

**Recommandation de l'OCDE sur
l'authentification électronique et
Orientations pour l'authentification électronique**

juin 2007



www.oecd.org/sti/securitevieprivee

**Recommandation de l'OCDE
sur l'authentification électronique
et
Orientations pour l'authentification électronique**



ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

L'OCDE est un forum unique en son genre où les gouvernements de 30 démocraties œuvrent ensemble pour relever les défis économiques, sociaux et environnementaux, que pose la mondialisation. L'OCDE est aussi à l'avant-garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu'elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et les défis posés par le vieillissement de la population. L'Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays membres de l'OCDE sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, l'Italie, le Japon, le Luxembourg, le Mexique, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Suède, la Suisse et la Turquie. La Commission des Communautés européennes participe aux travaux de l'OCDE.

Les Éditions OCDE assurent une large diffusion aux travaux de l'Organisation. Ces derniers comprennent les résultats de l'activité de collecte de statistiques, les travaux de recherche menés sur des questions économiques, sociales et environnementales, ainsi que les conventions, les principes directeurs et les modèles développés par les pays membres.

Cet ouvrage est publié sous la responsabilité du Secrétaire général de l'OCDE.

© OCDE 2007

Toute reproduction, copie, transmission ou traduction de cette publication doit faire l'objet d'une autorisation écrite.

Les demandes doivent être adressées aux Éditions OCDE : rights@oecd.org

Avant propos

La Recommandation sur l'authentification électronique et les Orientations pour l'authentification électronique ont été développées par le Comité de la politique de l'information, de l'informatique et des communications (PIIC) de l'OCDE via son Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP). Les travaux ont été menés par Jane Hamilton d'Industrie Canada avec le soutien de délégués de l'Australie, de la France, de la Hongrie, de la Norvège et des Etats-Unis, du Secrétariat de l'OCDE et du Comité Consultatif Économique et Industriel auprès de l'OCDE (BIAC). Le projet de Recommandation a été adopté en tant que Recommandation par le Conseil de l'OCDE le 12 juin 2007. Les Orientations pour l'authentification électronique ont été adoptées par le Comité PIIC en avril et déclassifiées par le Conseil le 12 juin 2007.

Table des matières

Préface	5
Recommandation du Conseil sur l'authentification électronique	7
Orientations de l'OCDE pour l'authentification électronique.....	13
Introduction.....	13
Objet de ces orientations.....	13
L'authentification dans son contexte	14
Importance de l'authentification.....	16
Principes pour l'authentification électronique	17
Remarques importantes concernant les Principes	17
Concepts et terminologie.....	18
Partie A – Principes fondateurs	20
Partie B –Principes opérationnels	22
Questions en suspens	24
References	26
Appendice A Historique des travaux de l'OCDE sur l'authentification (1998 – 2005).....	29
Appendice B Niveaux d'assurance de l'authentification	33

Préface

L'authentification électronique apporte un niveau d'assurance pour déterminer si quelqu'un ou quelque chose est ce qu'il ou elle prétend être dans un environnement numérique. Ainsi, l'authentification électronique joue un rôle fondamental dans l'établissement de relations de confiance pour le commerce électronique, l'administration électronique et de nombreuses autres interactions sociales. Elle constitue également une composante essentielle de toute stratégie visant à protéger les systèmes d'information et les réseaux, les données financières, les informations personnelles et autres avoirs contre des accès non autorisés ou le vol d'identité. L'authentification électronique est par conséquent essentielle pour établir la responsabilité en ligne.

L'importance de l'authentification pour l'administration électronique et le commerce électronique mondial a été reconnue en 1998 par les ministres de l'OCDE lors de la Conférence ministérielle « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial » qui s'est tenue à Ottawa, Canada¹. Dans leur « Déclaration sur l'authentification pour le commerce électronique », les ministres ont souligné un certain nombre d'actions destinées à promouvoir le développement et l'utilisation des technologies et mécanismes d'authentification électronique. L'un des aspects importants comprenait la nécessité d'élaborer des approches cohérentes de l'authentification électronique pour faciliter le commerce électronique transfrontalier.

L'OCDE a mené plusieurs initiatives afin de soutenir les efforts des pays Membres pour mettre en œuvre la Déclaration ministérielle. Il a en particulier œuvré pour relever deux défis importants : accroître la confiance dans les processus et opérateurs d'authentification et faire tomber les obstacles à l'utilisation de l'authentification transfrontalière. En 1999, un atelier conjoint de l'OCDE et du secteur privé a été organisé pour faciliter le dialogue entre toutes les parties prenantes². Il a été suivi en 2000 par le développement d'un « Inventaire des approches d'authentification électronique et de certification dans une société mondiale en réseau »³ et d'un rapport sur les « Progrès réalisés à la suite de la Déclaration d'Ottawa sur l'authentification pour le commerce électronique »⁴. Des travaux plus récents comprennent une « Enquête sur l'environnement législatif et le cadre des politiques concernant les services

-
1. SG/EC(98)14/FINAL
[www.oilis.oecd.org/olis/1998doc.nsf/linkto/sg-ec\(98\)14-final](http://www.oilis.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final)
 2. DSTI/ICCP/REG(99)14/FINAL
[www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg\(99\)14-final](http://www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)14-final)
 3. DSTI/ICCP/REG(99)13/FINAL
[www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg\(99\)13-final](http://www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final)
 4. DSTI/ICCP/REG(2001)10/FINAL
[www.oilis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg\(2001\)10-final](http://www.oilis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg(2001)10-final)

d'authentification électronique et les signatures électroniques »⁵ réalisée en 2003 ainsi qu'un rapport sur « L'usage transfrontalier de l'authentification »⁶, finalisé en 2005.

En 2006 et sur la base de ces travaux, le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) du Comité de la politique de l'information, de l'informatique et des communications (PIIC) a lancé la préparation d'un document comportant des orientations politiques et pratiques pour l'élaboration, la mise en œuvre et l'utilisation des produits et services d'authentification des personnes et des entités.

Ces orientations présentent le contexte et l'importance de l'authentification électronique pour le commerce et l'administration électroniques et fournissent un certain nombre de principes fondateurs et opérationnels qui constituent un dénominateur commun pour l'interopérabilité entre les différentes juridictions. Leur objectif est d'aider les pays Membres et les économies non Membres à établir ou, le cas échéant, amender leurs approches de l'authentification électronique afin de faciliter la co-opération transfrontalière. Ces orientations tiennent compte des travaux menés dans d'autres enceintes, et notamment des travaux de la Coopération économique Asie-Pacifique (APEC) concernant les éléments requis pour les services d'authentification transjuridictionnels. Certaines approches nationales de l'authentification ont également été utilisées comme une base supplémentaire.

