7. Dans la vie quotidienne

Alice aime son travail de paysagiste dans l'entreprise Thagem où elle doit aménager l'environnement de travail des mille cinq cents employés du site de Palombes sur Seine. L'essentiel de son activité est en plein air. C'est le printemps, les bouleaux lâchent leur pollen, et tout irait pour le mieux sans ce maudit rhume des foins qu'elle traîne depuis son adolescence.

Ce soir en quittant le travail, il faudra qu'elle passe voir son médecin pour se faire prescrire un traitement anti-allergique.

En descendant les escaliers de son appartement parisien, elle allume son téléphone mobile:

– Allô, docteur Maison ? Puis-je passer vous voir cette après-midi vers 17h30 ?

Le rendez-vous est rapidement pris. La journée commence bien. Elle croise sans le remarquer le facteur venu déposer le courrier dans le hall de son immeuble et s'engouffre dans le métro, passe machinalement son sac à main le long du tourniquet et pense déjà aux aventures du commissaire Evenberg, héros du roman qu'elle a commencé avant-hier et qui lui fera passer plus vite son trajet.

Après avoir présenté son badge aux tourniquets d'accès de Thagem, son esprit commute déjà sur ses tâches de la journée. Elle démarre la fourgonnette de service pour aller prendre livraison des nouveaux rosiers destinés à agrémenter les abords du lac artificiel, fierté du directeur, et qui a obtenu un prix du meilleur environnement d'entreprise de la région.

A midi, elle vérifie le solde de la carte Moneix qui lui permet de payer le repas sans avoir à se préoccuper de faire l'appoint aux caisses. 1\euro\ 23. Elle doit la recharger.

La journée passe vite. Elle repasse le tourniquet vers la sortie. C'est l'heure de son rendez-vous chez le médecin. Il fait beau. Elle décide de prendre un vélo en libre service avec son passe Circulo.

Elle avait oublié le changement d'adresse du docteur Maison ! Sans se démonter, elle télécharge l'application de navigation sur son téléphone qui lui indiquera la nouvelle adresse et l'itinéraire pour arriver à l'heure.

– Puis-je avoir votre carte Vitalix ?

Alice se laisse ausculter, et se réjouit d'avance à l'idée de soulager son nez bouché, ses démangeaisons et l'irritation insupportable de ses yeux.

– Vous n'avez qu'une sévère allergie au pollen, je n'ai rien remarqué d'autre, vous prendrez du Rhumactine en cas de production nasale abondante.

Alice sourit intérieurement en pensant au vocabulaire médical.

– Cela fera vingt-trois euros.

– Acceptez-vous la carte bancaire ?

– Oui, je préfère même! Avoir moins d'espèces dans mon cabinet me rassure. Je me suis déjà fait braquer.

De retour dans son appartement, elle branche son ordinateur en se souvenant soudain qu'aujourd'hui est la date limite pour valider la déclaration de revenus du foyer.

« Une mise à jour est disponible pour votre ordinateur, télécharger ? »

– Encore !

Elle accepte la mise à jour, l'ordinateur redémarre. Enfin elle valide la déclaration des revenus. Elle en profite pour commander sur Mississipi.fr la suite des aventures du commissaire Evenberg qui viennent de paraître. C'est fini pour les préoccupations de la journée. Il est temps de se détendre avec Bob en allumant le téléviseur. Il y a au programme un bon film du cinéma italien des années 70 sur la chaîne thématique à laquelle ils sont abonnés.

Cette tranche de vie fait intervenir quinze situations au cours desquelles ont été menées une ou plusieurs opérations cryptologiques. Ceci montre à quel point la cryptologie a maintenant envahit notre vie quotidienne sans que nous n'en ayons toujours conscience. Citons trois d'entre elles, qui chacune, utilisent une carte à puce :

- La voix est chiffrée sur les téléphones portables avant d'être transmise sur l'air.
- Les données sont authentifiées avant de valider une transaction par carte bancaire.
- Le programme de TV à péage est crypté pour n'être accessible qu'aux abonnés.

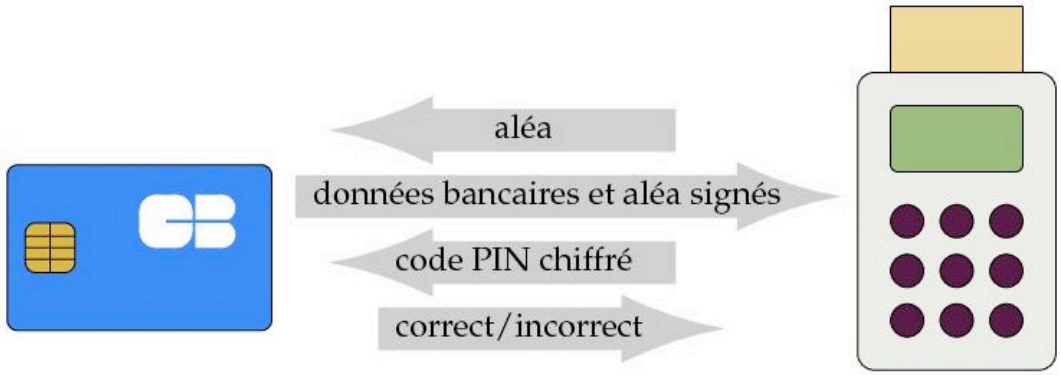

Fig. 5.3 Carte bancaire : authentification dynamique. La carte à puce signe elle-même les données bancaires en fonction d'une valeur aléatoire fournie par le terminal. Cela authentifie la puce elle-même et empêche le clonage des cartes.

