LE LECAM

PRESENTATION

Le LECAM est un lecteur de cartes à mémoire connectable au Minitel. Utilisé à travers le réseau d'accès Télétel, il permet de mettre en oeuvre de multiples fonctions selon la carte utilisée :

- connexion automatique à un service TELETEL,
- contrôle de l'accès à un service par authentification de la carte présentée et éventuellement, vérification du code confidentiel du porteur par la carte,
- calcul de signature électronique des messages émis permettant au serveur de s'assurer de l'intégrité des messages reçus,
- mémorisation certifiée de transactions dans la carte et lecture certifiée d'informations contenues dans la carte,
- confidentialité des échanges par chiffrement et déchiffrement des données transmises sur le réseau.

Ce lecteur a pour caractéristique essentielle son universalité car il accepte tous les types de cartes respectant le projet de norme DIS 7816 de l'ISO. Son usage sera donc multiple et évolutif. La DGT, qui a commandé 50 000 lecteurs, les commercialisera en 1987 moyennant un prix de location-entretien de 50 F. TTC par mois.

QU'EST-CE QU'UNE CARTE A MEMOIRE ?

La Carte à Mémoire est le résultat de l'insertion, ou encartage d'un microcircuit électronique, appelé parfois "puce", dans un support en plastique au format d'une carte de paiement. Depuis le dépôt des premiers brevets en 1974, divers produits, différents sous des apparences identiques, sont apparus sur le marché. Tous ces produits ont en commun la fonction de mémorisation, d'où l'appelation générique de"Carte à Mémoire". Les cartes de haut de gamme contiennent un micro-circuit constitué d'un micro-processeur doté de sa mémoire de programme ROM et de sa mémoire de travail RAM, et d'une mémoire de stockage des données, aujourd'hui, en technologie EPROM (une seule écriture) , demain en technologie EEPROM (réécriture possible). Leur atout majeur est la sécurité : le micro-circuit est conçu de telle façon que le comportement de la carte se trouve entièrement contrôlé de l'intérieur par le micro-processeur, élément de passage obligé entre la mémoire de données et l'extérieur.

Le micro-processeur réagit en fonction du programme, souvent appelé masque car inséré dans la ROM lors de la fabrication du circuit par opération de masquage, qu'il exécute et dont les fonctions essentielles sont :

- la gestion du protocole d'échanges avec le lecteur,
  le contrôle d'accès à la mémoire de données,
  la mise en oeuvre d'un algorithme de sécurité à des fins d'authentification de signature et de gestion des clés.

La mémoire de données contient trois types d'informations :

- des informations libres, accessibles de l'extérieur sans formalité particulière ; ce sont, par exemple, l'identité du porteur, le numéro de la carte, le numéro de série du micro-circuit,
- des informations confidentielles, lisibles seulement après présentation du code confidentiel du porteur ou d'un code de l'émetteur de la carte,
  des informations secrètes, accessibles uniquement au micro-processeur qui interdit leur communication vers l'extérieur ; ce sont les clés secrètes, le code confidentiel du porteur, les codes de l'émetteur.

L'organisation de la mémoire de la carte, les conditions d'accès aux informations, les instructions exécutées par la Carte sont inhérentes au programme du micro-processeur et sont donc susceptibles de variation, lors du développement de nouveaux programmes ou masques. Parmi les masques connus à ce jour, le plus diffusé est le M4 de BULL CP8 ; il sert donc de base à l'illustration du fonctionnement d'une carte à mémoire.

. LA GESTION DE LA MEMOIRE DE DONNEES

- Dès sa fabrication, le micro-circuit contient le programme ; le code de fabrication est inscrit dans sa mémoire secrète.

- Après l'encartage de la puce dans le support de plastique ,la personnalisation consiste à configurer la mémoire de données, à préciser les règles d'écriture et de lecture de la zone des transactions et à inscrire les données nécessaires à l'utilisation ultérieure de la carte : en zone libre, le numéro de carte défini par l'émetteur, la période de validité et le nom du porteur, en zone secrète les codes confidentiels de l'émetteur, le code confidentiel du porteur et la clé secrète.
La personnalisation n'est possible qu'après présentation du code de fabrication (CF).

