIENT vérifier chacun tour à tour ou en parallèle jusqu'à ce qu'un certificateur satisfaisant soit trouvé ou que tous les champs d'en-tête aient été vérifiés. Tous les champs d'en-tête VBR-Info dans un même message DOIVENT avoir des valeurs mc= identiques.

4.1 Syntaxe des champs d'en-tête VBR-Info

Dans l'ABNF ci-dessous, les jetons ALPHA et DIGIT sont importés de la [RFC5234], et les jetons FWS et domain-name sont importés de la [RFC4871].

```
vbr-info-header =  "VBR-Info:" 1*([FWS] element [FWS] ";")
element = md-element / mc-element / mv-element

md-element = "md=" [FWS] domain-name

mc-element = "mc=" [FWS] type-string
type-string = "all" / "list" / "transaction"

mv-element = "mv=" [FWS] certifier-list
certifier-list = domain-name *(":" domain-name)
```

5. Interrogation du DNS

Quand un receveur veut vérifier si une revendication de certification est valide, il compare la liste dans le message à la liste des services auxquels il fait confiance. Pour chaque service qui est à l'intersection des deux listes, il place un nom de domaine à chercher qui consiste en les étiquettes DNS suivantes (de gauche à droite) :

- le nom de domaine dont il affirme qu'il peut être certifié
- _vouch (un littéral de chaîne)
- le nom d'hôte du service de caution.

Un enregistrement TXT pour ce nom de domaine est cherché dans le DNS. Le receveur cherche le nom de domaine dans le DNS exactement de la même manière qu'il cherche tout autre nom de domaine.

Par exemple, si un message signé par somebank.exemple contenait le champ d'en-tête VBR-Info ci-dessus, le receveur pourrait chercher l'un ou l'autre des noms suivants, selon le service de caution auquel il fait confiance :

somebank.exemple._vouch.certifier-b.exemple
somebank.exemple._vouch.certifier-a.exemple

Si l'enregistrement TXT existe dans le DNS, il contient une liste délimitée par une espace de tous les types que le service certifie, donnée en ASCII minuscule. Par exemple, le contenu de l'enregistrement TXT pourrait être :

transaction list

Dans l'exemple ci-dessus, le receveur vérifie si un certificateur cautionne un message "transaction". Cela pourrait être indiqué par un des types suivants : "all" ou "transaction" ("all" indique que le certificateur cautionne tous les types de message envoyés dans le domaine en question). Si un de ces types apparaît dans un enregistrment TXT, le certificateur a garanti la validité du message. Bien sûr, le receveur doit ignorer les services auxquels il ne fait pas confiance ; autrement, un acteur malveillant pourrait juste ajouter une autorité qu'il a établie afin qu'l puisse se porter garant pour lui-même.

Le nom pour l'étiquette _vouch a été choisi parce que tout nom de domaine qui l'inclut comme une de ses étiquettes ne peut pas être un nom d'hôte valide. Il n'y aura jamais de chevauchement accidentel avec un nom d'hôte valide. De plus, il est sûr de créer une règle qui dit qu'un enregistrement TXT du DNS venant d'un nom de domaine qui inclut une étiquette _vouch va toujours avoir la structure définie dans le présent document.

Si les RDATA dans l'enregistrement TXT contiennent plusieurs chaînes de caractères (comme défini au paragraphe 3.3 de la [RFC1035]) le traitement du code qui répond du DNS DOIT assembler tous ces blocs de texte rassemblés en un seul avant qu'ait lieu toute vérification syntaxique.

Les vérificateurs DOIVENT alors s'assurer que l'enregistrement TXT consiste en chaînes de lettres minuscules séparées par des espaces, et éliminer tout enregistrement qui n'est pas dans ce format. Cela défend contre les enregistrements mal configurés et les enregistrements non pertinents synthétisés à partir de caractères génériques du DNS.

L'enregistrement VBR DOIT avoir seulement un enregistrement TXT.

Cette méthode d'interrogation s'appuie sur les avantages considérables d'efficacité, de fiabilité et d'expérience du DNS existant. La recherche est très efficace, et les certificateurs peuvent ajouter et supprimer les enregistrements de client aussi rapidement qu'ils le veulent. La recherche s'appuie aussi sur la mise en mémoire tampon négative du DNS ([RFC2308]).

6. Types de contenu de message

Cette section décrit les types de contenu pour lesquels un certificateur peut se porter garant. Alors que le reste de la spécification VBR est surtout technique et précis, la description des types de contenus dans les messages électroniques est par nature ouverte à l'interprétation. Donc, cette section fait des distinctions aussi spécifiques que possible, mais le lecteur doit comprrendre que ces définitions sémantiques peuvent être interprétées de manière très différentes par des personnes différentes.

