



Découvrir la PKI.



REMERCIEMENTS

Ce stage n'aurait pu se faire sans la volonté et la collaboration de nombreuses personnes. J'exprime ma reconnaissance au personnel de l'Institut National des Sciences Appliquées de Rouen et plus particulièrement à Monsieur Philippe WENDER, responsable du Service Informatique et Réseaux, qui a fait preuve de pédagogie et à Philippe SAVARY son assistant.

Je tiens aussi à citer Michael BEDIU (stagiaire TSS Télécommunications et Réseaux) avec qui je m'entendais bien.

Enfin mes derniers remerciements iront à la secrétaire Marie-Claude GAUQUELIN dont la gentillesse n'est plus à démontrer.

Je remercie chaleureusement ces personnes pour l'aide qu'elles m'ont apportée dans cette démarche rendue possible grâce à leur accueil et leur ouverture.

Résumé à l'attention du lecteur pressé

PKI (Public Key Infrastructure), en français **IGC** (Infrastructure de Gestion de Clés) ou **ICP** (Infrastructure à Clés Publiques) est un système de gestion de clés de chiffrement et de certificats qui constitue un cadre à l'usage des techniques de cryptographie.

Une PKI est donc une structure qui permet de gérer les certificats (l'identité numérique) et les clefs de chiffrement d'un ensemble d'utilisateurs (servant à la signature numérique et au cryptage). C'est une « couche de gestion » qui s'occupe de délivrer les certificats, assure leur valeur et leur validité, et permet à tout le monde d'utiliser la cryptographie.

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Désormais, la cryptographie sert non seulement à préserver la **confidentialité** des données mais aussi à garantir leur **intégrité**, leur **authenticité** et le caractère **non-répudiable** des documents signés.

Une PKI intègre les moyens techniques et organisationnels pour produire et diffuser les certificats numériques. D'un point de vue organisationnel, elle s'appuie sur une Autorité de Certification, qui émet les certificats, et sur une ou plusieurs Autorités d'Enregistrement, qui valident les demandes de certificats. Il faut souvent y ajouter un serveur de révocation, qui permet de déclarer les certificats révoqués avant leur date d'expiration. Pour obtenir un certificat l'utilisateur adresse sa demande à l'autorité d'enregistrement. Si la demande est complète, conforme à la politique de certification et authentique, alors elle est transmise à l'autorité de certification qui produit le certificat puis transmet ce certificat à l'utilisateur et le publie dans l'annuaire. Si un deuxième utilisateur veut communiquer avec cet utilisateur, alors, il envoie une requête à l'annuaire et reçoit en retour le certificat de la personne qu'il veut contacter. Il contrôle ce certificat grâce à la clé publique de l'autorité de certification déjà en sa possession.

La sécurité de la PKI repose sur la sûreté de deux mécanismes :

- la vérification de l'authenticité de la demande de certificat (l'utilisateur devra certainement se déplacer physiquement pour se faire reconnaître)
- la distribution du certificat contenant la clé privée de l'utilisateur et la distribution initiale du certificat de l'autorité de certification car il permet de vérifier l'authenticité des certificats utilisateurs délivrés (établissement d'une confiance commune à un groupe de certificats).

Dans l'étude suivante « **Découvrir la PKI** » nous verrons que la fiabilité de l'IGC repose sur un cadre juridique qui règle, désormais de façon plus libérale, l'utilisation de la cryptographie. Nous verrons aussi que loin de s'attacher à un éditeur de logiciels chacun peut, grâce au Logiciel Libre, mettre en place son infrastructure privée. Nous comprendrons également que la PKI ne se substitue pas à la sécurité informatique mais en est un élément supplémentaire.

