DomainKeys Identified Mail

DKIM (DomainKeys Identified Mail) est une norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique. Elle constitue une protection efficace contre le spam et l'hameçonnage.

En effet, **DKIM** fonctionne par signature cryptographique du corps du message ou d'une partie de celui-ci et d'une partie de ses en-têtes. Une signature **DKIM** vérifie donc l'authenticité du domaine expéditeur et garantit l'intégrité du message. DKIM intervient au niveau de la couche application du modèle OSI, ainsi il constitue une double protection pour des protocoles de messagerie électronique tels que SMTP, IMAP et POP en plus de l'utilisation de ces protocoles en mode sécurisé (POPS, IMAPS).

Cette technologie a été normalisée par l'IETF dans la RFC 4871 remplacée depuis par la RFC 6376.

Historique

DKIM est le résultat d'un projet d'un consortium industriel en 2004, intégrant et améliorant le système DomainKeys, de la société Yahoo! (standard DomainKeys qui a par ailleurs été défini ultérieurement - en 2007 - dans la spécification historique RFC 4870), et Identified Internet Mail, de Cisco.

La spécification résultante est utilisée en production. Tous les courriels émanant de Yahoo, GMail, AOL et FastMail contiennent en principe une signature DKIM.

Il a également été pris en compte par le groupe de travail de l'IETF pour affinage et standardisation, ce qui a abouti à la RFC 6376.

Principe

Il s'agit d'ajouter dans tous les emails sortants, une signature DKIM contenant une liste de "clé=valeur". Les clés sont courtes, généralement une ou deux lettres.

Les paramètres par défaut du mécanisme de facteur d'authentification sont d'utiliser SHA-256 comme fonction de hachage cryptographique, le chiffrement RSA pour la cryptographie asymétrique, et de coder le hachage avec Base64.

Un serveur SMTP réceptionnant un email signé utilise ensuite l'identifiant de domaine responsable de la signature (SDID) et le sélecteur associé annoncés dans les en-têtes afin de récupérer la clé publique publiée dans le serveur DNS du SDID. Cette clé est utilisée pour vérifier la validité des signatures.

Exemple de signature jointe en en-tête d'un mail :

```
DKIM-Signature: v=1; a=rsa-sha256; s=brisbane; d=example.com;
     c=simple/simple; q=dns/txt; i=joe@football.example.com;
     h=Received : From : To : Subject : Date : Message-ID;
     bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
     b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
     4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
     KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
     4bmp/YzhwvcubU4=;
Received: from client1.football.example.com  [192.0.2.1]
     by submitserver.example.com with SUBMISSION;
     Fri, 11 Jul 2003 21:01:54 -0700 (PDT)
From: Joe SixPack <joe@football.example.com>
To: Suzie Q <suzie@shopping.example.net>
Subject: Is dinner ready?
Date: Fri, 11 Jul 2003 21:00:37 -0700 (PDT)
Message-ID: <20030712040037.46341.5F8J@football.example.com>
```

Les paramètres sont décrits dans la RFC 6376. Les plus pertinents sont :

- **b** pour les véritables signatures numériques des contenus (en-têtes et corps de mail) ;
- **bh** pour le hachage du corps ;
- **d** pour l'identifiant de domaine responsable de la signature (SDID) ;
- **s** pour le sélecteur.

Puis on trouve :

- **v** pour la version ;
- **a** pour l'algorithme de signature ;
- **c** pour l'algorithme de canonicalisation d'en-tête et corps ;
- **q** pour une liste de méthodes de requêtes utilisées afin de récupérer la clé publique de signature ;
- **l** pour la taille de la partie du corps signé à la forme canonique ;
- **t** pour l'horodatage de la signature ;
- **x** pour la durée d'expiration ;
- **h** pour la liste des champs d'en-tête signés, éventuellement répétés pour ceux qui apparaissent plusieurs fois (ex *keywords* ci-dessus). Il est à noter que le champ d'en-tête de la signature DKIM est lui-même toujours inclus implicitement dans **h**, avec la valeur du champ **b**, traité comme s'il était vide.

Un vérificateur teste l'enregistrement DNS TXT de `brisbane._domainkey.example.com`. Il n'y a ni autorité de certification, ni système de liste noire. Le sélecteur est une méthode directe pour autoriser un signataire à ajouter ou retirer des clés quand il le souhaite, sans archivage des signatures. Les données renvoyées par ce test sont également structurées en paires clé-valeur. Cela inclut la clé publique du domaine, ainsi que des tokens et flags. Le destinataire peut utiliser cela pour déchiffrer la valeur de hachage du champ en-tête et simultanément recalculer la valeur du hachage du mail reçu (en-tête et corps). Si les deux valeurs correspondent, cela prouve cryptographiquement que le mail a été signé par le domaine indiqué, et n'a pas été altéré pendant le transit.

L'échec de vérification de la signature n'impose pas de rejet systématique du message. En effet, ces raisons précises peuvent être rendues disponibles dans des processus en amont et en aval. Ces méthodes peuvent inclure un message FBL **(en)**, ou ajouter des champs résultats d'authentification au message, comme décrit dans la RFC 7001. La politique de rejet d'un email dont la signature DKIM ne serait pas vérifiée peut être publiée dans une entrée DNS de type TXT DMARC (`_dmarc.example.com`).

Utilisation

Microsoft Exchange utilise automatiquement la vérification DKIM pour tous les messages IPv6[1].

Faiblesses

- détails - en langue anglaise - sur les faiblesses intrinsèques de DKIM

Le système DKIM ne gère pas l'ajout d'annotations par un serveur de liste de diffusion, l'ajout d'une signature tierce cassant le code de la signature DKIM. Une option l dans l'entête DKIM-Signature header peut permettre de ne signer qu'un nombre donné d'octets du message initial. Tout ajout de texte au-delà de la longueur ainsi spécifiée n'est alors pas pris en compte lors du calcul de la signature DKIM, mais cette solution ne fonctionne pas pour les messages au format MIME.

L'utilisation complémentaire d'un système Sender Policy Framework (SPF) est envisageable, permettant ainsi de vérifier une liste blanche d'expéditeurs désirés (white list de domaines d'expéditeurs reconnus).

Références

1. Prise en charge de la validation des messages signés DKIM: Exchange Online Help (https://technet.microsoft.com/fr-fr/library/dn720849%28v=exchg.150%29.aspx)

Voir aussi

- Sender Policy Framework
- S/MIME
- OpenPGP

Liens externes

- **(en)** Le site officiel (http://www.dkim.org/)
- **(en)** RFC 4686, analysant les menaces auxquelles répond DKIM.
- Analyse en français du (http://www.bortzmeyer.org/6376.html)RFC 6376.
- **(en)** Liste des erreurs fréquentes (http://blogs.cisco.com/security/common_errors_causing_dkim_verification_failures/)

Ce document provient de « https://fr.wikipedia.org/w/index.php?title=DomainKeys_Identified_Mail&oldid=188712328 ».