En phase d'utilisation, seule la zone des transactions peut être accessible en écriture. Selon la règle fixée à la personnalisation, l'écriture de cette zone est soit libre (L), soit protégée ; dans ce dernier cas, la présentation du code du porteur (CP) ou d'un code de l'émetteur (CE) est nécessaire. Pendant toute opération de lecture de la mémoire de données, le micro-processeur contrôle le type de données demandées et exécute ou non l'instruction . A défaut des deux cas de restriction où la lecture des données secrètes est impossible (I) et où la lecture des données confidentielles n'est possible qu'après présentation du code du porteur (CP) ou du code de l'émetteur (CE), les données sont communiquées librement (L).

- IDENTIFICATION

A la demande du serveur, le LECAM demande au porteur son code confidentiel qui est présenté pour contrôle à la carte. Le serveur est averti de façon sûre et inimitable par certification de la réponse de la carte.

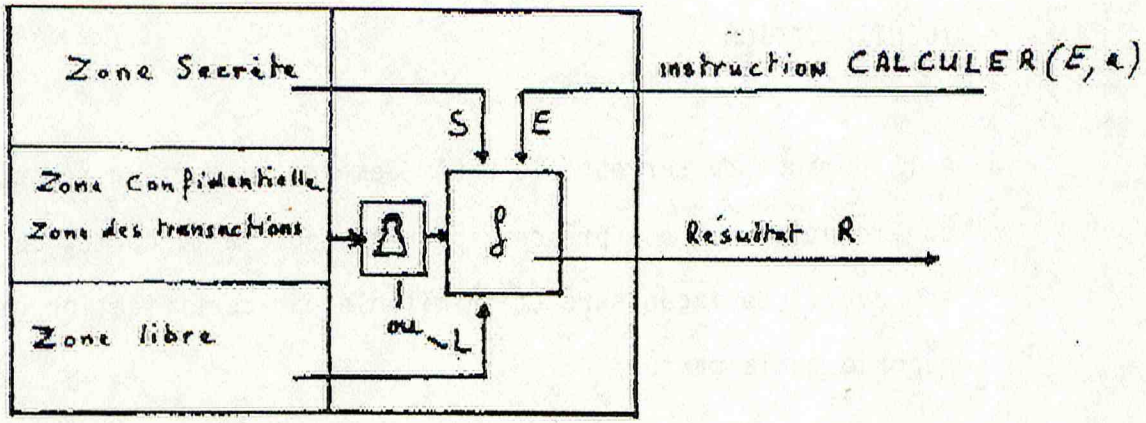
- SIGNATURE

Un texte, frappé au clavier du Minitel, est condensé par le LECAM, la certification, par la carte, du résultat de cette opération sert de signature au texte transmis en clair au serveur.

- GESTION DES CLES DE CHIFFREMENT

Par le même algorithme de sécurité, la carte à mémoire calcule la clé qui initialise l'algorithme de chiffrement/déchiffrement exécuté dans le lecteur de cartes.

PRINCIPE D'EXECUTION DE L'ALGORITHME DE SECURITE



Soit R = f(E//a,S,C)

si code porteur présenté correctement
sinon pas de résultat

Soit R = f(E//a,S,L)

sans obligation de présentation de code porteur

E : donnée externe (en général nombre aléatoire)