Ces orientations ont servi de base à la Recommandation du Conseil sur l'authentification électronique qui réaffirme le rôle important de l'authentification électronique pour l'établissement de la confiance en ligne et la poursuite du développement de l'économie numérique. La Recommandation encourage les pays Membres à poursuivre leurs efforts pour établir des approches pour une authentification électronique efficace des personnes et des entités au niveau national et transfrontalier qui soient compatibles et technologiquement neutres.

La Recommandation et les Orientations concluent un ensemble de travaux conduits à la suite de la "Déclaration sur l'authentification pour le commerce électronique" adoptée par les Ministres à la Conférence ministérielle d'Ottawa tenue du 7 au 9 octobre 1998 et établissent un pont avec les futurs travaux de l'OCDE sur la gestion de l'identité.

La Recommandation et les Orientations devraient contribuer aux discussions en cours et à venir dans d'autres enceintes internationales, telles que la Coopération économique Asie-Pacifique (APEC), la Commission des Nations Unies pour le droit commercial international (CNUDCI) ainsi que les organisations nationales et régionales de standardisation.

5. DSTI/ICCP/REG(2003)9/FINAL
[www.oilis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg\(2003\)9-final](http://www.oilis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)9-final)

6. DSTI/ICCP/REG(2005)4/FINAL
[www.oilis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg\(2005\)4-final](http://www.oilis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg(2005)4-final)

Recommandation du Conseil sur l'authentification électronique

Recommandation du Conseil sur l'authentification électronique

LE CONSEIL,

Vu l'Article 5 b) de la Convention relative à l'Organisation de Coopération et de Développement Économiques, en date du 14 décembre 1960 ;

Vu l'article 18 b) du Règlement de procédure ;

Vu la Déclaration sur l'authentification pour le commerce électronique [C(98)177] ;

Vu la Recommandation du Conseil concernant les Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité [C(2002)131/FINAL], ci-après les « Lignes directrices pour la sécurité des systèmes d'information et des réseaux » ;

Vu la Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel [C(80)58/FINAL] ;

Reconnaissant que la confiance est une condition essentielle pour la conduite de nombreuses transactions en ligne et que, dans un cadre plus général de mesures et de stratégies, l'authentification électronique des personnes et entités joue un rôle important à cet égard ;

Reconnaissant que l'authentification électronique, qui est une composante essentielle de la vérification et de la gestion des identités en ligne, fournit un degré d'assurance quant à la réalité de ce que l'autre partie prétend être et, partant, qu'elle réduit l'incertitude inhérente aux interactions et transactions électroniques au plan intérieur et transfrontières ;

Reconnaissant qu'une authentification électronique efficace contribue à renforcer la sécurité des systèmes et des réseaux ainsi que la vie privée en réduisant les risques tels que l'accès non autorisé à des données de caractère personnel, le vol d'identité et la compromission de données, et en fournissant des moyens additionnels d'imputabilité ;

Reconnaissant que l'authentification électronique est un élément important dans la poursuite du développement des activités gouvernementales et autres activités sociales et individuelles en ligne, qu'elle ouvre de nouvelles perspectives économiques, qu'elle contribue au développement du commerce électronique et qu'elle est un élément essentiel d'un Internet viable et pérenne ;

Reconnaissant finalement que cette Recommandation prend en compte les questions d'authentification électronique des personnes et des entités mais non d'autres aspects de l'authentification électronique tels que la valeur juridique des documents ou des signatures électroniques ;

Sur la proposition du Comité de la politique de l'information, de l'informatique et des communications :

RECOMMANDE que les pays Membres :

- Oeuvent pour l'instauration d'approches technologiquement neutres pour une authentification électronique efficace des personnes et des entités au plan intérieur et transfrontières, dans le respect des Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information et des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel.
- Favorisent la mise au point, la fourniture et l'utilisation de produits et services d'authentification qui intègrent de solides pratiques commerciales, notamment des garanties techniques et non techniques répondant aux besoins des participants, s'agissant particulièrement de la sécurité et de la confidentialité de leurs informations et identités.
- A la fois dans le secteur public et privé, encouragent la compatibilité commerciale et juridique et l'interopérabilité technique des dispositifs d'authentification afin de faciliter les interactions et transactions transsectorielles et transjuridictionnelles en ligne et de permettre que les produits et services d'authentification puissent être déployés aux niveaux à la fois national et international.
- Prennent des mesures pour mieux sensibiliser tous les participants, y compris dans les économies non Membres, aux avantages de l'utilisation de l'authentification électronique aux niveaux national et international.

RAPPELLE les orientations sur l'authentification électronique [DSTI/ICCP/REG(2006)3/REV3], qui peuvent aider les pays Membres à élaborer des approches efficaces et compatibles à l'égard de l'authentification électronique aux niveaux tant national qu'international.

INVITE les économies non Membres à prendre en compte la présente Recommandation.

CHARGE le Comité de la politique de l'information, de l'informatique et des communications de suivre les évolutions liées à l'authentification électronique dans les pays Membres de l'OCDE et dans les autres enceintes internationales, et de réexaminer cette Recommandation dans les trois années suivants son adoption, et par la suite, en tant que de besoin.

Orientations de l'OCDE pour l'authentification électronique

Orientations de l'OCDE pour l'authentification électronique

Introduction

L'authentification couvre un très large éventail de notions différentes. Toutefois, les travaux de l'OCDE se concentrent sur l'authentification des personnes (physiques ou morales). L'OCDE a commencé à examiner l'authentification dans le cadre de ses travaux sur le commerce électronique. Dès l'origine, l'OCDE s'est rendu compte que le commerce électronique transcende le temps et l'espace et se produit souvent sans médiation humaine. Ainsi, la nécessité d'identifier convenablement les parties à une transaction est apparue comme essentielle pour développer la confiance dans le commerce électronique. Aujourd'hui, on peut considérer ces questions dans le cadre plus général de la gestion de l'identité qui devient un élément de fonctionnement essentiel du fonctionnement de l'économie numérique et de la société de l'information.