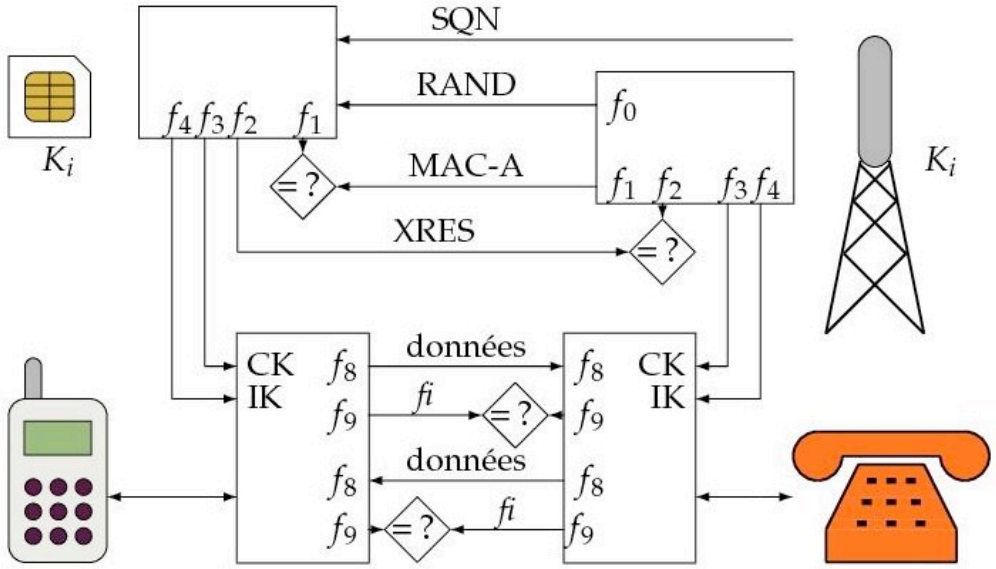

Fig. 5.4 La carte USIM et le centre de diffusion partagent une clé K_i propre à chaque abonné. Lors d'une demande de connexion au réseau, le centre d'authentification transmet des données RAND, SQN et MAC-A que la carte USIM peut contrôler avec K_i. En retour, elle renvoie une réponse XRES assurant l'authenticité de l'abonné. Ces données permettent également de calculer une clé de chiffrement CK et une clé d'intégrité IK qui serviront à la protection des données émises et reçues par voie radio. Ces clés sont transmises au téléphone par la carte USIM afin que celui-ci puisse chiffrer le signal et l'assortir d'une figure *fi* de contrôle d'intégrité à l'émission, ainsi que déchiffrer le signal et en contrôler l'intégrité à la réception.

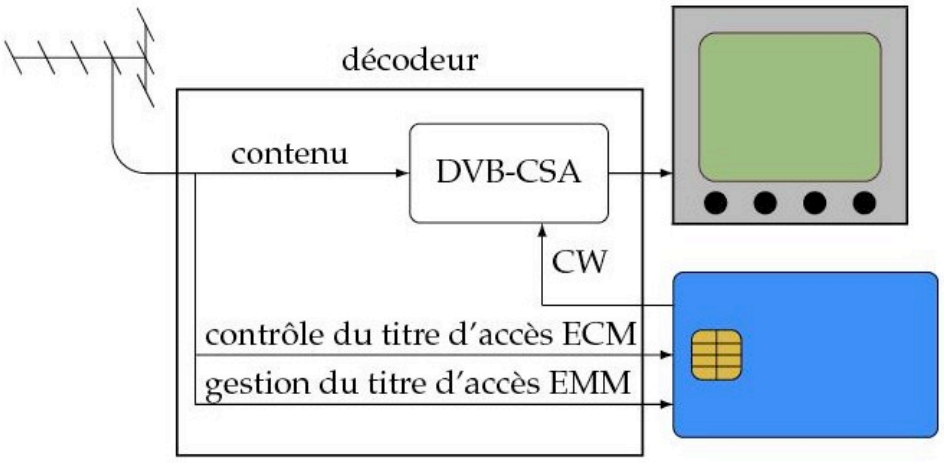

Fig. 5.5 Le décodeur reçoit un signal composé de plusieurs informations : le contenu audiovisuel chiffré avec le mot de contrôle CW (*Control Word*), les messages de contrôle des titres d'accès ECM et les messages de gestion des titres d'accès EMM. Les messages ECM et EMM sont transmis à la carte à puce qui, en fonction des titres d'accès, renvoie ou non le mot de contrôle en clair au décodeur en vue du déchiffrement du contenu par l'algorithme DVB-CSA.