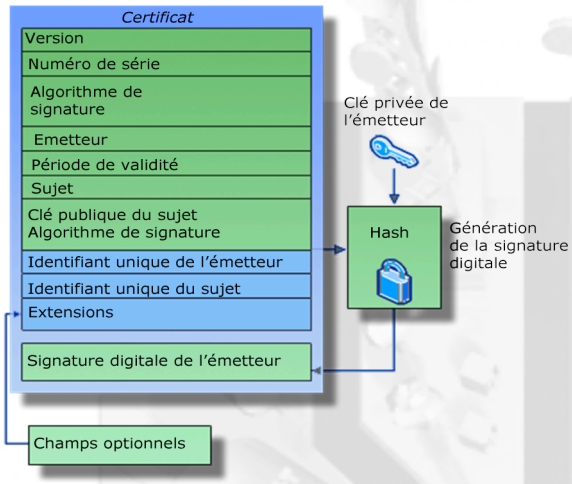
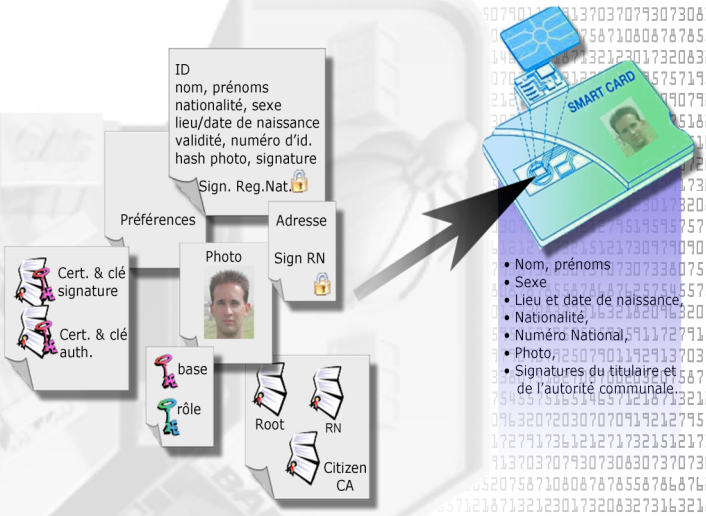
printemps des sciences
Science et ville 14-20 mars 2005

La carte d'identité électronique

DÉPARTEMENT D'INFORMATIQUE
Rémy Drijkoningen – Maurice Schubert – Paty Ilunga



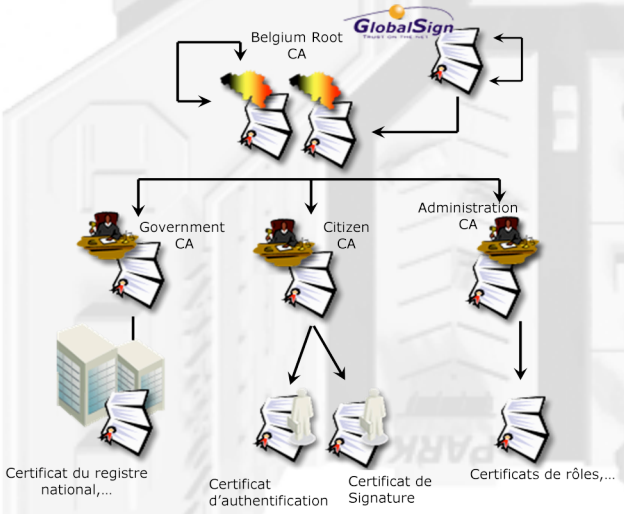


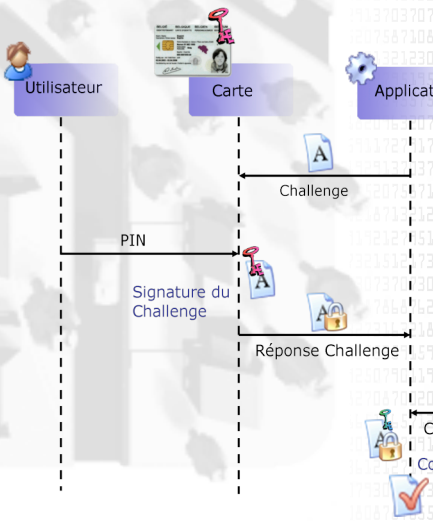
Le certificat

Document qui, par le biais d'une signature digitale, lie une clé publique à un ensemble d'attributs (individu, compétences,…).
Il peut donc permettre de vérifier qu'une clé publique appartient bien à un citoyen.

Contenu de la puce et de la carte

Comme pour la carte d'identité classique, la carte d'identité électronique comportera des informations visibles, mais également une puce contenant les éléments qui permettent de s'identifier et de signer de manière électronique.





Chemin de confiance

Chaque certificat pouvant être signé par la clé privée d'un autre certificat, on est en mesure d'établir un chemin de confiance remontant à une autorité dont la crédibilité est communément admise.

Protocole d'identification

Une application s'assure de manière sécurisée de l'identité d'un utilisateur. A aucun moment le PIN et la clé privée ne sont transmis à l'application. Le but est d'en prouver sa connaissance en répondant à une (ou plusieurs) question(s) : le(s) challenge(s).

FACULTE DES SCIENCES
UNIVERSITE LIBRE DE BRUXELLES