Objet de ces orientations

Le présent document d'orientations:

- Présente le contexte et l'importance de l'authentification.
- Définit un ensemble de principes formant un cadre pour la création, la mise en œuvre et l'utilisation de produits et services d'authentification de personnes ou entités. Les principes traitent également les défis de l'authentification par delà les frontières.
- Enumère les questions en suspens relatives à l'utilisation de l'authentification.

Ces orientations seront utiles aux pays Membres ou non Membres de l'OCDE pour établir leurs approches à l'égard de l'authentification et aideront les pays qui ont déjà établi des politiques à discerner et aborder des modifications possibles à leur approche. S'il est bien entendu que les pays Membres doivent se conformer aux dispositions légales en vigueur dans leur juridiction, les orientations offrent néanmoins un dénominateur commun qui ouvre des possibilités pour l'interopérabilité transjurisdictionnelle.

En plus d'orientations sur l'authentification électronique auquel peuvent se référer les pays Membres de l'OCDE et les économies non Membres, ce document offre aussi un inventaire des instruments et des mécanismes qui ont contribué aux travaux et aux constatations du GTSIVP dans ce domaine. Ainsi, outre un élément utile pour une juridiction donnée, il peut aussi servir pour les discussions en cours ou futures dans des enceintes internationales comme le Telecommunications and Information Working Group et l'Electronic Commerce Steering Group de l'APEC, la CNUDCI et les organisations de normalisation nationales, régionales et internationales, entre autres.

Enfin, et bien qu'il ait principalement pour objet d'offrir, au sujet de l'authentification, des orientations politiques et pratiques sur la base des travaux de l'OCDE réalisés à ce jour, ce document identifie les questions en suspens que l'OCDE considère comme encore nécessaires à traiter par les pays Membres et les autres enceintes internationales.

Sur cette base, le présent document :

- Réunit quelques-uns des résultats des travaux de l'OCDE sur l'authentification réalisés jusqu'à présent.
- Offre un ensemble général d'indications sur certaines questions relativement complexes concernant l'authentification.
- Met en lumière les points sur lesquels il pourrait être approprié que l'OCDE ou d'autres organismes conduisent d'autres travaux.

L'authentification dans son contexte

L'authentification peut avoir différentes significations suivant le contexte dans lequel on utilise ce terme. Une recherche sur Internet sur le terme "authentification" produit un très large éventail de définitions, certaines concernant l'authentification des personnes ou autres entités, d'autres concernant des choses, des documents ou des systèmes. Dans ces définitions, l'authentification s'accomplit par des processus ayant divers degrés de détail et de spécificité technique. Ces processus ont pour but de déterminer si quelqu'un ou quelque chose est bien en réalité la personne ou la chose qu'il prétend être. Ainsi, une authentification efficace contribue de manière essentielle à l'établissement d'une relation de confiance dans un environnement numérique. Pour les besoins des présentes orientations, l'authentification est définie comme :

Une fonction destinée à établir la validité et l'assurance de l'identité déclarée par un utilisateur, un dispositif ou une autre entité dans un système d'information ou de communications. Le fait d'apporter une assurance de l'identité déclarée par une entité.

Cette définition implique deux processus et un résultat :

- Une déclaration concernant une personne, une autre entité ou une chose est présentée (processus de déclaration).
- Cette déclaration est corroborée (processus de corroboration).
- En conséquence, un certain degré de confiance, ou de manque de confiance, en cette déclaration est généré.

L'authentification n'est pas une fin mais un sous-processus dans un système de sécurité et qui doit fonctionner en conjonction avec des processus d'autorisation, de gestion des droits, de contrôle d'accès et d'audit. L'authentification dépend de la corroboration d'un ou plusieurs des facteurs suivants : quelque chose que le déclarant sait (par exemple, un secret partagé tel qu'un mot de passe), quelque chose que le déclarant a (par exemple, un jeton ou « token ») ou quelque chose que le déclarant est (par exemple, une caractéristique biométrique ou un ensemble d'attributs comme la taille, l'âge et le poids). Une fois qu'une personne, une autre entité ou une chose a été authentifiée (par exemple, quand la déclaration présentée est valide), diverses choses peuvent être rendues possibles. Par exemple, dans le cas de l'authentification d'un individu, certains droits peuvent être attribués à cet individu authentifié (processus d'autorisation), avec les responsabilités qui peuvent être associées à l'exercice de ces droits. L'authentification peut être bidirectionnelle et apporter une assurance⁷ aux deux parties dans une transaction.

Le plus souvent, dans le cas de l'authentification d'une personne, il s'agit d'authentifier l'identité de cette personne. Toutefois, dans certaines circonstances, le but est d'authentifier un attribut relatif à une personne plutôt que son identité. Par exemple, dans certaines transactions en ligne, l'authentification sert à vérifier que les visiteurs d'un site Web ont un certain âge minimum prescrit par la loi. Dans ce genre de cas, l'attribut – l'âge (quelque chose

7. Voir Appendice B, Niveaux d'assurance de l'authentification.

que le client est) – est le point principal de l'authentification. Il est donc possible d'utiliser des technologies d'authentification électronique pour authentifier des attributs sans donner d'information sur l'identité.

L'assurance d'un certain degré d'anonymat peut aussi jouer un rôle important en faveur de la confiance dans les systèmes en ligne. Les technologies d'authentification qui ne recueillent pas d'informations à caractère personnel peuvent garantir que les informations qui, dès l'abord, ne sont pas nécessaires à la transaction ne seront pas collectées ni utilisées à une autre fin ultérieurement. S'abstenir tout simplement d'utiliser l'authentification quand elle n'est pas nécessaire est un autre moyen de contribuer au développement de la confiance des utilisateurs.

L'authentification des documents existe depuis longtemps avec la certification devant notaire et les méthodes qui l'ont précédée, mais de nouvelles formes d'authentification électronique des documents sont aussi en cours de mise au point. Dans le monde physique, cela peut nécessiter la présence de la personne concernée et la présentation d'un justificatif d'identité portant une signature et une photographie. Dans l'environnement en ligne, il existe divers moyens nouveaux de créer des justificatifs numériques. Ces justificatifs peuvent servir à authentifier des personnes (ou entités) et ils peuvent permettre de "signer" électroniquement des documents. L'utilisation de signatures électroniques afin de produire un effet juridique équivalent aux signatures manuscrites soulève un certain nombre de questions traitées par la Loi type de la CNUDCI sur les signatures électroniques de 2001. Les pays Membres de l'OCDE apportent leur soutien à l'utilisation des signatures électroniques de façon équivalente aux signatures manuscrites, et ils préconisent une neutralité à l'égard des technologies dans leur utilisation.