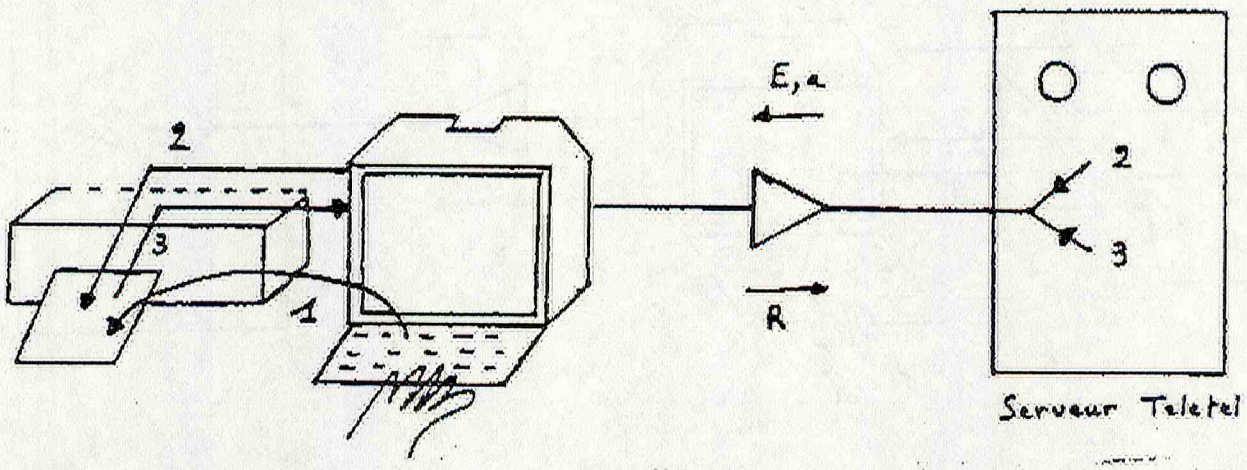
// : opération de concaténation

a : adresse du mot à certifier

L : mot d'adresse a de la zone libre

C : mot d'adresse a de la zone confidentielle ou de la zone des transactions.

AUTHENTIFICATION / CERTIFICATION / IDENTIFICATION



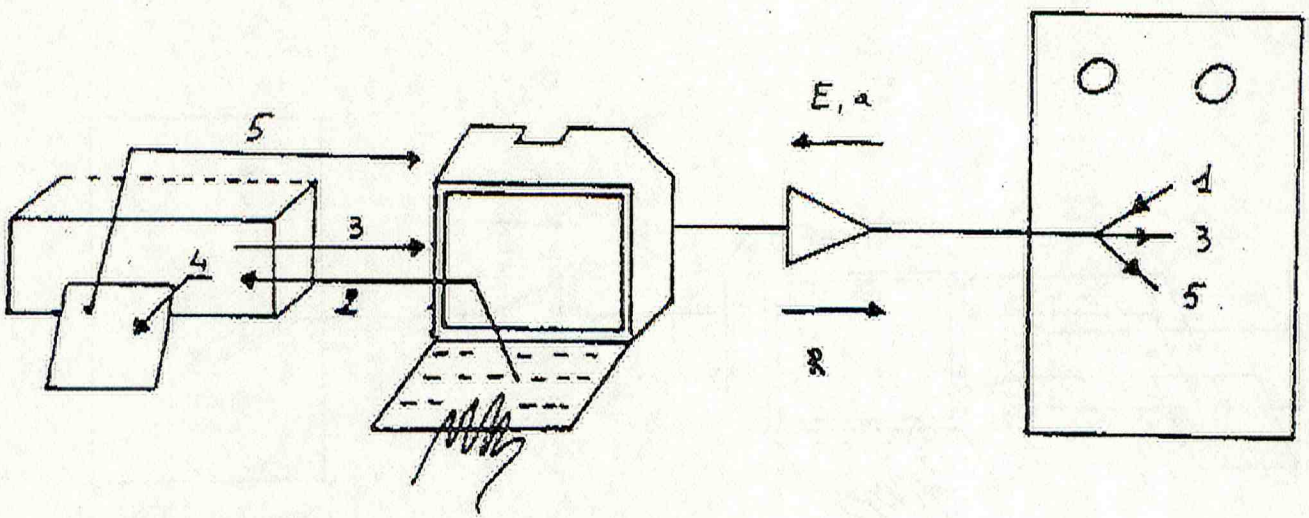
1 : Frappe du code confidentiel et contrôle par la carte

2 : génération du nombre aléatoire par le serveur et transmission à la carte

3 : exécution de l'algorithme de sécurité par la carte et analyse du résultat par le serveur

N.B la frappe du code confidentiel est optionnelle dans le cas où il n'est pas demandé. Il s'agit d'une authentification de la carte dans identification du porteur.

