assauts. En revanche, quand le pirate connaît au moins une partie du message, ses chances de succès augmentent. Par exemple, s'il sait qu'il commence par «Cher Monsieur Dupond», il peut d'abord chercher une clé qui décrypte la partie «Cher Monsieur Dupond» du texte clair, puis poursuivre le décryptage à l'aide des informations trouvées. Même quand le pirate ne connaît que le langage utilisé dans le texte clair, russe, français ou COBOL, il peut exploiter cette information. Si le message est en français, par exemple, alors le mot le plus fréquemment utilisé est sans doute «le» ou «la». Pour déjouer de telles attaques, certains systèmes cryptographiques compriment le message en clair,

L e s

Les certificats numériques sont importants en cryptographie à clé publique, parce qu'ils garantissent qu'un intermédiaire n'espionne pas les échanges. Pour envoyer ou recevoir des messages en utilisant les clés publiques, un utilisateur doit posséder deux clés cryptographiques, l'une secrète, l'autre publique. Ces clés sont de longues suites de 0 et de 1 (entre 500 et 1 000 chiffres binaires). L'utilisateur garde sa clé secrète dans un endroit sûr, chiffrée sur un disque dur par exemple, mais il distribue sa clé publique à ceux avec qui il veut communiquer.

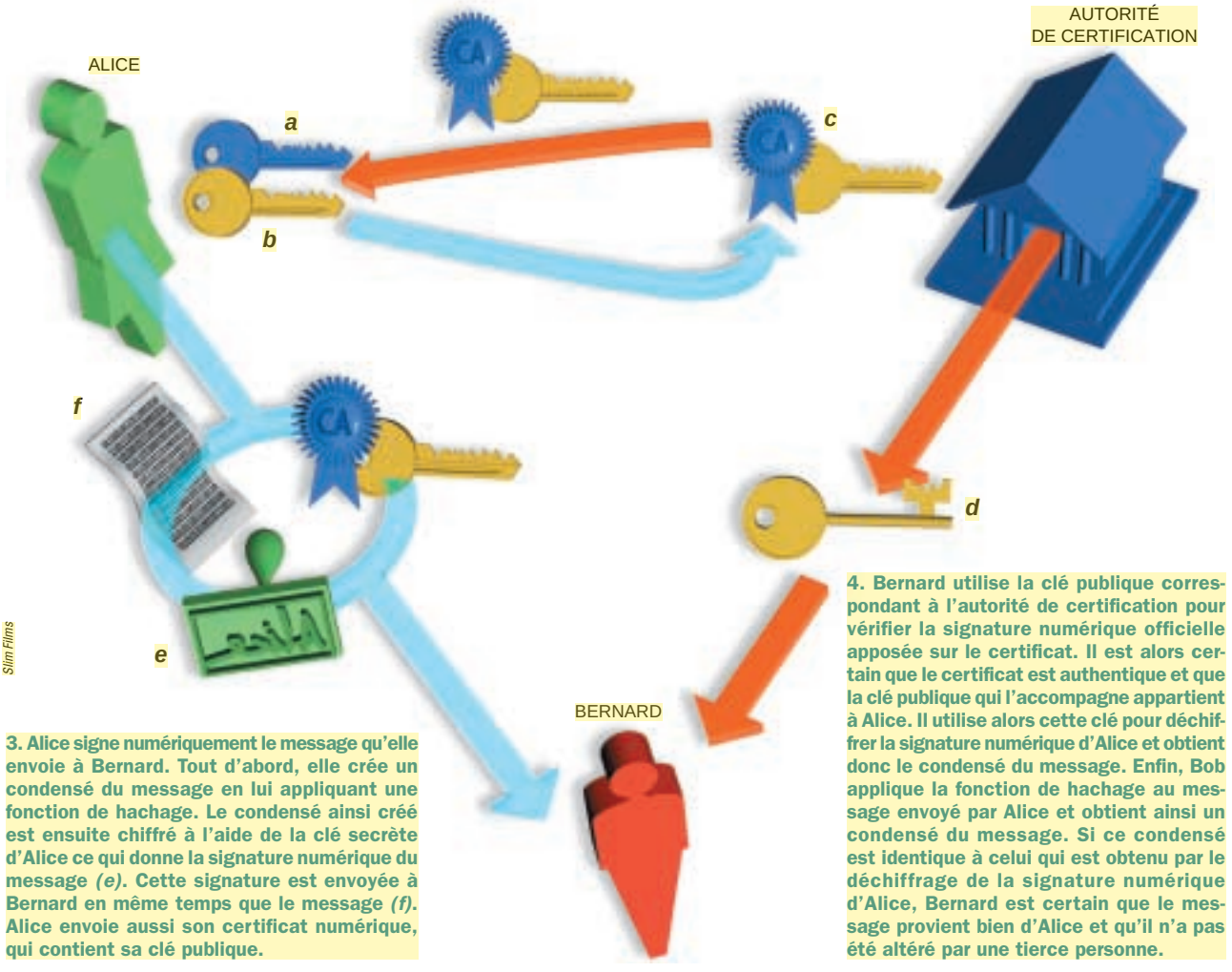
Supposons qu'Alice veuille envoyer à Bernard un message authentifié, c'est-à-dire un message dont Bernard saura de façon certaine qu'il vient d'elle. En utilisant sa clé secrète, Alice crée une signature numérique qu'elle joindra au message. Puis, en utilisant la clé publique d'Alice, Bernard vérifiera cette signature. Cependant, comment Bernard saura-t-il que la clé publique appartient effectivement à Alice ?