Noter que la valeur dans l'élément mc= est auto affirmée. L'objet de cet élément est pour l'audit. Il y aura probablement des

cas où un certificateur va cautionner un type de message d'un envoyeur (comme un message transactionnel) mais pas un autre type (comme une publicité). Un envoyeur qui ne peut pas obtenir quelqu'un pour certifier ses messages de publicité, mais a un certificateur pour ses messages transactionnels, pourrait être tenté de tricher et de les étiqueter comme du transactionnel. L'élément mc= crée une piste d'audit pour aider leurs certificateurs a saisir de telles tricheries et permettre la suppression de la certification pour la messagerie transactionnelle.

Trois types de contenu sont définis.

6.1 All

"all" signifie tous les messages provenant de l'envoyeur.

6.2 List

"list" est la catégorie pour les messages électroniques envoyés à plusieurs receveurs où chaque message est identique ou très similaire aux autres.

6.3 Transaction

"transaction" est la catégorie pour les messages transactionnels. C'est une réponse à une action spécifique de l'utilisateur, ou une remarque à l'envoyeur sur un événement dans le compte de l'utilisateur.

7. Obtention d'un nom de domaine utile

VBR s'appuie sur un nom de domaine qui spécifie une partie responsable du message. Cela exige d'obtenir le nom de domaine et de posséder une forte base d'assurance que l'utilisation du nom de domaine est valide, c'est-à-dire, qu'il n'a pas éte usurpé.

Il y a différentes façons de réaliser cela et cette section discute des mécanismes permis. Les envoyeurs DEVRAIENT utiliser la messagerie identifiée par clés de domaine (DKIM, *Domain Keys Identified Mail*) (et PEUT utiliser des clés de domaines, le cadre de politique d'envoyeur (SPF, *Sender Policy Framework*) ou l'identifiant d'envoyeur) pour donner une identité responsable pour l'envoyeur.

7.1 DKIM

La messagerie identifiée par clés de domaine (DKIM), [RFC4871], définit une identité responsable en associant un nom de domaine au message. Elle donne l'assurance que l'association est valide par un mécanisme d'authentification fondé sur une clé publique.

- Quand DKIM est le mécanisme de validation, le md= de VBR DOIT correspondre au nom de domaine pris d'un des champs d'en-tête de la signature DKIM. Si la signature DKIM contient un champ i=, le nom de domaine provenant de ce champ est utilisé ; autrement, le nom de domaine provenant du champ d= de la signature DKIM est utilisé.

- Le champ d'en-tête VBR-Info DEVRAIT être inclus dans l'ensemble de champs d'en-tête protégés par DKIM pour empêcher une partie malveillante de changer le contenu du champ d'en-tête VBR-Info ou d'ajouter des champs d'en-tête VBR-Info bogués.

- Le champ d'en-tête VBR-Info DEVRAIT être ajouté dans l'en-tête immédiatement après le champ d'en-tête DKIM-Signature correspondant.

Si la signature DKIM se valide, le nom de domaine pris de cette signature est valide pour être utilisé avec VBR.

7.2 DomainKeys

Les clés de domaine (DK, *DomainKeys*), [RFC4870], définissent une identité responsable en associant un nom de domaine au message dans l'étiquette d= du champ d'en-tête DomainKey-Signature. Elles fournissent l'assurance que l'association est valide par un mécanisme d'authentification fondé sur une clé publique.

- Quand DomainKeys est le mécanisme de validation, le md= de VBR DOIT être la même valeur que le nom de domaine trouvé dans le paramètre d= de DomainKey-Signature.

- Le champ d'en-tête VBR-Info DEVRAIT être inclus dans l'ensemble de champs d'en-tête protégés par DK pour empêcher une partie malveillante de changer le contenu du champ d'en-tête VBR-Info ou d'ajouter des champs d'en-tête VBR-Info bogués.

- Le champ d'en-tête VBR-Info DEVRAIT être ajouté immédiatement après le champ d'en-tête DomainKey-Signature correspondant.

Si la signature de DomainKeys se valide, le domaine dans l'étiquette d= est valide pour être utilisé avec VBR.

7.3 SPF

Le cadre de politique d'envoyeur (SPF, *Sender Policy Framework*) [RFC4408], définit une identité responsable en utilisant une adresse de messagerie existante et en interrogeant le DNS pour découvrir si elle est valide pour l'usage de SPF.

Quand SPF est le mécanisme de validation, le md= de VBR DOIT être la même valeur que le nom de domaine dans l'adresse <reverse-path> qui est le premier paramètre de la commande SMTP MAIL.

Un domaine est valide pour être utilisé avec VBR seulement quand le processus SPF produit un résultat "pass".

