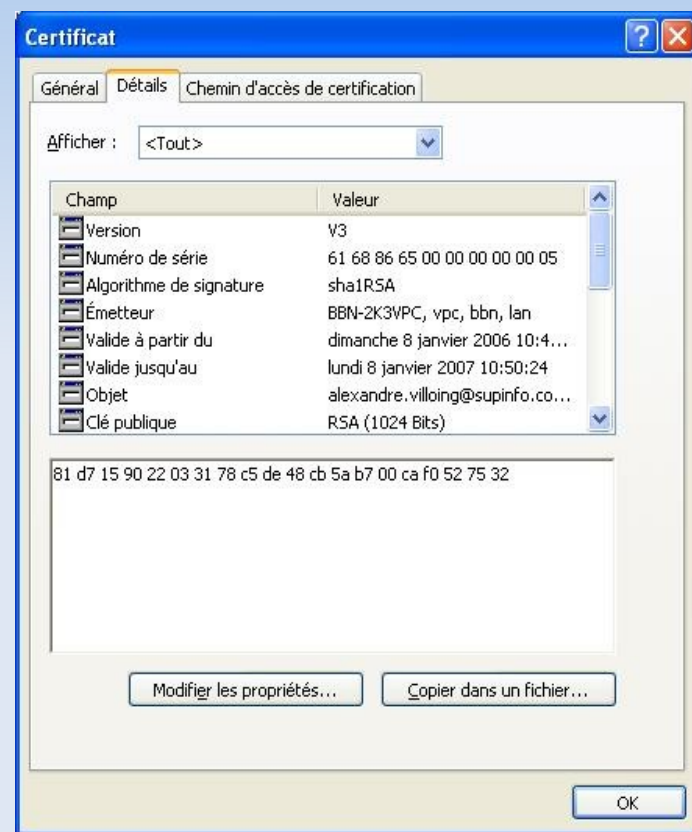


Une identité numérique

- Portée par un certificat numérique unique relative à :
 - Usage : Authentification ; Signature ; Chiffrement ; Horodatage ; ...
 - Un niveau de confiance partagé (Montant financier, valeur juridique, niveau de confidentialité,...)



La confiance numérique

- Définit par :
 - Des outils carte à puce, certificat logiciel, ...
 - Des procédures : face à face, courrier, ...
 - Décrit dans une Politique de certification
- Validé
 - Engagement de conformité à une politique
 - Confirmé par une identité de plus haut niveau (Autorité de certification Racine)
- Garanti par une Autorité Administrative
 - qui élabore et est garante de l'application de la politique

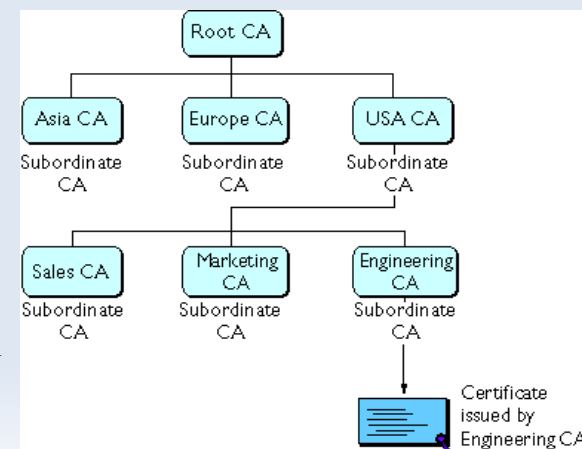


Les questions de la confiance

- En qui ai je confiance ? Ou comment reconnaître une Autorité de confiance :
 - Ne pas se poser de question
 - Faire confiance au navigateur (AC commerciales)
 - Une publication au JO.
04/06/2010, texte : 159
- La confiance s'hérite (modèle hiérarchique principalement)