La complexité est encore accrue quand interviennent un ensemble automatisé d'agents logiciels et l'authentification de systèmes ou de machines. Beaucoup de concepts juridiques reposent sur la notion d'intention entre des acteurs humains. On ne sait alors pas très bien comment transposer l'intention et assigner une obligation à des transactions dépourvues de médiation humaine.

Dans les environnements numériques, l'authentification soulève d'autres questions complexes et de multiples défis. Certaines de ces questions concernent la façon de définir et de saisir l'identité de manière à promouvoir la confiance dans un environnement virtuel où tout aspect doit être formalisé afin de permettre un traitement automatisé. Si, à de nombreux égards, ces questions sont les mêmes que dans le monde physique, le degré accru d'ambiguïté, auquel s'ajoutent de sérieuses menaces pour la sécurité dans l'environnement en ligne, introduit une nouvelle complexité qu'il convient de traiter. On peut considérer les défis comme technologiques (par exemple, interopérabilité, sécurité), juridiques (par exemple, reconnaissance juridique, responsabilité, vie privée) ou économiques (par exemple, coût de déploiement et d'utilisation). Il peut y avoir de larges variations entre les mises en oeuvre sectorielles, ce qui contribue aussi à accroître la complexité. L'ampleur et la rapidité des innovations technologiques compliquent encore ces problèmes.

Le fait que les approches à l'égard de l'authentification se soient développées de manière sectorielle ou application par application (ou service) et dans des conditions de propriété exclusive est une difficulté supplémentaire. Afin d'exploiter quelques unes des économies d'échelle qui peuvent être essentielles pour la viabilité économique des fournisseurs de services d'authentification, il faut identifier les points communs entre les applications. Ces défis illustrent la nécessité d'adopter une démarche plus complète et globale à l'égard du problème de la confiance et d'explorer des approches sûres, respectueuses de la vie privée, efficaces et commodes pour la gestion des identités en ligne, afin de tirer le meilleur profit de l'environnement en ligne. On espère que les futurs travaux de l'OCDE sur la gestion de l'identité faciliteront la résolution de quelques unes des questions précédemment mentionnées, telles que ce caractère sectoriel ou compartimenté des approches à l'égard de l'authentification.

Il est nécessaire d'améliorer constamment les mécanismes d'authentification pour garder l'avantage sur les nouvelles formes de fraude (par exemple, des justificatifs sont volés et utilisés pour commettre des fraudes ou autres délits). Il est donc souhaitable que les méthodes d'authentification mises en œuvre aient la capacité d'exploiter ultérieurement des technologies d'authentification futures plus robustes. L'utilisation croissante de l'authentification multifactorielle, ainsi que l'utilisation de la biométrie (par exemple, lecture de l'iris ou empreintes digitales), est un exemple de cette tendance.

L'existence de modèles d'entreprise viables pour les services d'authentification est une condition préalable pour le développement et l'utilisation durables de nouvelles méthodes d'authentification. Ces modèles doivent prendre en compte les caractéristiques spécifiques du marché de l'authentification, où les effets de réseau⁸ et les effets de marché à deux côtés⁹ sont prépondérants.

Il importe de comprendre la vaste complexité des questions qui entourent l'authentification, aussi bien du point de vue des relations mutuelles avec les autres systèmes et procédures que de la diversité des utilisations possibles. Cette présentation avait pour objectif d'éclairer quelque peu le contexte de ces orientations. Toutefois, le champ des principes proposés se limite aux aspects découlant des travaux réalisés jusqu'à présent par l'OCDE sur l'authentification, qui visent deux des défis majeurs de l'authentification : la confiance dans les processus et dans les opérateurs d'authentification, et les problèmes que les parties se fiant à l'authentification peuvent rencontrer au-delà des frontières. Dans la mesure où l'authentification est une composante de base de tout processus ou système de gestion de l'identité, les principes ci-dessous établissent un "pont" entre les travaux de l'OCDE sur l'authentification qui ont maintenant atteint un certain degré de maturité et les travaux naissants sur le sujet plus général de la gestion de l'identité. Un historique de ces travaux depuis la "Déclaration sur l'authentification pour le commerce électronique", et un résumé des enquêtes, rapports et ateliers réalisés par l'OCDE sont présentés dans l'Appendice A. On trouvera la liste des documents de l'OCDE relatifs à l'authentification depuis 1998 dans la section Références à la fin du présent document.

Importance de l'authentification

Les entreprises, les gouvernements et les individus ont tous des données et avoirs sensibles à protéger. On a besoin d'assurance notamment dans le cas de transferts monétaires, ou quand on fait des déclarations comportant un engagement juridique, ou quand des transactions entraînent la divulgation d'informations à caractère personnel. En fournissant un certain degré d'assurance concernant l'identité déclarée par les parties engagées dans une relation en ligne, l'authentification réduit l'incertitude inhérente aux transactions à distance, développant ainsi la confiance dans les interactions électroniques, et elle participe à la lutte plus générale contre les activités délictueuses et autres menaces en ligne.

L'authentification est un élément d'un système plus large de pratiques, procédures et mises en œuvre techniques, qui fonctionnent ensemble pour sécuriser les systèmes d'information, les réseaux et les communications électroniques qu'ils véhiculent. Les Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité¹⁰ reconnaissent le caractère d'interdépendance de ces systèmes et

-
8. Suivant lesquels l'utilité d'un produit donné (par exemple, le télécopieur) augmente avec le nombre de participants qui l'utilisent.
 9. Cela signifie que le marché de l'authentification comporte au moins deux types de produits ou services qui sont complémentaires (c'est-à-dire les justificatifs ou services d'authentification et les applications qui les utilisent). Les deux sont nécessaires pour que le marché fonctionne.
 10. Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité. <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

soulignent la nécessité d'adopter une approche globale et cohérente à l'égard de la sécurité des systèmes si l'on veut atteindre les objectifs organisationnels de sécurité, mettre en œuvre les politiques et établir une culture de la sécurité. Étant donné que l'authentification forme la base de la plupart des types de contrôle d'accès et des méthodes permettant d'établir une responsabilité en ligne, il convient de la considérer comme une composante essentielle de la sécurité de l'information. En outre, une authentification efficace contribue à la protection de la vie privée en réduisant les risques tels que l'accès non autorisé à des informations à caractère personnel ou le vol d'identité.