Un imposteur pourrait créer sa propre paire de clés et envoyer sa clé publique à Bernard en prétendant qu'elle appartient à Alice. On évite cette fraude en utilisant une autorité de certification, qui fournira un certificat numérique sur la clé publique reconnu par tous. Plusieurs entreprises, telles *VeriSign* ou *GTE CyberTrust*, délivrent des certificats numériques. Ainsi, le certificat numérique est l'analogue informatique de la carte d'identité.

Warwick FORD, *VeriSign*

1. À l'aide des logiciels de cryptographie, Alice crée une clé secrète *(a)* ainsi qu'une clé publique *(b)*. Elle envoie la clé publique à une autorité de certification, à qui elle demande un certificat numérique. Pour authentifier Alice, cet organisme vérifie les informations fournies par Alice. Si tout est en ordre, l'organisme de certification envoie un certificat numérique *(c)* qui authentifie la clé publique d'Alice. Sur ce certificat se trouve la signature numérique du tiers de confiance qui peut être vérifiée par toute personne connaissant la clé publique de cet organisme.

2. La clé publique *(d)* de l'autorité de certification est fournie à ceux qui en ont besoin, dont Bernard. Elle peut être incluse dans les programmes de navigation sur le réseau Internet et dans d'autres logiciels utilisés pour les communications informatiques sécurisées.



3. Alice signe numériquement le message qu'elle envoie à Bernard. Tout d'abord, elle crée un condensé du message en lui appliquant une fonction de hachage. Le condensé ainsi créé est ensuite chiffré à l'aide de la clé secrète d'Alice ce qui donne la signature numérique du message *(e)*. Cette signature est envoyée à Bernard en même temps que le message *(f)*. Alice envoie aussi son certificat numérique, qui contient sa clé publique.

4. Bernard utilise la clé publique correspondant à l'autorité de certification pour vérifier la signature numérique officielle apposée sur le certificat. Il est alors certain que le certificat est authentique et que la clé publique qui l'accompagne appartient à Alice. Il utilise alors cette clé pour déchiffrer la signature numérique d'Alice et obtient donc le condensé du message. Enfin, Bob applique la fonction de hachage au message envoyé par Alice et obtient ainsi un condensé du message. Si ce condensé est identique à celui qui est obtenu par le déchiffrage de la signature numérique d'Alice, Bernard est certain que le message provient bien d'Alice et qu'il n'a pas été altéré par une tierce personne.