

Statut du document	Guide interne du gouvernement fédéral américain
Titre	<i>Federal Agency Use of Public Key Technology for Digital Signatures and Authentication.</i>
Mot clé	Attestation et sécurité
Source	NIST (<i>National Institute of Science and Technology</i>) http://csrc.ncsl.nist.gov/publications/nistpubs/800-25/sp800-25.pdf
Date de publication	Octobre 2000
Nombre de pages	30
Langue	Anglais
Lien avec autres normes	Recours aux normes ouvertes telles X.509 et XML. Un des éléments du Cadre de gestion en technologie de l'information, « A-130 » (voir http://www.cio.gov/text/Recompiled_A-130.htm) qui s'appuie notamment sur le <i>Government Paperwork Elimination Act</i> .
Situation actuelle	
Description	<p>Ce document du NIST, institution fédérale américaine, est un guide ayant pour but d'aider les organismes gouvernementaux à bien utiliser une ICP (infrastructure à clé publique), que ce soit à des fins d'authentification, ou à des fins de signature numérique, ou aux deux. Ce document fait partie d'un ensemble de dispositions légales et administratives orientant l'usage des technologies de l'information par l'administration gouvernementale : Justice aide sur les questions légales liées aux transactions électroniques, le Trésor voit aux politiques et règles quant aux techniques d'authentification et de transaction dans les paiements et encaissements gouvernementaux, les Archives (NARA) orientent les pratiques en matière de gestion, de conservation et de disposition de documents signés numériquement; le NIST a, quant à lui, pour rôle d'indiquer comment les organisations gouvernementales doivent établir les coûts, les bénéfices et les risques qu'il y a à se mettre à adopter des processus électroniques.</p> <p>Là où il y a un besoin de sécurité pour une transaction, il faut que les parties interagissant soient identifiées et authentifiées, que l'intégrité de l'information soit garantie, qu'il y ait une garantie technique de non-répudiation (responsabilité du signataire sur contenu), et que la confidentialité de l'information soit protégée. Le déploiement ordonné d'une ICP est capable de satisfaire toutes ces exigences dans un contexte de réseau public. La participation à des projets pilotes est fortement encouragée afin de s'assurer d'inclure dans les arrangements de l'ICP tous les scénarios d'utilisation pour les affaires du gouvernement, à l'interne et avec la clientèle. Le document cite pour modèles les secteurs automobiles, bancaires, de la santé qui, aux Etats-Unis du moins, sont en voie de structurer de vastes ICP dans leur secteur industriel. La relation client-gouvernement implique cependant des renseignements variés, abondants et, souvent, très intimes qui font que la protection des renseignements personnels est un enjeu sensible.</p> <p>Quand les organisations gouvernementales veulent utiliser une ICP, elles doivent d'abord envisager les formules proposées dans l'administration sous formes de contrats préconçus auprès de fournisseurs certifiés (programme ACES). Le reste du document est consacré à la présentation d'une structure de questionnement visant à aider les organisations gouvernementales à prendre ces décisions sur le quoi, le quand et le comment d'utiliser une ICP. Cinq points sont à évaluer :</p> <ol style="list-style-type: none"> 1- les bénéfices de l'utilisation d'une ICP : les bénéfices peuvent sembler provenir du simple fait de recourir à des processus d'affaires électroniques, mais en fait la sécurité qu'une ICP permet d'apporter à ces processus en est une condition préalable essentielle. Les principales sources de bénéfices à rechercher sont les gains de temps, les réductions de coût, l'amélioration du service, le gain de qualité et d'intégrité des données. 2- les coûts : il faut envisager le cas du simple ajout de la signature numérique à des applications existantes ainsi que le cas de la transformation d'un processus papier en un processus électronique, et les coûts d'opération une fois que cette conversion est faite. L'établissement des coûts doit être fait en tenant compte : <ul style="list-style-type: none"> - du niveau de confiance ou de fiabilité qui est requis en contexte (nature des transactions et des menaces, conventions établies, etc.). - des obligations de gestion aptes à assurer l'intégrité des clés publiques et privées,

	<p>ceci étant notamment lié à la façon de se doter ou d'acquérir les services d'ICP en distinguant l'enregistrement de la certification initiale du service de répertoire pour validation à la demande des applications.</p> <ul style="list-style-type: none"> - les risques potentiels doivent être évalués en comparant ce qu'ils seraient avec une ICP par rapport à ce qu'ils sont avec les processus existants (soit papier, soit électroniques avec un simple mot de passe). - l'obligation de concevoir une Politique de certification prévoyant le détail institutionnel et technique de la vérification d'identité, de l'émission de certificats, de leur utilisation, de leur révocation. Il faut examiner les exigences de signature des documents utilisés à l'interne et avec l'externe, la vérification et l'audit, la protection des renseignements personnels dans divers processus et dans les données enregistrées en lien avec l'ICP elle-même, les exigences de conservation administratives et juridiques, les obligations du détenteur qui utilise un certificat de clé publique. - la possibilité pratique de connecter les applications avec les serveurs <p>3- les risques : l'évaluation des risques doit procéder en comparant les risques traditionnels associés à procéder avec le papier avec la nouvelle situation possible en recourant aux transactions électroniques avec une ICP. Trois formes de risques sont mentionnées : la fraude, l'interruption de service et la responsabilité. Les points critiques liés à l'ICP sont l'établissement d'identité préalable à l'émission de certificat et la protection de sa clé privée par chacun. Dans les applications offertes aux clients, il faut que ce qui est signé soit clairement délimité et que le client sache très bien quelle responsabilité il assume en signant (clicquant).</p> <p>4- comment comparer bénéfices, coûts et risques dans la prise de décision ? si l'ICP est une condition essentielle pour des services électroniques en pouvant donner confiance à leurs clients, la barrière de coûts est vite abaissée. Il faut considérer que l'ICP servira autant à des fins de sécurité internes qu'externes, dans une variété d'applications importantes où justement les besoins de sécurité sont grands.</p> <p>5- les grandes questions d'implantation : un déploiement d'ICP est une affaire d'envergure requérant beaucoup de planification. Une douzaine de questions sont soulevées pour en faciliter l'exécution :</p> <ul style="list-style-type: none"> - politique de certification, définition des services essentiels de répertoire, définition des conditions d'échange avec l'externe, relier toute application opportune avec l'ICP, y aller par étapes, associer les procédures de l'ICP aux procédures administratives existantes en gestion des ressources humaines et financières par exemple, identifier les exigences de validation synchrones (en ligne) ou via des listes de révocation, bien intégrer le fonctionnement technique de l'ICP avec les pare-feu, vérification et audit, archivage à long terme...
--	---

Remarque

Lexique anglais-français

Rédacteur : Richard Parent
Organisation source : Secrétariat du Conseil du trésor
Date de publication : 16 janvier 2001
Raison d'être : Connaissance technologique
Programme gouvernemental : Inforoutes et ressources informationnelles
Nom du modificateur :
Date de dernière modification :
Note numéro : 87