Plus généralement, l'authentification est un outil essentiel pour établir la confiance et protéger l'identité en ligne, facteurs primordiaux pour promouvoir le commerce et l'administration électroniques.

Principes pour l'authentification électronique

Les Principes contenus dans le présent document visent à faire en sorte que les produits et services d'authentification reflètent de saines pratiques d'entreprise et de marché, répondent aux besoins des utilisateurs, tendent vers l'interopérabilité dans toute la mesure possible et soient acceptés internationalement. Ils servent de repères pour la création, la fourniture et l'utilisation de services d'authentification opérant au niveau national ou international. De cette façon, ces Principes visent à faciliter les communications électroniques transfrontières.

Ces Principes ont été élaborés afin d'établir une approche cohérente de l'évaluation des risques inhérents aux transactions électroniques et une base de comparaison pour des mécanismes qui reposent sur des technologies très différentes. Sur cette base, ces Principes visent à promouvoir la compatibilité de schémas d'authentification différents. Les pays Membres de l'OCDE sont invités à prendre ces Principes en considération dans leurs approches nationales à l'égard de l'authentification électronique. Ces Principes peuvent aussi constituer une base pour des initiatives volontaires spécialement adaptées aux besoins d'industries particulières.

Remarques importantes concernant les Principes

Ces Principes identifient les fonctions et les responsabilités des participants dans les systèmes d'authentification et offrent un cadre à l'intérieur duquel on peut évaluer et gérer les risques accompagnant ces responsabilités. Ces Principes identifient aussi les points qu'il faut prendre en compte en matière de sécurité, de protection de la vie privée, d'information et de traitement des plaintes, à chaque stade de la conception, de la mise au point, de la mise en œuvre et de l'évaluation d'un processus d'authentification.

Ces Principes sont destinés à s'appliquer aux processus d'authentification utilisés en relation avec les communications électroniques qui ont lieu entre entreprises (B) ou administrations publiques (G) et autres organisations (B2B, B2G et G2G), entre organisations et individus (C) (consommateurs ou citoyens – B2C, G2C) et entre individus (C2C).

Un ensemble varié de relations techniques, légales, contractuelles et commerciales peuvent exister entre les fournisseurs de services d'authentification et les utilisateurs de ces services. Une grande partie de ces relations sont régies par des accords. Les Principes contenus dans le présent document sont destinés à guider l'élaboration de ces accords et à s'appliquer à tout l'éventail de ces relations.

Les dispositions des divers Principes sont mutuellement liées et interdépendantes. Ainsi, il leur serait difficile d'atteindre leur but si on les mettait en œuvre sélectivement. Les personnes amenées à appliquer ces Principes pour définir ou mettre en œuvre des processus d'authentification sont invitées à surpasser les normes que les Principes établissent et à les

étendre pour répondre aux besoins de leur application ou environnement particulier en matière de sécurité.

Ces Principes sont formulés à un haut niveau de généralité et de neutralité technologique. Il existe une large variété de technologies et techniques d'authentification et les choix devraient être déterminés par la nature de la communication particulière considérée et par les besoins des participants. La mise en œuvre des processus d'authentification diffère aussi suivant les objectifs commerciaux ou juridiques à atteindre et suivant les caractéristiques de l'environnement dans lequel a lieu la communication électronique, telles que les besoins de sécurité et de protection de la vie privée ou d'autres obligations légales ou réglementaires. Ces facteurs définissent la fonctionnalité que l'on demande à un processus d'authentification et, dans certains cas, le type même d'authentification à utiliser. Les choix dépendront aussi du degré de déploiement des divers types de solutions d'authentification (c'est-à-dire des solutions ou justificatifs qui sont déjà en place).

Les Principes recouvrent l'authentification dans son sens le plus large mais :

- Ils ne concernent pas l'authentification des documents.
- Ils ne couvrent pas l'authentification des appareils, ni l'authentification au niveau du domaine mais ont néanmoins des liens avec les éléments de la Boîte à outils anti-spam élaborée par le Groupe de réflexion sur le spam¹¹ de l'OCDE (par exemple, applications d'authentification visant à réduire le spam et les messages électroniques nuisibles).
- Ils ne couvrent pas "l'autorisation" (qui est un processus distinct mais connexe consistant à vérifier si la personne ou organisation considérée est habilitée à réaliser telle ou telle transaction). Généralement, les décisions concernant l'autorisation sont du ressort de la partie en confiance (c'est-à-dire l'entité ou personne qui se fie à la déclaration d'identité pour prendre la décision d'autorisation).
- Ils ne traitent pas des signatures électroniques en elles-mêmes (ou des signatures numériques avec une authentification étroitement liée à l'objet signé).

Ainsi, il sera peut-être nécessaire d'explorer certains aspects de l'authentification, ou des sujets hors du champ de ces Principes, et d'élaborer des outils d'orientation complémentaires (dans le cadre de l'OCDE ou dans d'autres enceintes) pour s'assurer que des réponses adéquates sont apportées aux besoins d'utilisateurs ou d'applications spécifiques.

L'environnement de l'authentification est changeant et les technologies utilisées continueront d'évoluer. Bien que l'on se soit efforcé de définir des Principes qui puissent couvrir l'évolution prévisible, ils pourront être soumis à une révision le cas échéant de manière à prendre en compte d'éventuels changements importants sur le plan du progrès technologique, des caractéristiques de marché ou de l'évolution internationale.

Concepts et terminologie

Ces Principes concernent l'authentification de la communication électronique dans son sens le plus large. En conséquence, les concepts et termes utilisés sont relatifs à tous les participants, actions ou techniques couvrant tous les aspects de l'authentification, aussi bien du point de vue technique que juridique ou commercial. Chaque concept ou terme est lié aux autres ; aucun ne doit être considéré isolément.

Dans l'élaboration des notions qui suivent, on a considéré les définitions existantes, notamment celles établies par les organismes de normalisation internationaux tels que l'Organisation internationale de normalisation (ISO). Cependant, le large champ des présentes orientations pour les politiques a conduit à des définitions qui peuvent différer de

11 . Voir "Boîte à outils anti-spam" de l'OCDE, www.oecd-antispam.org.

celles de termes similaires employés ailleurs dans des contextes spécifiques ou à un niveau technique.