7.4 Identifiant d'envoyeur

L'identifiant d'envoyeur, [RFC4406], définit une identité responsable en utilisant une adresse existante de message connue comme l'adresse du responsable prétendu ([RFC4407]) et en interrogeant le DNS pour découvrir si elle est valide pour l'usage d'identifiant d'envoyeur.

Quand l' identifiant d'envoyeur est le mécanisme de validation, le md= de VBR DOIT être la même valeur que le nom de domaine dans l'adresse du responsable prétendu dans le message.

Un domaine est valide pour l'utilisation avec VBR seulement quand le processus d'identifiant d'envoyeur produit un résultat de "pass".

8. Considérations sur la sécurité

VBR est utilisé pour permettre aux utilisateurs de faire confiance à des tiers indépendants pour certifier le possesseur d'un nom de domaine associé au message reçu. La partie qui valide le message pourrait utiliser cette relation de confiance pour effectuer des actions qui affectent la sécurité de leur système.

Le receveur d'un message avec un champ d'en-tête VBR-Info DOIT ignorer les certificateurs en qui ils n'ont pas confiance ; autrement, un acteur malveillant pourrait juste ajouter une autorité qu'il a établie afin qu'il puisse se cautionner lui-même.

Les mises en œuvre DEVRAIENT limiter le nombre de champs d'en-tête VBR-Info qu'il traitent dans un seul message afin de se protéger contre des attaques fabriquées ou de déni de service.

9. Considérations relatives à l'IANA

L'IANA a enregistré le champ d'en-tête VBR-Info dans le registre des champs d'en-tête de message ([RFC3864]) comme suit :
Nom de champ d'en-tête : VBR-Info
Protocole applicable : mail
Statut : standard
Auteur/contrôleur des changements : IETF
Document de spécification : RFC 5518

Informations en rapport : aucune

10. Références

10.1 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)

[RFC5234] D. Crocker, P. Overell, "BNF augmenté pour les spécifications de syntaxe : ABNF", janvier 2008. (STD0068)

[RFC5322] P. Resnick, éd., "Format du message Internet", octobre 2008. (*Remplace* RFC2822) (MàJ RFC4021) *(D.S.)*

10.2 Références pour information

[RFC1035] P. Mockapetris, "Noms de domaines – Mise en œuvre et spécification", STD 13, novembre 1987. (*MàJ par* RFC1101, 1183, 1348, 1876, 1982, 1995, 1996, 2065, 2136, 2181, 2137, 2308, 2535, 2673, 2845, 3425, 3658, 4033, 4034, 4035, 4343, 5936, 5966, 6604, 7766, 8482, 8767)

[RFC2308] M. Andrews, "Mise en antémémoire négative des interrogations du DNS (DNS NCACHE)", mars 1998. (*MàJ par les RFC* 4033, 4034, 4035, 6604, 8020) *(P.S.)*

[RFC3864] G. Klyne, M. Nottingham, J. Mogul, "Procédures d'enregistrement pour les champs d'en-tête de message", septembre 2004. (BCP0090 ; *MàJ par* RFC9110)

[RFC4406] J. Lyon, M. Wong, "Identifiant d'expéditeur : authentification de message électronique", avril 2006. *(Expérimentale)*

[RFC4407] J. Lyon, "Adresse du responsable prétendu dans les messages électroniques", avril 2006. *(Expérimentale)*

[RFC4408] M. Wong, W. Schlitt, "Cadre de la politique de l'expéditeur (SPF) pour l'autorisation d'utilisation des domaines dans la messagerie électronique, version 1", avril 2006. *(Remplacée par* RFC7208)

[RFC4870] M. Delany, "Authentification de message électronique fondée sur le domaine avec des clés publiques annoncées dans le DNS (DomainKeys)", mai 2007. (*Obsolète, voir* RFC4871) *(Historique)*

[RFC4871] E. Allman et autres, "Signatures de messagerie identifiées par DomainKeys (DKIM)", mai 2007. *(Remplace* RFC4870 *Màj par* RFC5672 *; Remplacée par* RFC6376) *(P.S.)*

Appendice A. Remerciements

De nombreux membres du conseil d'assurance de domaine (Domain Assurance Council) ont contribué à la conception du protocole et à la rédaction de ce document. De plus, des suggestions constructives ont été reçue de Jim Fenton et Murray Kucherawy.

Adresse des auteurs

Paul Hoffman
Domain Assurance Council
mél : paul.hoffman@domain-assurance.org

John Levine
Domain Assurance Council
mél : john.levine@domain-assurance.org

Arvel Hathcock
Alt-N Technologies
mél : arvel.hathcock@altn.com