SOMMAIRE

INTRODUCTION	1
A) <i>Présentation de l'INSA</i>	1
A.1 En France.....	1
A.2 Les missions des INSA.....	1
A.3 Un projet d'ampleur nationale : Campus numériques et TICEs	1
B) <i>L'INSA de Rouen</i>	2
C) <i>Le Service Informatique et Réseaux</i>	3
D) <i>La mission proposée</i>	4
E) <i>Plan de l'étude</i>	5
PREMIERE PARTIE : L'environnement légal	6
<i>PREAMBULE, Infrastructure à clés publiques</i>	6
A) <i>SIGNATURE ELECTRONIQUE : définitions, Principes et législation</i>	7
A.1 Qu'est-ce que la signature électronique ?.....	7
A.2 Législation française et signature électronique	7
A.3 Les points importants du décret du 30 mars 2001	8
A.4 Définition juridique de la signature.....	8
A.5 Signature électronique sécurisée	8
A.6 Principes de la signature électronique par cryptographie asymétrique	8
A.7 Différents types de bi-clé	9
A.8 Prestataire de services de certification électronique	9
A.9 Différents modèles de confiance	9
A.10 Différentes architectures.....	11
A.11 Obtention et contenu d'un certificat de clé publique	12
A.12 Notion de certificat « qualifié ».....	13
A.13 Schéma national de qualification	14
A.14 Les cadres réglementaires divergent	15
B) <i>SIGNATURE ELECTRONIQUE : La preuve</i>	15
B.1 Le support de l'écrit est-il toujours le papier ?.....	15
B.2 L'écrit sous forme électronique peut-il avoir valeur probante ?	16
B.3 La signature électronique peut-elle avoir valeur probante ?.....	16
B.4 Présomption de fiabilité d'un procédé de signature électronique	16
C) <i>SIGNATURE ELECTRONIQUE : Responsabilités</i>	17
C.1 Comment choisir un certificat de signature électronique ?	17
C.2 Responsabilité d'une personne se fiant à la signature d'un certificat erroné	17
C.3 Responsabilité des Prestataires de Service de Certification Electronique (PSCE)...	17
D) <i>SIGNATURE ELECTRONIQUE : Services associés</i>	18
D.1 L'horodatage sécurisé est-il indissociable de la signature électronique ?.....	18
D.2 L'archivage sécurisé est-il indissociable de la signature électronique ?.....	18
D.3 Comment est créée et vérifiée une signature numérique?.....	19
E) <i>Le certificat X.509</i>	19
E.1 Les champs « standards »	20

E.2 Les champs « extensions ».....	20
F) <i>L'annuaire électronique léger</i>	22
F.1 Introduction.....	22
F.2 Qu'est-ce que LDAP?.....	22
G) <i>Protection des informations nominatives</i>	23
G.1 Définition.....	23
G.2 Obligation de déclaration	23
G.3 Obligation de sécurité.....	23
G.4 Obligation d'information.....	24
G.5 Sanctions pénales	24
G.6 CNIL.....	24
H) <i>Le point sur la cryptographie en France</i>	25
I) <i>Synthèse de la première partie</i>	26
DEUXIEME PARTIE : Les outils protocolaires de la sécurisation.....	27
<i>Comprendre la PKI</i>	27
Quelques chiffres.....	28
Principales technologies de défense	28
A) <i>IPSec</i>	29
A.1 La nécessité d'un paramétrage avancé.....	29
A.2 Trois mode de protection possible	30
A.3 Forces et faiblesses du protocole IPSec	31
B) <i>IPv6 ou IPng (next generation)</i>	31
B.1 Historique du protocole IP.....	31
B.2 Les objectifs principaux d'IPv6.....	31
B.3 Les principales fonctions d'IPv6	32
B.4 La notation IPv6	32
B.5 Transition d'IPv4 à IPv6	33
C) <i>SSL : Secure Socket Layer</i>	34
C.1 Le protocole SSL.....	34
C.2 Pourquoi SSL ?.....	35
C.3 Les sous-protocoles de SSL.....	35
C.4 Déroulement des échanges SSL	36
C.5 Les problèmes liés à SSL.....	37
C.6 La pratique	37
D) <i>SSH / SSF : Secure SHell</i>	39
D.1 Présentation.....	39
D.2 De quoi SSH peut-il protéger ?	39
D.3 Un défaut ?	40
D.4 Une histoire peu banale	40
D.5 Méthodes de chiffrement et d'authentification SSH.....	40
D.6 Clé publique et clé privée sous SSH	41
D.7 Conclusion.....	41
E) <i>Pourquoi ne pas choisir Netware de Novell ?</i>	41
F) <i>Synthèse de la deuxième partie</i>	41

