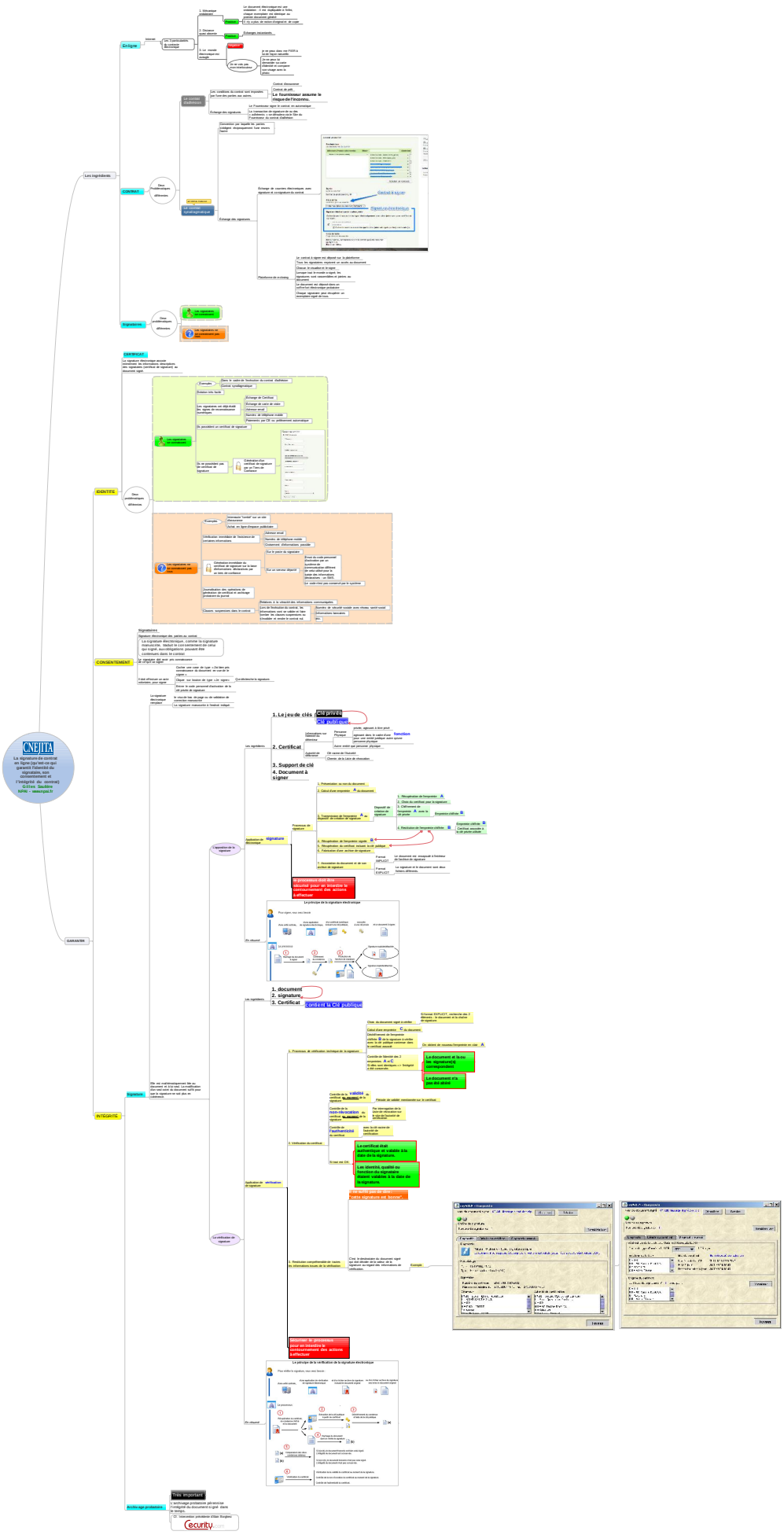
CNEJITA
La signature de contrat en ligne (qui lit-on qui signe, quelle valeur du signataire, son consentement et l'intégrité du contrat)
Gilles Sauton
NPM - www.npm.fr
Les ingrédients
Enjeux
Internet
Les transactions de contrats électronique
1. Mécanique d'abdication
Chaque
Le document électronique n'est ni
2. Distance quasi absente
Chaque
Échanges nécessaires
3. Le monde électronique est nouveau
Chaque
Je ne peux dans mes PC/PDA, ni en façon naturelle
Je ne peux le faire
Je ne peux le faire
Je ne suis pas
Je ne suis pas
Je ne suis pas
CONTRAT
Deux problématiques différentes
Le contrat d'adhésion
Les conditions du contrat sont imposées par l'une des parties aux autres
Contrat discussion
Contrat de gré
Le fournisseur assume le risque de l'inconnu.
Le Fournisseur signe le contrat en automatique
La connection de signature et du site
Échange des signatures
Connection par boutte de papier
Intégrant nécessairement l'une envers l'autre
Contrat Contract
Le contrat Contract
Échange des signatures
Échange de courriers électroniques avec signature et consignation du contrat
Contact à signer
Signer numériquement
Plateforme de stockage
Le contrat à signer est déposé sur la plateforme
Tous les signataires requises en accès au document
Choisir le situation et le signe
Les signataires sont responsables et paiers du document
Le document est déposé dans un coffre-fort électronique probatoire
Chaque signataire peut récupérer un exemplaire signé en ligne.