SIGNATURE



1 : Génération d'un nombre aléatoire par le serveur et transmission au LECAM
Lancement de la fonction de signature dans le LECAM

2 : Frappe texte et condensation par le LECAM

3 : Transmission du texte au serveur

4 : Fin de saisie :
Transmission à la carte du nombre aléatoire (E), d'une adresse (a) et du texte condensé aprés présentation éventuelle du code du porteur -

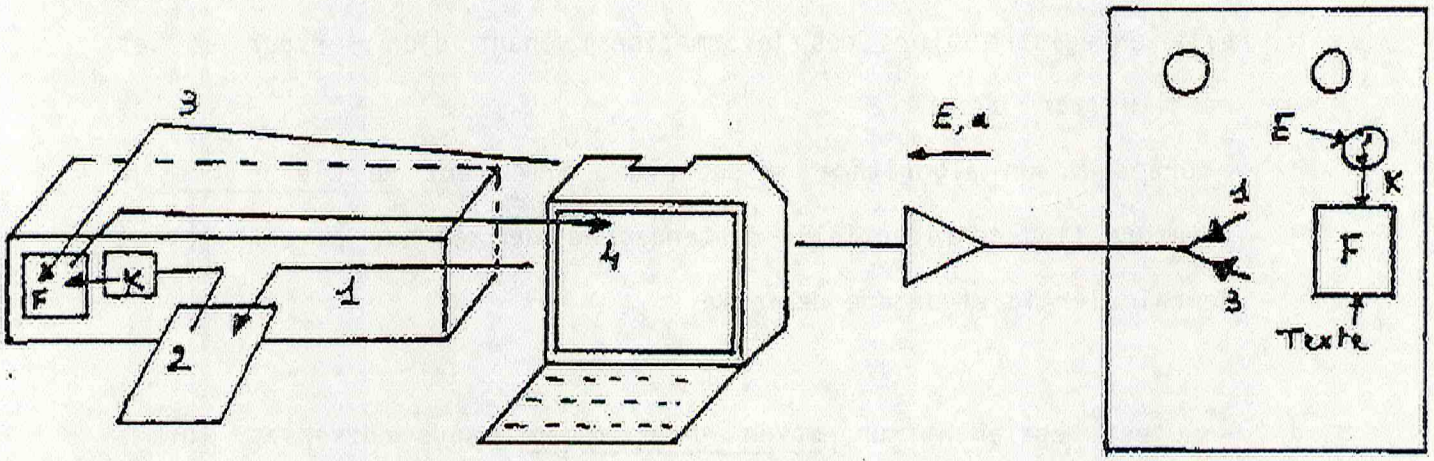
5 : restitution de la signature par la carte, transmission au serveur qui contôle

R signature = f (E//a//condensé, S, C ou L)

// opération de concaténation

C ou L mot d'adresse a

GESTION DE CLES POUR DECHIFFREMENT



1 : Tirage du nombre aléatoire E par le serveur qui calcule la clé K pour initialiser l'algorithme de chiffrement
transmission E à la carte

2 : calcul clé K par la carte et initialisation de l'algorithme de chiffrement du LECAM

3 : Chiffrement du texte par le serveur
transmission au LECAM

4 : Déchiffrement par le LECAM et affichage sur l'écran du Minitel

LA CARTE A MEMOIRE
UN CHAMP D'APPLICATIONS DIVERSIFIEES
ACCESSIBLES SUR LE RESEAU TELETEL

Les applications sont nombreuses .

- La carte à mémoire peut être considérée comme un support de données elle enregistre alors des informations venant d'un serveur et les restitue par la suite,
- Grâce à son algorithme de sécurité, elle sert de clé d'accès à l'information confidentielle contenue dans un serveur et elle permet de calculer la signature de texte,

- C'est également un moyen de paiement sous diverses formes assimilables au

  - chéquier électronique :
    . l'ordre de virement constitué du numéro de carte et du montant de la transaction certifié par la carte, sera traité par la banque afin de débiter le compte du porteur et créditer le compte du commerçant.
  - porte-monnaie électronique :
    . le compte de l'utilisateur est débité lors du chargement d'unités de compte dans la carte.
    . une fois la carte débitée du montant de la transaction, le commerçant disposera d'un enregistrement certifié lui permettant de se faire créditer du montant équivalent.

LES FONCTIONS DU LECAM

Le LECAM se présente comme un périphérique du Minitel à alimentation autonome.

