

# Des clés dynamiques inviolables pour l'identification

**La jeune société française NTX Research s'appuie sur un brevet européen pour exploiter Internet Passport, son système d'identification sécurisé.**

Internet Passport est basé sur le principe d'identification par défi/réponse. L'accès à un service s'effectue par un ensemble d'échanges qui mettent en œuvre une technologie propriétaire.

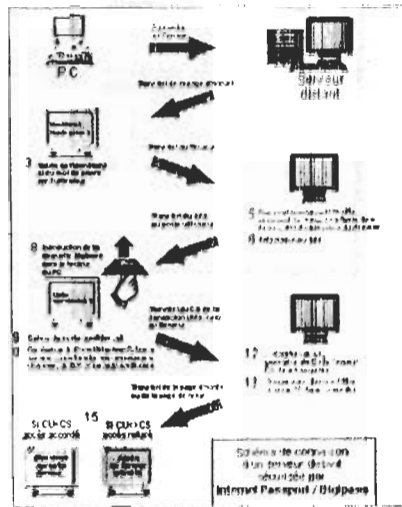
Côté serveur, Digipass (disponible en versions Unix et NT) émet vers le client un défi dont la clé est générée dynamiquement et sur 80 bits. La résolution de la réponse s'opère de façon transparente du côté client, l'utilisateur devant

seulement communiquer son code confidentiel à sa propre machine. Le noyau du système client réside obligatoirement sur un périphérique de type CD-Rom, disquette, carte à puce, etc. L'intérêt du système est lié au fait que le code confidentiel du client n'est pas un code d'activation et, en conséquence, ne se trouve pas stocké pour une reconnaissance sur le support du noyau client. Ainsi, aucune lecture du support ne peut dévoiler ce code.

Lorsqu'il valide le code confidentiel client, le système génère ensuite la clé de la réponse qui sera transmise au serveur. La clé de la réponse dynamique est codée sur 40 bits. Le

noyau client est également protégé contre les duplications, grâce au système de contrôle de copies de Microcosm Software, leader de ce marché.

La technologie d'identification Internet Passport peut être utilisée ponctuellement pour la signature sécurisée. En autorisant le scellement entre deux clients via un serveur équipé de Digipass, elle fait figure de solution complète et légère. Digipass serveur est disponible au prix de 100 000 francs (ht) pour cent licences utilisateurs et à 200 000 francs (ht) pour 5 000 utilisateurs. Le prix de la



La séparation physique de la machine client et des moteurs de développement minimise les risques.

licence supplémentaire est de 20 francs • R.C-T