- **Authentification** : Fonction destinée à établir la validité et l'assurance de l'identité déclarée par un utilisateur, un dispositif ou une autre entité dans un système d'information ou de communications.
- **Assurance** : Processus destiné à confirmer un des multiples objectifs visés en matière de sécurité pour la protection des informations et des systèmes d'information, y compris l'authentification, l'intégrité, la disponibilité, la confidentialité et l'imputabilité. L'assurance n'est pas absolue, c'est un niveau de confiance défini. On peut aborder les niveaux d'assurance relatifs à l'authentification de divers points de vue – un d'entre eux étant les pratiques de gestion des risques et un autre les solutions technologiques appropriées.
- **Attributs** : Information concernant des types spécifiques de caractéristiques d'une identité donnée.
- **Autorisation** : Les actions qu'une personne ou entité authentifiée a la permission d'effectuer à la suite de l'authentification. L'autorisation peut dépendre de certains attributs d'une identité. Les décisions concernant l'autorisation sont du ressort de la partie qui se fie à l'authentification.
- **Communication électronique** : Transmission, message ou transaction électroniques.
- **Cryptage** : La conversion de données (texte en clair) en une forme appelée cryptogramme que des personnes réceptrices non autorisées ne peuvent pas facilement comprendre. Le décryptage est le processus consistant à reconvertir dans leur forme originale les données cryptées de manière à les rendre intelligibles. Parmi les types de cryptage courants figure le cryptage symétrique ou asymétrique (à clé publique).¹²
- **Identité** : Au niveau opérationnel, un ensemble dynamique d'attributs définissant une référence unique à une personne ou entité, y compris quand les attributs sont fournis sous forme électronique au moyen d'une sorte ou une autre de justificatif. Les attributs peuvent être particuliers au contexte, suivant la nature de l'interaction.
- **Justificatif** : Données servant à établir les attributs ou l'identité déclarés par une personne ou entité.
- **Participants** : Individus ou organisations participant aux processus d'authentification. Cela comprend les individus ou organisations déclarant une identité, les parties en confiance, les autorités tierces fournissant des justificatifs d'identité, les fournisseurs de services de confiance et les certificateurs de systèmes tels que les auditeurs, organismes d'accréditation, organismes gouvernant une fédération d'identités, organismes de supervision publics. Un participant peut avoir plusieurs rôles.
- **Partie en confiance** : L'entité ou personne qui se fie à un justificatif d'identité ou à une déclaration d'identité pour prendre une décision quant à l'action à adopter dans le contexte d'une application donnée.

12. Les Lignes directrices régissant la politique de cryptographie de l'OCDE sont une importante référence. Ces Lignes directrices reconnaissent le rôle important que joue le cryptage en contribuant à assurer la sécurité des données et la protection de la vie privée dans les infrastructures, réseaux et systèmes d'information et de communication nationaux et mondiaux.
www.oecd.org/document/11/0,2340,en_2649_201185_1814731_1_1_1_1,00.html.

- **Signature électronique** : Données sous forme électronique dans, attachées à, ou logiquement associées à un message et utilisées par une personne, ou pour le compte d'une personne, dans l'intention d'identifier cette personne.

Dans la perspective des effets bénéfiques que peuvent apporter des méthodes d'authentification nationales et transjuridictionnelles, on propose les principes fondateurs et opérationnels suivants. Les principes fondateurs constituent des orientations pour l'utilisation et la mise en œuvre des méthodes d'authentification ; ils sont mutuellement liés et liés aussi aux principes opérationnels. Les principes opérationnels sont des orientations pour tous les utilisateurs, et notamment ceux qui sont impliqués dans la conception, à la mise au point et au déploiement des services et produits d'authentification.

Partie A – Principes fondateurs

1. Approche systémique

La conception, la mise au point et la mise en œuvre des solutions d'authentification doivent être vues comme un processus de développement de système cohérent faisant intervenir tous les participants concernés à des stades appropriés. Il faut s'attacher notamment à faire intervenir les utilisateurs finals de l'authentification au stade de la conception du système. Des garanties techniques et non techniques doivent être envisagées comme étant des parties complémentaires de la conception système de solutions d'authentification. L'interopérabilité des solutions d'authentification devrait aussi être considérée à ce stade. Des garanties techniques et non techniques devraient être envisagées comme des parties complémentaires de la conception système des solutions d'authentification.

Quand on conçoit et qu'on met en œuvre des solutions d'authentification, la sécurité de l'ensemble du système doit être une motivation essentielle. Les dangers et les problèmes émanant de tous les participants concernés en matière de processus de transmission et de stockage des données doivent être abordés à tous les stades de la conception système et de la mise au point de solutions d'authentification.

Le choix des niveaux d'assurance et des mécanismes pour l'authentification doit reposer sur une évaluation des risques des diverses composantes du système et du ou des comportement(s) des participants. La convivialité et la facilité d'utilisation doivent aussi être un principe directeur pour le choix des mécanismes d'authentification car elle contribue à développer la confiance des utilisateurs dans les transactions en ligne. Il faut établir un équilibre entre les mesures de sécurité et la facilité d'utilisation de telle sorte que la sécurité globale du système soit en place.

2. Proportionnalité

Le degré de responsabilité et de risque assumé par chaque participant au processus d'authentification doit être proportionné au degré de connaissances et de contrôle que ce participant est raisonnablement censé posséder et exercer, ainsi qu'à la nature et à la valeur de la transaction ou de la communication elle-même. Étant donné que les participants peuvent accomplir plusieurs fonctions selon des combinaisons variées, le degré de responsabilité et de risque assumé par un participant donné peut varier selon ces fonctions.

3. Rôles et responsabilités

Les participants aux processus d'authentification doivent avoir conscience de leur rôles, des fonctions qu'ils accomplissent et des responsabilités associées à ces fonctions. Les fonctions et responsabilités doivent être clairement formulées et indiquées. Tous les

participants doivent agir avec prudence et prendre des mesures raisonnables pour s'informer de la nature du processus d'authentification, notamment de ses exigences et de ses limites, pour protéger les informations associées au processus et pour gérer les risques auxquels ils s'exposent.