- LES VOYANTS DE CONTROLE

L'emploi du LECAM est facilité par la présence en face avant de trois voyants :

- le voyant rouge allumé "M-A" signale la mise sous tension du lecteur,
- le voyant jaune "carte" s'éclaire durant chaque dialogue entre la carte et le lecteur ; il est maintenu éclairé tant que la carte est alimentée, signifiant ainsi l'accessibilité aux zones confidentielles ouvertes en lecture et en écriture, après présentation du code confidentiel du porteur,
- le voyant vert "secret" s'éclaire de façon fixe :
  . à la mise sous tension du LECAM pendant les tests de bon fonctionnement ; il s'éteint si le résultat est correct,
  . pour indiquer que la carte est prête à recevoir le code confidentiel du porteur frappé au clavier,
- le voyant vert clignote pendant la transmission de données chiffrées sur le réseau, quel que soit le sens, et pendant la compression de texte par le LECAM en vue de demander une signature à la carte.

- LA CONNECTIQUE

En face avant, le LECAM présente une fente pour l'introduction de la carte dans le connecteur. L'interface électrique, le protocole d'échange et la structure des commandes sont conformes au projet de norme DIS 7816/3 de l'ISO, avec :

- fréquence d'horloge : 3,57 Mhz
- taux de modulation : 9600 Bauds
- tension d'écriture dans la mémoire de la carte : 5 à 25 volts.

En face arrière, le LECAM est muni de deux prises péri-informatiques DIN, banalisées, pour le branchement au terminal Minitel d'une part et à un autre périphérique d'autre part. Le LECAM envoie des commandes au Protocole du Minitel tel qu'il est défini dans le document "Minitel 1B, Spécifications Techniques d'Utilisation (STUM 1B) ; il assure ainsi la gestion des aiguillages entre les modules du Minitel (prise, modem, clavier, écran) et les affichages sur l'écran.

Le LECAM est également compatible avec le système d'échanges assurant la gestion des échanges entre les divers périphériques raccordés au Minitel et les serveurs accessibles à travers le réseau Télétel. Cette communication est construite sur une connexion en chaîne de périphériques selon le protocole décrit dans le document "Spécifications Techniques d'Utilisation du Réseau Minitel" (STURM).

- LE MODE AUTONOME, AVANT CONNEXION AVEC LE SERVEUR

Dès l'introduction d'une carte et si le Minitel n'est pas connecté, le LECAM recherche dans la carte s'il existe des données de connexion à un serveur. Dans ce mode, le LECAM accepte les cartes dont les instructions de "lecture", "présentation de code" et éventuellement de "recherche en mémoire" et "demande de résultat" sont compatibles avec celles des cartes M4 et B1 dont les spécifications sont respectivement disponibles auprès de BULL et auprès du GIE des cartes bancaires. Les données de connexion sont contenues dans un bloc de mémoire, repéré par une entête particulière.

Dans le cas d'une carte M4, le LECAM scrute d'abord la zone libre et en cas d'échec la zone des transactions. Si cette dernière est protégée en lecture, le LECAM demande le code confidentiel et en gère la saisie. Pour faciliter cette saisie le lecteur dispose d'un éditeur de texte qui permet la correction des erreurs de frappe et analyse la réponse de la carte afin de demander éventuellement un nouvel essai.

Si un bloc de connexion est trouvé et en fonction des données enregistrées dans la carte, le LECAM procède à l'établissement de la communication téléphonique avec le réseau Télétel (cas du Minitel 10) puis à la connexion avec le serveur et avec le service requis. Si le Minitel est du type M1, le LECAM demande à l'utilisateur d'établir la communication téléphonique puis il gère la connexion au service.

- LE MODE TELECHARGE, APRES CONNEXION AVEC LE SERVEUR

Une fois la connexion établie, le LECAM agit en fonction des instructions téléchargées par le serveur précisant l'enchainement des ordres à destination de la carte, les traitements locaux (saisie d'information au clavier, opérations arithmétiques et logiques, conversions, branchements en fonction de la réponse de la carte...) et la destination des données manipulées (carte, écran, serveur). Le LECAM met ainsi en oeuvre les fonctions de la carte pour y rechercher une information particulière, demander l'exécution de l'algorithme de sécurité, inscrire une transaction au premier emplacement libre... sans que le serveur ait la visibilité des traitements élémentaires, ce qui a pour effet de minimiser les échanges sur le réseau.