Signatures
Deux problématiques différentes
Les signatures ne consentent pas
Les signatures ne consentent pas
CERTIFICAT
Le signataire électronique associé (ensemble des informations d'exception des signataires (certificat de signature)) au document signé
Exemples
Dans le cadre de l'exécution du contrat d'adhésion
Contrat synallagmatique
Solution très facile
Échange de Certificat
Échange de codes de mêlé
Adresse email
Numéro de téléphone mobile
Paiements par CB ou prélèvement automatique
Ils possèdent un certificat de signature
Les signataires ne consentent
Ils ne possèdent pas de certificat de signature
Génération d'un certificat de signature par un Tiers de Confiance
ENTITÉ
Deux problématiques différentes
Exemples
Inscription "contrat" sur un site d'annonces
Achat en ligne d'espace publicitaire
Adresse email
Numéro de téléphone mobile
Vérification immédiate de l'existence de certaines informations
Contenant d'informations prédéfini
Sur le poste de signature
Les signataires ne consentent pas
Génération immédiate du certificat de signature sur la base d'informations présentes sur un tiers de confiance
Sur un serveur déporté
Envoi du code personnel d'activation par un moyen de communication différent
Sur la base d'une ou plusieurs autres informations détenues, un SMS
Le code n'est pas conservé par le système
Dématérialisation des opérations de signature, de consentement et de archivage probatoire de journal
Relatives à la vérification des informations communiquées
Clauses suspectes dans le contrat
Les de l'exécution du contrat, les informations sont se valide et bien ou mal, elle ne peut pas être invalidée et rendre le contrat nul
Bandes de sécurité sociale avec clicks sanitaire
Informations bancaires
Etc.
CONSENTEMENT
Signatures
Signature électronique des parties au contrat
La signature électronique, comme la signature manuscrite, traduit le consentement de celui qui signe, aux obligations pouvant être contenues dans le contrat
Le signataire doit avoir pris connaissance
Cocher une case de type « Je lisen pris connaissance du document en cas de le signer »
Cliquer sur bouton de type « Je signe »
Qu'est-ce-ce-ce la signature...
Il doit effectuer un acte volontaire, pour signer
Prévoir le code personnel d'activation de la clé privée de signature
Le signataire électronique accepter
le situation les de signe ou de validation de signature électronique
Les signature manuscrite à l'instant indique
GARANTIR
INTÉGRITÉ
Signature
Elle est «indéfinissablement liée au document» (Elle ne peut pas être modifiée, Elle rend nulle le document qu'elle peut que la signature ne soit plus en conformité)
L'opération de la signature
Les ingrédients
1. Le jeu de clés : Clé privée
Clé publique
Informations sur le signataire
Personne Physique
Fonction
Agissant dans le cadre d'une personne morale
Agissant dans le cadre d'une personne morale
Autre entité que personne physique
2. Certificat
Adjectif de Informations
Clé racine de l'Autorité
Chaînes de la Liste de révocation
3. Support de clé
4. Document à signer
Application de cryptographie
signature
1. Présentation au tiers du document
2. Calcul d'une empreinte du document
Processus de signature
3. Transmission de l'empreinte signée au
Dépendant de l'utilisation de signature
1. Récupération de l'empreinte
2. Déchiffrement du hash pour la signature
3. Calcul de l'empreinte avec la clé publique
Empreinte calculée
4. Prévisualisation de l'empreinte calculée
Empreinte calculée
Certificat associée à la clé publique utilisée
4. Récupération de l'empreinte signée
5. Récupération du certificat incluant la clé publique
6. Fabrication d'une archive de signature
Format ASN.1/DER
Le document est encapsulé à l'intérieur de l'archive de signature
7. Annotation du document et de son archive de signature
Format ASN.1/DER
La signature et le document sont deux fichiers différents.
Il convient dès lors de mettre en place un processus dont le déroulé pour et interdire le contournement des actions à effectuer
La principe de la signature électronique
Pour signer, vous avez besoin
Avec cette clefs...
Avec application de signature électronique
Avec un certificat contenant informations d'identification
associée à cette clé privée
et un document à signer
En résumé
Le processus
Signature numérisée
Signature numérisée
La vérification de signature
Les ingrédients
1. document
2. signature
3. Certificat : Contient la Clé publique
Clefs du document signé à vérifier
Format ASN.1/DER : rechercher des 2 éléments : le document et la chaîne de signature
Calcul d'une empreinte du document
Déchiffrement de l'empreinte chiffrée de la signature à vérifier avec la clé publique du signataire contenue dans le certificat associé
Du dépend de nouveau l'empreinte en clair
Contrôle de fidélité des 2 empreintes A et C
Le document et la sa ne signature(s) correspondent
Le document n'a pas été altéré
1. Processus de vérification technique de la signature
Contrôle de la validité de la signature
Contrôle de la non-révocation du certificat
Contrôle de l'intégrité du certificat
Période de validité mentionnée sur le certificat
Par interrogation de la liste de révocation sur le site de l'autorité de certification
avec la clé racine de l'autorité de certification
2. Vérification du certificat
Si tout est OK
Le certificat était authentique et valable à la date de la signature.
Les identité, qualité ou fonction du signataire étaient valables à la date de la signature.
"Cette signature est bonne"
3. Résolution compréhensible de toutes les informations issues de la vérification
Crée la destination du document signé (signature) et rassemble des informations de vérification
Exemple
Il convient dès lors de mettre en place un processus dont le déroulé pour et interdire le contournement des actions à effectuer
La principe de la vérification de la signature électronique
Pour vérifier la signature, vous avez besoin
Avec application de vérification de signature électronique
et du document signé
Avec la clé publique associée à la clé privée ayant servi à la signature
et du document signé
En résumé
Le processus
Archivage probatoire
Très important
L'archivage probatoire pérennise l'intégrité du document et gère dans le temps
Un système probatoire d'Alain Bensoussan
security.com