4. Sécurité et confiance

Tous les participants aux processus d'authentification ont la responsabilité de contribuer à la sécurité et à l'atténuation des risques par de saines pratiques de sécurité, comme indiqué dans le huitième principe des Lignes directrices de l'OCDE sur la sécurité, intitulé « gestion de la sécurité ». ¹³

Tous les participants à un processus d'authentification doivent être responsables et comptables de la sécurité en proportion de leurs rôles dans ce processus. Ceux qui conçoivent et mettent en œuvre les services de sécurité et de confiance doivent assumer une plus grande responsabilité que les autres pour l'atténuation des risques. Cela inclut de promouvoir une culture mondiale de la sécurité en incorporant des éléments de sécurité et de confiance (par exemple, de protection de la vie privée) dans les systèmes et technologies de l'information. En appliquant de sains principes de sécurité, les organisations contribueront à développer la confiance en l'utilisation des technologies qui facilitent les transactions en ligne. L'authentification joue un rôle clé pour assurer la confiance dans les transactions en ligne et le commerce électronique en établissant des contrôles d'accès et une responsabilisation fiables.

5. Protection de la vie privée

Les organisations qui conçoivent ou exploitent des processus d'authentification doivent se conformer aux Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE et aux codes de bonnes pratiques dans ce domaine, en plus de la législation applicable. Ce principe est particulièrement important dans le contexte de l'authentification transfrontière, où les lois et règlements de protection de la vie privée peuvent varier.

Ceux qui conçoivent et mettent en œuvre des processus d'authentification doivent examiner comment les systèmes peuvent adéquatement respecter la vie privée et la protection des données à tous les stades du processus. Cela peut impliquer de limiter la collecte, l'utilisation, le stockage, le transfert et la divulgation d'informations à caractère personnel aux fins jugées nécessaires à l'accomplissement de l'authentification. Quand on présente un avertissement informatif aux personnes, celui-ci doit être exact, clair, bien visible et sans ambiguïté. Le contrôle individuel sur ses données à caractère personnel par la personne sujette à l'authentification est préconisé, même si la gérance de ces données est confiée à une autorité publique ou à un autre tiers.

Le niveau de l'authentification (et, par définition, la quantité d'informations à caractère personnel collectées pour le processus d'authentification) doit être proportionné à la nature de la transaction ou de la communication et prendre en compte le degré d'importance et de sensibilité requis. Ce principe est particulièrement important dans le contexte de l'authentification transfrontière, où les lois et règlements de protection de la vie privée peuvent varier.

L'authentification offre des moyens de protéger la vie privée mais seulement si elle est utilisée en adéquation avec les fins recherchées et d'une manière qui prenne en compte les intérêts des utilisateurs. On peut avoir tendance à exiger le niveau d'authentification le plus

13. Ce Principe reprend les Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information. Le texte complet de ces Lignes directrices est accessible à <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

fort pour toutes les transactions avec l'idée de protéger les systèmes et leurs utilisateurs. Cependant, si une plus grande quantité d'informations à caractère personnel peut être requise pour obtenir des justificatifs plus fiables (vérification d'identité), on peut et l'on doit concevoir les systèmes de manière à ce qu'ils ne dévoilent pas ces informations durant les phases de routine de la transaction d'authentification ou de la communication électronique.

6. Gestion des risques

Les risques associés aux processus d'authentification pour les communications électroniques doivent être identifiés, évalués et gérés de manière raisonnable, équitable et efficace. Les responsabilités des participants concernant la gestion des risques doivent être proportionnées au degré de connaissances, de contrôle et au pouvoir d'agir que chaque participant est raisonnablement censé posséder et exercer. La capacité des participants d'identifier, d'évaluer et de gérer les risques variera sensiblement et on ne peut pas raisonnablement attendre de certains types de participants (par exemple, des consommateurs et des petites entreprises) qu'ils le fassent aussi bien que d'autres participants. (Voir le Principe 2 – Proportionnalité)

On doit aussi appliquer ce principe quand on envisage le choix de niveaux d'assurance appropriés à divers types d'applications. Le choix du niveau d'assurance de l'authentification doit avoir pour guide la plausibilité et les conséquences des risques et effets identifiés (par exemple, d'un détournement d'identité, pour tous les participants).

Le choix de niveaux d'assurance sur la base de l'analyse des risques doit être étroitement associé au choix de mécanismes d'authentification adéquats, répondant par des éléments de sécurité appropriés, et d'une manière économique et efficace, aux risques et effets que l'on a identifiés.

Partie B – Principes opérationnels

1. **Aptitude à l'utilisation** : Les processus d'authentification doivent être efficaces, opérationnels, fiables et faciles à utiliser et ils doivent prendre en compte les intérêts et les besoins des personnes et des organisations. L'aptitude à l'utilisation doit avoir pour guide la minimisation des risques associés à l'utilisation.
2. **Adéquation aux fins** : L'authentification, comme beaucoup de pratiques et de technologies liées à la sécurité, se situe sur un continuum de risque. Cela signifie que les technologies et processus d'authentification doivent être considérés dans le contexte d'une application et qu'ils doivent être appropriés et proportionnés à la fonction de cette application et à l'utilisation souhaitée. La sécurité doit être suffisante pour répondre au risque de façon acceptable, mais elle ne doit pas peser déraisonnablement sur l'accomplissement de la communication électronique. Les besoins des entreprises en matière de confiance se reflètent dans le niveau d'assurance fourni et ils sont en relation avec le type de justificatif utilisé. (Voir l'Appendice B pour plus d'information et des exemples de niveaux d'assurance). Dans le choix des technologies d'authentification à utiliser, les décisions fondées sur le marché devraient jouer un rôle déterminant. Les fournisseurs de services devraient considérer le niveau de risque pour le système dans son ensemble, le coût de mise en œuvre, la commodité, l'avantage global pour l'entreprise et les obligations légales applicables.
3. **Continuité des affaires** : La mise en place de mesures destinées à assurer la continuité des affaires et la reprise après incident développera la confiance des utilisateurs et facilitera l'acceptation transjuridictionnelle d'activités ou outils d'authentification fiables.
4. **Éducation et sensibilisation** : L'utilisation de processus d'authentification efficaces peut être dissuasive contre le vol d'avoirs et d'informations en ligne. L'éducation et

la sensibilisation concernant les avantages et les utilisations adéquates de l'authentification sont des conditions préalables pour une large diffusion de l'authentification électronique, et elles sont essentielles pour maintenir la confiance des utilisateurs dans les réseaux et les systèmes d'information. Les campagnes d'éducation doivent souligner l'importance des outils qui à la fois sont conviviaux et établissent un degré de sécurité approprié. Une attention particulière doit être portée à l'éducation des consommateurs et des petites entreprises, en mettant l'accent non seulement sur les avantages de l'authentification mais aussi sur les responsabilités et les risques associés à son utilisation.