Le serveur a la possibilité de demander l'exécution du programme résident de saisie du code confidentiel et d'utiliser les programmes de traitement local des anomalies.

Le serveur peut également demander au LECAM de chiffrer les données frappées au clavier ou lues dans la carte et de déchiffrer les données reçues pour affichage sur l'écran, chargement dans la carte ou transfert vers un périphérique.

Enfin, le serveur peut placer le LECAM en mode "saisie signée", opération qui consiste à condenser le texte frappé par l'utilisateur. Le texte est saisi par tranche de caractères avec une possibilité de correction lors de la frappe. En fin de saisie de la tranche le texte est alors transmis au serveur et à l'algorithme de compression du LECAM. En fin de saisie d'un texte constitué d'une ou plusieurs tranches, l'utilisateur donne son accord en actionnant la touche ENVOI. Le condensé est alors soumis à la carte pour calcul de la signature que le LECAM transmet au serveur en fin de texte.

Les échanges entre le serveur et le LECAM sont régis par un protocole assurant la transparence du réseau aux données, et la protection contre les erreurs en ligne.

- LA SECURITE

Les informations sensibles (code confidentiel frappé par l'usager, clé de chiffrement, condensé du texte à signer) sont mémorisées dans des zones protégées du LECAM, non accessibles au serveur lui-même. Pour cela, le LECAM contrôle l'état des aiguillages de Minitel afin que ces informations ne puissent être détournées de leur usage local. L'utilisateur est averti du mode de fonctionnement du lecteur par les voyants de contrôle et si nécessaire par des messages sur l'écran du Minitel. La carte fournit au LECAM la liste des instructions sensibles qui seront appliquées pour le calcul de la clé de chiffrement et de la signature de texte. Ces ordres prennent exclusivement leur paramètre dans la zone protégée du LECAM afin d'éviter qu'un texte issu du réseau et non agréé par l'utilisateur soit soumis à la signature ce qui constituerait une fraude.

QUELQUES EXEMPLES DE FONCTIONNEMENT DU LECAM

- CONNEXION AUTOMATIQUE A UN SERVEUR

A l'introduction de la carte et si le Minitel n'est pas connecté, le LECAM recherche les informations correspondant à une connexion automatique à un serveur par scrutation de la zone libre (inscription lors de la personnalisation), puis de la zone des transactions (inscription éventuellement téléchargée) ; si cette dernière est

protégée en lecture, il demande le code confidentiel du porteur.

Ces informations décrivent les données nécessaires à la connexion à un serveur (n° téléphonique du point d'accès, code du service ou numéro TRANSPAC) et à la sélection d'un service interne ainsi que toutes les actions répétitives conduisant à l'information requise (Log on).

- CONTROLE D'ACCES A UN SERVEUR

Sur instruction du serveur, le LECAM lui envoie l'identité de la carte suivi d'un certificat obtenu par l'exécution de l'algorithme de sécurité de la carte dont le résultat, dépend d'un nombre aléatoire fourni par le serveur, de la clé secrète inscrite dans la carte lors de la personnalisation et de la référence du service requis inscrite dans la carte lors de la personnalisation ou en phase d'utilisation. Les services personnalisés, par exemple la gestion de comptes, demandent une identification du porteur ; dans ce cas, l'obtention du certificat calculé n'est possible que si le contrôle effectué sur le code confidentiel présenté est positif.

- PAIEMENT ET PRISE DE COMMANDE

Sur instruction du serveur, le lecteur recherche le numéro de la carte et sa période de validité , informations inscrites lors de la personnalisation et définies par l'émetteur. Il retransmet ces informations avec un certificat prouvant leur authenticité (lecture certifiée) et donc celle de la carte. Le serveur a alors la certitude de l'identité de la carte, repérée par son numéro de carte. Il peut également contrôler la présence de la personne habilitée à utiliser cette carte ; dans ce cas, il télécommande une procédure d'identification par exécution du programme résidant dans le LECAM, ayant pour objet de demander le code confidentiel du porteur et de le présenter à la carte.

Le serveur doit également disposer des mécanismes de sécurité afin de reconstituer, en fonction d'une clé secrète maîtresse et du numéro de carte, les clés secrètes diversifiées des cartes pour vérifier la validité des certificats reçus.