TROISIEME PARTIE : Dispositifs matériels pour la sécurisation.....	43
<i>Préambule</i>	43
Protéger un réseau d'entreprise.....	43
Protéger les données de l'entreprise	43
Problème de la gestion des clés	44
A) <i>Protéger le réseau de l'entreprise</i>	45
A.1 Entre 2 sites : le réseau virtuel permanent.....	45
A.2 L'entrée du réseau : Firewalls et autres systèmes filtrants	45
B) <i>Protéger les données de l'entreprise par le chiffrement</i>	46
B.1 Les processeurs spécialisés et cartes accélératrices.....	46
B.2 Les boîtiers de chiffrement	47
B.3 Permettre l'accès à son réseau à partir de postes isolés ou nomades	48
C) <i>La carte à puce</i>	48
C.1 Bref historique	48
C.2 Le crypto-processeur garantit l'identité de l'utilisateur (carte ou clé à puce).....	50
C.3 La carte (ou clé USB) à puce, compagnon idéal de la PKI.....	50
C.4 Authentification Web	50
D) <i>Les autres moyens</i>	51
D.1 les HARD TOKEN	51
D.2 les SOFT TOKEN	51
D.3 La Biométrie	51
D.4 Une alternative non encore explorée ?	52
E) <i>Tableau de synthèse des moyens de sécurisation</i>	52
F) <i>Conclusion de cette partie</i>	53
QUATRIEME PARTIE : La mise en œuvre d'un projet d'IGC.....	54
<i>Une Brève introduction</i>	54
Définir, avant tout, une politique de sécurité	54
Appréhender toutes les facettes	54
L'IGC n'a de raison d'être que si les certificats sont utilisés.....	55
A) <i>Une politique d'ENTREPRISE</i>	56
A.1 L'autorité d'approbation des politiques (AAP).....	56
A.2 La politique de sécurité (PS).....	56
A.3 Une esquisse de plan de mise en chantier de la PS	57
A.4 La politique de certification (PC)	58
A.5 Déclaration des pratiques de certification (DPC)	59
A.6 Autre documents.....	59
A.7 Une ébauche de sommaire de la PC	60
B) <i>Les facettes du projet d'IGC</i>	61
B.1 Infrastructure technique	61
B.2 Intégration des applications	61
B.3 Organisation et processus	61
B.4 Exploitation	61
B.5 Marketing et communication.....	62
B.6 Juridique et légal.....	62
C) <i>Internalisation ou externalisation de l'IGC ?</i>	62

C.1 Externalisation.....	62
C.2 Internalisation.....	62
C.3 Solution hybride	62
C.4 Tendances et éléments du choix	63
<i>D) Ressources et coûts.....</i>	<i>64</i>
D.1 Coûts initiaux hors personnel.....	64
D.2 Coûts d'exploitation.....	64
D.3 Les ressources humaines	65
D.4 Les coûts du projet, estimation et répartition.....	65
D.5 Comparaison entre solution « achetée » et logiciel libre.....	66
D.6 La maîtrise des coûts	66
<i>E) L'IGC en CINQ expériences</i>	<i>67</i>
E.1 Ministère de la culture	67
E.2 AIRBUS	67
E.3 MAGIC AXESS	68
E.4 TÉLÉ TVA	68
E.5 Le GIP « Carte des Professionnels de Santé »	68
<i>F) Démarche de mise en oeuvre.....</i>	<i>69</i>
F.1 Phase de cadrage	69
F.2 Phase d'étude préalable.....	70
F.3 Phase de réalisation.....	70
F.4 Une ébauche de projet.....	71
<i>G) Synthèse et conclusion de cette partie.....</i>	<i>72</i>
CINQUIEME PARTIE : Des solutions en Open Source	74
Une définition.....	74
Des craintes concernant la sécurité : exemples connus	74
La réponse est le recours à l'Open Source.....	75
L'Open Source : conformité aux RFC ?	75
Les outils nécessaires	75
Vers une baisse des coûts ?	76
<i>A) Des projets Open Source.....</i>	<i>76</i>
A.1 Le projet EuPKI : http://www.gnupki.org	76
A.2 Le projet IDX-PKI : http://www.idealx.org	77
<i>B) EXPERIENCE pratique : importer un certificat</i>	<i>80</i>
B.1 A-t-on la capacité de codage en 128 bits ?	80
B.2 Réception du premier certificat	82
B.3 Premier message signé.....	84
<i>C) La maquette : INSA-TEST.....</i>	<i>85</i>
C.1 Préparation préliminaire	85
C.2 Fichiers de configuration.....	85
C.3 Les executables (batch)	87
C.4 Mode opératoire.....	92
C.5 Distribution des certificats utilisateurs, AC et LCR.....	92
C.6 Pourquoi doit-on avoir le certificat de l'AC ?	93
C.7 Format de la base de données	94

