Échange de clés, encapsulation de clés, transport de clés ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 février 2026

https://www.bortzmeyer.org/echange-cles.html

Comme j'écris souvent des articles où je parle de cryptographie, alors que je ne connais pas grand'chose à la cryptographie moderne (et un peu plus à la cryptographie antique), je me suis demandé quelle était la définition exacte de l'échange de clés, terme qu'on voit souvent dans les RFC.

Donc, je commence par te mettre en garde, cher lecteur et brillante lectrice : on est nettement en dehors de mon domaine de compétence. Cela ne va pas m'empêcher d'écrire, mais je préviens les expert·es en cryptographie qu'ils risquent des maladies cardiaques violentes à me lire. Ceci dit, je prends avec intérêt toutes les remarques que les dit·es expert·es pourraient envoyer, et pas la peine de prendre des gants <http://sl4.org/crocker.html>, je ne suis pas fragile. Autre problème, j'ai bien l'impression que la terminologie dans ce domaine n'est pas consensuelle, ou pas encore stabilisée.

Lorsqu'on a de la cryptographie hybride (hybride au sens ancien, celui du RFC 9180[1], pas au sens plus récent en cryptographie post-quantique, tel que discuté dans le RFC 9794), on a de la cryptographie asymétrique pour sa souplesse et de la cryptographie symétrique pour sa performance. Une clé pour la cryptographie symétrique (forcément privée puisqu'on est en cryptographie symétrique) est créée et les deux parties l'utilisent pour chiffrer. Le mécanisme par lequel les deux parties connaissent la clé est appelé l'**échange de clés** ("*key exchange*" dans les RFC) même si, en pratique, la clé n'est pas toujours échangée (avec Diffie-Hellman, la même clé est générée des deux côtés, elle ne voyage jamais). Mais j'ai déjà vu une autre définition d'échange de clés, qui est de restreindre ce terme au cas où la clé n'est pas échangée (oui, je sais, c'est bizarre), comme avec Diffie-Hellman cité plus haut. Et la définition du NIST <https://csrc.nist.gov/glossary/term/key_exchange> est encore différente.

J'ai dit que la terminologie n'est pas stable ou en tout cas pas universellement adoptée, du moins c'est ce que je vois du haut de ma grande ignorance de la cryptographie moderne. J'ai vu passer « établissement de clé » ("*key establishment*") au lieu du plus classique « échange de clé » (j'ai aussi vu « accord sur la

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9180.txt

clé » - "*key agreement*"). Et, fin février 2026, les articles de Wikipédia sur l'échange de clés et l'encapsulation de clé donnaient des définitions différentes de ce qu'est un échange de clés. Donc, je vais expliquer ce que j'utilise, moi, et rappelez-vous que tout le monde n'est pas d'accord sur la terminologie.

Lorsque la clé de chiffrement (cryptographie symétrique) est générée par une seule des deux parties, puis transmise à l'autre partie, grâce à la cryptographie asymétrique, on parle de transport de clé ou d'encapsulation de clé (comme dans le sigle KEM, "*Key Encapsulation Mechanism*", très à la mode en ce moment avec les algorithmes post-quantiques, mais qui n'est pas spécifique à ces algorithmes). Pour compliquer les choses, le RFC 4949 donne une autre définition d'« encapsulation de clé », mais qui semble dépassée désormais…

Un exemple de transport de clé serait un mécanisme où une des deux parties crée la clé de chiffrement symétrique, puis la chiffre avec la clé publique (cryptographie asymétrique, donc) de l'autre partie avant de lui envoyer. N'utilisez pas cette méthode telle quelle, elle est trop simpliste et a plusieurs failles de sécurité (comme, entre autres, l'absence de confidentialité persistante), ce qui explique qu'on utilise plutôt aujourd'hui un KEM, qui obéit à une définition plus stricte. Notez que, pour la confidentialité persistante, utiliser un KEM ne suffit pas, il faut quelques précautions supplémentaires, mais on s'éloigne du sujet.

À l'inverse, si la clé est générée par les deux parties (cas de ECDH par exemple), on va parler d'échange de clés (définition étroite, la définition large étant que tout est un échange de clés).

Bref, comme j'écris beaucoup sur les RFC, je vais m'en tenir à la terminologie des RFC, où « échange de clés » ("*key exchange*") désigne toutes les méthodes d'établissement de clé et où « encapsulation de clé » est un sous-ensemble des méthodes d'échange de clés.

Et je vais conclure avec une citation en anglais de l'excellent blogueur Martin Fowler `<https://martinfowler.com/bliki/AvoidingVideo.html>` sur pourquoi j'écris sur un sujet que je ne connais pas : « "*When I'm writing, I'm not usually explaining things I've already figured out, I'm doing the figuring out as I write. It's often pointed out that the etymology of the word [Caractère Unicode non montré [2]]essay[Caractère Unicode non montré] comes the French essayer, meaning [Caractère Unicode non montré]to try[Caractère Unicode non montré], and that writing an essay is about trying out your ideas. The act of writing something down has often helped me understand a topic, indeed I think that's a large part of why I write as much as I do. I enjoy trying to understand things, and writing for others is a vital tool to help me do that.*" »

2. Car trop difficile à faire afficher par LaTeX