Deux architectures sont possibles :

- le système est privé :

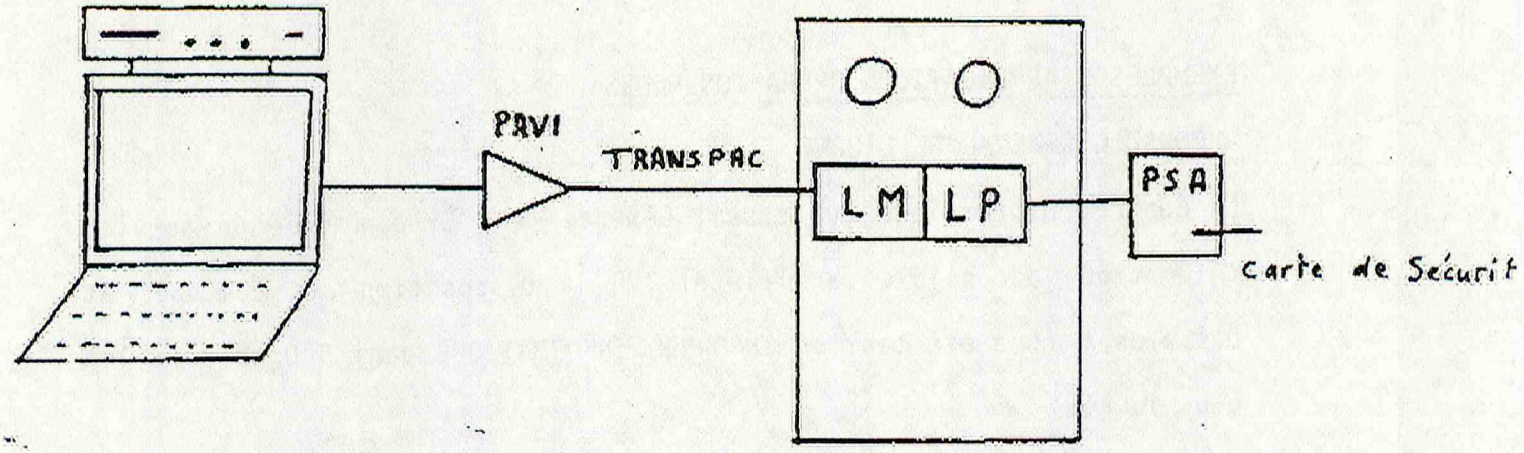
  Le serveur accepte des cartes dédiées à une application particulière dont l'algorithme de sécurité et les règles de calcul des clés diversifiées sont tous deux connus. Dans ce cas les fonctions de sécurité peuvent être programmées dans le serveur ;

- le système est partagé avec d'autres applications :

  Le serveur accepte les cartes des émetteurs avec qui il a passé un contrat. Dans ce cas, plutôt que de diffuser ses propres secrets, l'émetteur confie au serveur un circuit de sécurité apte à contrôler l'authenticité des cartes et la validité des certificats reçus. Le serveur doit donc être muni d'un périphérique faisant l'interface avec ces circuits de sécurité, et du logiciel de gestion de ce périphérique. Un tel périphérique, appelé PSA, est aujourd'hui commercialisé par BULL.

  Des logiciels de dialogue avec le LECAM et la carte à mémoire ainsi qu'avec le PSA sont en cours de développement par les principales sociétés de service d'ingénierie et d'informatique. Ils seront disponibles en 1987, certains dès le début de l'année, pour les matériels de la gamme BULL DPS6, DPS7, DPS8, pour les matériels IBM 30XX et 40XX, pour les matériels PRIME et pour les matériels sous UNIX et PICK. Il existe également une solution sans PSA pour DPS7.

