RFC 5408 : Identity-based Encryption Architecture and Supporting Data Structures

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 janvier 2009

Date de publication du RFC : Janvier 2009

https://www.bortzmeyer.org/5408.html

L'IBE ("*Identity-Based Encryption*") est une technique d'identité numérique où les clés cryptographiques sont dérivées de l'identité (par exemple d'une adresse de courrier). Ce RFC normalise son utilisation, notamment dans S/MIME.

C'est fou ce qu'on fait avec les identités numériques. Il y avait des cas où l'identité était elle-même une clé publique (HIP, cf. RFC 7401 [1] et CGA, cf. RFC 3972) mais, avec IBE, les clés cryptographiques dérivent de l'identité. Si je prends comme identité une adresse de courrier comme `stephane+ibe@bortzmeyer.fr`, divers algorithmes comme celui de Boneh-Franklin (cf. RFC 5409) permettent de fabriquer une clé publique, que mes correspondants peuvent utiliser pour chiffrer des messages qui me sont destinés.

La clé privée, dans les systèmes d'IBE, est générée par un serveur dédié, dont la sécurité devient donc vitale (la section 7 du RFC le discute en détail). IBE est donc un système avec une bonne dose de centralisation. Ce serveur utilise les mêmes paramètres que pour le calcul de la clé publique, plus un secret.

La section 2.1 du RFC résume l'essentiel sur les IBE. Comme indiqué plus haut, il faut disposer d'un PPS ("*Public Parameter Server*") qui distribuera les paramètres publics nécessaires au calcul des clés et d'un PKG ("*Private Key Generator*") qui générera les clés privées. Il y a typiquement un PPS et un PKG par « domaine », un domaine étant un groupe d'identités ayant les mêmes paramètres. Comme une identité comprend souvent un nom de domaine (c'est le cas des identités basées sur l'adresse de courrier), la distribution des PPS et PKG suit typiquement celle du DNS.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc7401.txt`

Le RFC ne discute absolument pas des problèmes politiques que posent les IBE, problèmes qui avaient pourtant été soulevés dans le groupe de travail S/MIME de l'IETF, mais ignorés. Le principal problème est qu'IBE est typiquement soutenu par des gens qui veulent garder le contrôle des clés privées des utilisateurs, gouvernements dictatoriaux ou entreprises paranoïaques. L'argument principal est de simplifier la gestion des clés (celle-ci est la faiblesse courante des autres techniques de cryptographie car peu d'utilisateurs ont la compétence et l'envie de gérer leurs clés correctement). Un autre argument est le désir de mettre en œuvre des techniques de menottes numériques, par exemple pour empêcher la lecture d'un message après une certaine date. Ces points, absents du RFC, sont à garder en tête lorsqu'on évalue les IBE.

Le format de chiffrement et de signature des messages S/MIME (RFC 3851) est moins utilisé que son concurrent PGP (RFC 4880) mais il est le premier à permettre d'utiliser les IBE.

La section 2.2 explique le fonctionnement des IBE. Un client IBE doit récupérer les paramètres publics de génération de la clé publique (section 2.2.1) à un URI « bien connu ». Il peut ensuite fabriquer la clé publique et chiffrer (section 2.2.2). Pour lire un message ainsi chiffré (section 2.3), le destinataire doit obtenir les mêmes paramètres publics puis contacter le PKG (section 2.3.2). Il doit évidemment s'authentifier auprès de ce dernier.

Maintenant, place aux détails. La section 3 définit le format des identités en ASN.1. Elles seront typiquement encodées en DER. L'identité elle-même est une chaîne de caractères. La structure qui la contient contient aussi un domaine "*district*", qui est l'URI du PPS.

La section 4 donne le protocole d'interrogation du PPS, le serveur qui donnera les paramètres publics. Il s'agit d'un simple `GET` HTTP (RFC 7231, section 4.3.1) sur l'URI du domaine (section 4.1). Les paramètres seront encodés en DER et surencodés en Base64 et marqués comme du type `application/ibe-pp-data` (section 4.3).

Et pour les paramètres privés ? La section 5 s'en occupe. Le récepteur d'un message IBE contacte son PKG en HTTP (qui doit être chiffré et authentifié) et envoie une requête `POST` (RFC 2616, section 9.5). Dans le corps de cette requête, il enverra du XML (section 5.3) qui codera son identité et des paramètres optionnels (curieusement, il n'existe aucun schéma pour définir le XML acceptable). La réponse, de type `application/ibe-pkg-reply+xml`, sera également en XML (section 5.6), contenant entre autres un code de réponse et la clé privée en DER. Le code sera par exemple `IBE100` (succès) ou `IBE301` (clé inconnue ou irrécupérable).