RSA4096 bits

Module :00 aa 7c 28 9f 11 30 98 cd 6f 6e 2c 85 12 26 3b 08 06 ca 41 fd 52 4f 43 bd c0 26 27 71 76 1a 5996 d8 09 eb 07 aa 26 4e 4f 3e 4b a1 e3 97 87 8566 81 71 c9 b9 15 76 6f 77 50 18 93 10 2d37 884d 17 b7 f3 45 bd 22 2e b7 27 98 5b c7 05 fd bd33 ed a2 f5 53 1d 28 23 65 bf 40 35 6e ce 6a 0bc3 a9 f5 25 0c ab 22 f0 b8 c0 c4 7d 37 0c a3 627c ee b4 db 3d 21 39 a7 9c 89 e3 9b a2 10 f8 8ab6 4a 2f 2e98 69 2b 6a a0 86 da f1 08 e5 be 4c67 16 2d 25 61 f3 d5 0d 0b 17 44 47 09 d4 46 059d 0f c0 88 4d 61 e4 24 c4 c7 68 09 af ac d2 afb9 95 26 6f 80 04 fc 76 ac aa c7 23 b6 e4 06 9155 44 ec 64 db 99 81 1c d2 56 74 fd d6 32 28 bbcb c9 37 0d fb 69 6c 6f ba a3 6b 06 8c 6a 40 2e17 3a 39 ea d0 0c df 5a 1c ba 6f a4 32 b0 b8 cc3e 77 1b d3 8b 1f 86 fa ff 3e 3e 6f 5c 88 46 e7e3 0f fa ab 1d f3 7d 4b f8 54 6e 4e cc dc 32 5a63 78 a2 32 af 33 78 ea 43 e1 4c 7a 4d d7 94 062d e6 4f a5 42 92 af 28 8a 4f c3 15 ec a9 6b a9df e0 dd 13 02 bc cc 7d ff 2d e6 07 a9 be 75 96ea 42 5e 5b 1a de a2 33 b3 63 bd ab 05 f9 8b e6bd 4d d1 6d 56 9a eb 89 3c 9f c0 78 e4 be 25 7006 c5 11 73 a0 c8 ca 14 cb 3a d4 12 9c 2a 3c da5f 17 33 d9 76 14 37 aa 49 87 65 d9 f4 d9 2e 195f f9 a0 cd a8 b9 41 32 6d 71 a6 a4 cb f7 63 22d0 29 e4 ba 81 1a 6a 29 1d 9a a5 a4 5c 46 54 2445 d4 c8 ed 7a 79 85 ec 84 77 6e 67 4d 64 0f 43de 7a 83 a4 a7 d8 db b5 53 4c fe 62 c8 13 c3 6236 a5 28 31 32 9b b4 96 87 e2 99 c6 1f 56 bf 46a3 a9 64 31 e5 d5 b1 4b a8 66 cc 5b a1 ff 16 b0a 38 2a 18 8f 17 24 26 ad 91 74 85 68 c1 7f 1ae5 5a 14 b8 7d 0e b7 23 31 c0 64 b7 05 2f 41 58 55Exposant : 01 00 01



RGS et identité

- Définir des niveaux de confiance :
 - Étude des Politiques de certification
 - Le RGS facilitateur de reconnaissance des niveaux de confiance
 - 3 niveaux
 - pour différentes fonctions de sécurité
 - Authentification
 - Confidentialité
 - Horodatage
 - Signature
 - * : signature élémentaire
 - ** : signature sécurisée
 - *** : signature qualifiée (présomption de fiabilité)

Paysage de l'identité

- Des prestations
 - Commerciales : PSCE / OC (infogérants)
 - Modèle de coût principalement au certificat
 - Privé : IGC Notarial
 - Publique : IGCA, ANTS
- Des usages :
 - Télé-TVA / contrôle de légalité
 - Idénium
 - Recommandé numérique
 - Identité Agent Ministériel
 - Radar, Décodeur, box adsl, avionique...