SYSTEME PARTAGE

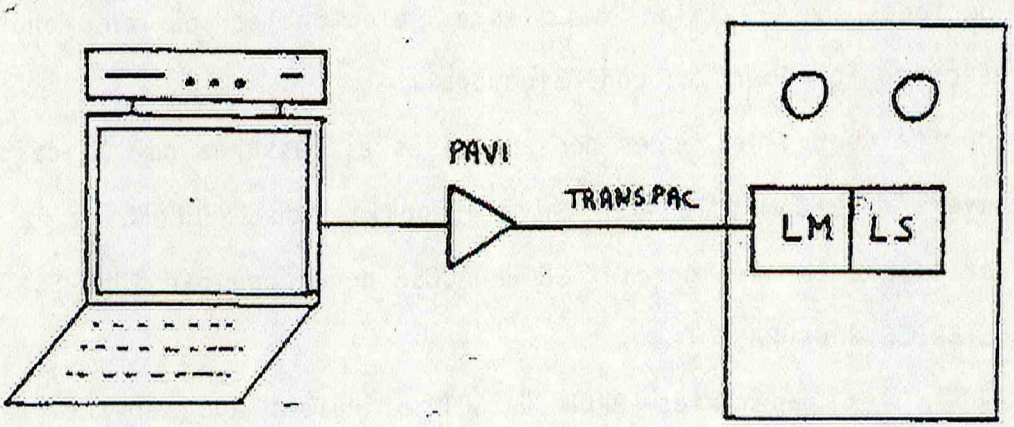


La carte du porteur donne accès à plusieurs applications

LP : logiciel de gestion du PSA

LM : logiciel de dialogue avec le Minitel et le LECAM

SYSTEME PRIVE



La carte du porteur est dédiée à l'application

LM : logiciel de dialogue avec le Minitel et le LECAM

LS : logiciel de sécurité contenant l'algorithme de sécurité de la règle et la méthode de calcul des clés diversifiées.

EXEMPLES D'APPLICATIONS OPERATIONNELLES

- CONSEIL GENERAL DE L'ORNE

Le Centre Informatique du Conseil Général de l'Orne a créé un service télématique accessible par Télétel 2 à la disposition des communes et des élus ; il a été baptisé INFORNEL INFORMATIQUE dans l'Orne pour les élus locaux.

Le site informatique est un DPS7/35 ; le terminal est le Minitel doté d'une imprimante et du LECAM. Le système de sécurité est du type privé. Une des applications originales de ce service concerne la gestion des listes électorales politiques ; l'application conçue et réalisée par le service informatique du Conseil Général, décharge les secrétariats de mairie de toutes les tâches répétitives engendrées par une gestion manuelle. Depuis chaque mairie, il est en effet possible d'assurer la saisie des électeurs, les modifications et radiations prévues pendant les périodes de révision des listes électorales ou en dehors de celles-ci conformément au code électoral.

La sécurité contre les accès non autorisés est assurée par la carte CP8 au travers du LECAM ; le lien entre l'application INFORNEL et la carte CP8 est assuré par le logiciel SECUR'ACCES developpé par BULL-SCAT.

- PAPETERIES BRUN PASSOT

Dès 1983, les papeteries BRUN PASSOT offraient un service télématique :BUREAUTEL 2000. Afin de prolonger les fonctionnalités de ce service, BRUN PASSOT ouvre BUREAUTEL CP8 utilisant une carte à mémoire M 4 et le LECAM. Le système de sécurité est du type partagé.

L'utilisateur du service peut grâce à son Minitel consulter la base d'information représentative des articles les plus souvent approvisionnés et passer une demande d'achat.

Au préalable, il lui aura fallu s'identifier en insérant sa carte BUREAUPASS dans le LECAM. Cette carte, outre les coordonnées du porteur comporte une allocation budgétaire fixée par le gestionnaire et décrémentée à chaque commande engagée. Tout dépassement du budget alloué (mensuel, trimestriel, annuel) entraîne une non exécution de la transaction en cours. Il est nécessaire alors soit d'attendre la réinitialisation sur la période suivante, soit de formuler une demande de "rallonge".

BUREAUTEL CP8 diminue très sensiblement les coûts administratifs de lancement d'approvisionnements, garantit le respect des seuils de dépenses (engagements budgétaires) en orientant et en régularisant les demandes de produits afin de permettre des économies complémentaires.

BUREAUTEL CP8 apporte ainsi une solution aux entreprises à unités éclatées, en permettant une décentralisation des actes d'approvisionnement et un contrôle des achats dans une ligne budgétaire.

BUREAUTEL CP8 est supporté par des ordinateurs PRIME, les logiciels mettant en oeuvre la carte à mémoire sont développés par la SEGIN.