<i>D) Copies d'écran : chez l'utilisateur.....</i>	<i>94</i>
D.1 Installer son certificat personnel en 12 étapes	94
D.2 Réception du premier message signé	98
D.3 Envoi d'un message signé et crypté	100
D.4 Le carnet d'adresses	100
D.5 Réception d'un message crypté	101
<i>E) Conclusion de cette partie</i>	<i>102</i>
CONCLUSIONS.....	103
<i>A) Soyons pragmatiques : les recommandations</i>	<i>103</i>
A.1 Bref rappel : du côté des Prestataires	103
A.2 Du côté utilisateur	103
A.3 En cas de pertes, de vols ou de diffusion intempestive	104
A.4 Du choix du Mot de Passe	104
A.5 Si l'INSA prend une AC externe	105
A.6 Quelques mises au point.....	105
A.7 Les choix avant le déploiement	106
A.8 Mises en garde	107
<i>B) A titre personnel</i>	<i>108</i>
<i>En guise de conclusion générale</i>	<i>108</i>
ANNEXES	A
<i>Bibliographie.....</i>	<i>A</i>
<i>Liens Internet.....</i>	<i>H</i>
<i>Glossaire</i>	<i>H</i>
<i>Contenu du CDRom d'accompagnement.....</i>	<i>T</i>
<i>Lettre de Motivation et Curriculum Vitae.....</i>	<i>U</i>

ILLUSTRATIONS

Accès géographique aux INSA de Rouen	2
L'INSA de Mont St Aignan	2
L'INSA de St Etienne du Rouvray.....	2
Interconnexion RENATER / SYRHANO	3
Philippe WENDER	3
Liaison Inter Campus	3
L'exemple IDENTRUS.....	11
Certifications croisées	12
Point Focal	12
Obtention d'un certificat, schéma simplifié	12
Certificat dans Windows 98	13
Évaluation et certification des dispositifs de création de signature électronique	14
Qualification et contrôle des prestataires de services de certification électronique	14
Schéma de synthèse du modèle français de Qualification.....	14
LDAP : un annuaire global.....	22
Obtention d'un certificat : schéma complet	27
TCP / IP et sécurisation des échanges	28
IPSec et Politiques de sécurité.....	30
IPv4 à IPv6.....	33
Découpage des données dans SSL	34
SSL par rapport àTCP / IP et comparaison des modèles OSI/TCP	35
Etablissement d'une session dans SSL.....	36
Indicateur de connexion sécurisée dans les navigateurs	38
Nbre de clés à stocker.....	44
Le Virtual Private Network	45
Le PIX firewall de Cisco.....	45
Le FireBox.....	45
Accélérateur SSL d'AEP.....	47
Carte à puce SAGEM.....	48
Différent lecteurs de carte à puce.....	49
Une brève présentation	49
Quelques systèmes à puce.....	50
Un lecteur synchronisé.....	50
Générateurs de mots de passe à usage unique	51
Empreinte digitale	51
Lecteur d'empreintes digitales.....	52
Lecteur / encodeur	52
Clé sans contact COGES	52
Sommaire type d'une PC.....	60
Les facettes du projet	61
Répartition des choix pour la mise en œuvre d'une IGC.....	63
Ventilation du budget d'investissement d'un projet d'IGC	66
Démarche de mise en œuvre d'un projet d'IGC.....	69
Phase de Réalisation	71
Ebauche de planning sous MS Project	71
Une ébauche sous forme de Time Line (EuPKI)	72
Le consortium EuPKI.....	77
Guide Open Source d'IdealX	77
La iKey de Rainbow	78
Analogie Signature personnelle et Signature de l'AC	93
Réception du 1 ^{er} E-mail signé	98
Signature Numérique Vérifiée, certificat Utilisateur présent	99
Expédition d'un message signé et chiffré.....	100
Réception d'un message crypté	101
Règles élémentaires concernant le Mot de Passe	104

TABLES

Modèle d'IGC privé, avantages et inconvénients	10
Modèle d'IGC en réseau, avantages et inconvénients	10
Modèle de confiance de 1 à 5 coins, description	11
Cadres réglementaires divergents.....	15
Différents supports pour l'archivage : avantages et inconvénients	18
Certificat X509 : description des champs standards	19
La Cryptographie en France : obligations légales	25
Forces et faiblesses d'IPSec.....	31
Transition IPv4 à IPv6	33
Ports des protocoles liés à SSL.....	38
Cartes cryptographiques accélératrices	47
Risques comparés des moyens d'authentification	51
Tableau de synthèse des moyens de sécurisation.....	52
Quelques éléments pour le choix entre Internalisation ou Externalisation.....	63
Postes de coût d'un projet d'IGC.....	65
Comparaison logiciel libre / acheté.....	66
Open Source : les logiciels nécessaires	76
RFC applicables à IDX-PKI.....	79
Base de données des utilisateurs référencés (OpenSSL)	94