5. **Information** : Les participants qui offrent des services d'authentification doivent informer les autres participants de telle sorte que tous connaissent les risques et les responsabilités associés à l'utilisation de l'authentification. Ces informations doivent être fournies de manière suffisamment détaillée eu égard au but recherché, dans un langage simple et être bien visibles. Ces trois facteurs influenceront sur le degré de connaissance que l'on peut raisonnablement attendre des autres participants au sujet de ces informations.

6. **Traitement des plaintes** : Les organisations qui utilisent des processus d'authentification doivent offrir un processus de traitement des plaintes permettant aux participants d'aboutir à une solution de manière opérationnelle et efficace et de répondre de manière appropriée aux problèmes de non-conformité des services. Les processus de traitement des plaintes doivent être visibles, accessibles, réactifs et objectifs.

7. **Audit et évaluations indépendants** : L'utilisation d'audits et d'évaluations de conformité réalisés par des parties indépendantes, de préférence selon des normes internationalement reconnues, développera la confiance des utilisateurs et facilitera l'acceptation transjuridictionnelle des services. Chaque phase du processus d'authentification, de la vérification d'identité à la gestion technique ou administrative du service, influe sur la conformité du processus et la confiance qu'il peut inspirer. Idéalement, toutes les phases du processus devraient être cohérentes en force et en robustesse. Les organismes d'accréditation qui supervisent les exigences requises pour la certification et qui accréditent les auditeurs qui font la certification ont aussi un rôle important à jouer. Leur adhésion à des procédures reconnues peut aussi faciliter l'acceptation transjuridictionnelle des services.

8. **Approches transjuridictionnelles** : Idéalement, les approches nationales à l'égard de l'authentification devraient permettre l'acceptation des services d'authentification basés à l'étranger dès lors qu'ils satisfont aux exigences locales ou à leurs équivalents. Ces exigences locales ne devraient pas être conçues ou appliquées de manière discriminatoire. La cohérence dans l'application des normes et une concordance générale sur la façon de définir les niveaux d'assurance peuvent faciliter l'interopérabilité transjuridictionnelle (et transsectorielle). L'interopérabilité aussi bien commerciale que technique et juridique est nécessaire pour les transactions transsectorielles et transjuridictionnelles. L'interopérabilité doit être prise en compte au stade de la conception chaque fois que possible.

9. **Normes** : Le déploiement à grande échelle de technologies d'authentification pouvant être utilisées dans un contexte mondial dépend fortement des normes, qu'elles soient de droit ou de fait. Les normes visent à regrouper les besoins des fournisseurs, des utilisateurs, des parties en confiance et des organismes législatifs à l'intérieur de cadres contribuant à la mise en œuvre coordonnée de structures d'authentification. Les organismes de normalisation qui publient des normes importantes pour l'interopérabilité mondiale des structures d'authentification sont notamment : l'ISO, l'UIT, l'ETSI, le CEN, l'ANSI, le NIST, OASIS – Liberty Alliance, le W3C, l'IETF et l'accord multilatéral CC (Common Criteria).

Afin d'achever un certain degré d'interopérabilité des divers schémas d'authentification, des standards devraient être appliqués lors de l'élaboration et de la mise en œuvre des solutions d'authentification, en particulier à l'égard des procédures d'enrôlement, du

déploiement des justificatifs, des capacités techniques et de la sécurité des justificatifs, de la gestion des justificatifs, des interfaces techniques entre les solutions et applications d'authentification ainsi que toute procédure gouvernementale de supervision pour les fournisseurs d'authentification.

Questions en suspens

Les principes ci-dessus forment un cadre destiné à promouvoir des approches communes à l'égard de l'authentification afin de développer l'utilisation de l'authentification au niveau national et à travers les frontières. Cependant, un certain nombre de questions mises en lumière dans les travaux précédents de l'OCDE et dans les discussions entre les pays Membres, les entreprises et la société civile tenues dans le cadre du Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) et du Comité de la politique de l'information, de l'informatique et des communications (PIIC) restent en suspens. Ces questions persistantes sont signalées à l'attention du ou des comité(s) de l'OCDE appropriés et à d'autres enceintes internationales, à l'industrie et à la société civile, pour leurs débats relatifs à l'économie numérique et aux défis futurs de la gestion de l'identité.

- La grande diversité des méthodes d'authentification utilisées actuellement pourrait être une source de difficultés pour les utilisateurs et les fournisseurs qui cherchent la méthode correspondant le mieux à leurs besoins. Cette diversité peut devenir un obstacle aux services interorganisationnels ou transfrontières. Des normes internationales pourraient peut-être atténuer en partie la complexité existant actuellement sur le marché de l'authentification, mais des accords plus larges sur les niveaux d'assurance et sur les méthodes d'authentification susceptibles de leur être associées sont nécessaires pour établir des solutions durables, aussi bien à l'échelon national qu'à travers les frontières.
- Sur un marché mondialisé, les travaux visant à harmoniser les normes sont essentiels si l'on veut maximiser leur efficacité. Certains efforts dans cette direction ont déjà donné des résultats, comme la coopération entre les gouvernements des États-Unis et du Canada pour des solutions sous forme de "ponts", et la reconnaissance entre les États-Unis et l'Union européenne (ETSI) de schémas définissant les exigences requises des autorités de certification (fournisseurs de services d'infrastructure à clé publique). On pourrait encourager davantage ce genre d'efforts, et des travaux sur les correspondances de normes pourraient avoir lieu sous les auspices des organismes internationaux concernés.
- Les différences dans le traitement et la reconnaissance juridiques des documents et signatures électroniques restent un obstacle à l'utilisation transfrontières de l'authentification. Les travaux conduits au sein d'organisations internationales comme la CNUDCI établissent des approches communes, mais des travaux multilatéraux supplémentaires au niveau pratique demeurent nécessaires.
- Des mécanismes ont été mis au point pour la reconnaissance des services d'authentification étrangers mais on a peu d'expérience des applications transjuridictionnelles. Il manque aux juridictions des moyens d'évaluer le cadre régissant la confiance chez leurs partenaires. Le présent document d'orientation et le cadre qu'il propose peuvent apporter une aide à cet égard mais des travaux plus complets sur cette question sont nécessaires.
- Les travaux précédents de l'OCDE ont mis en lumière le manque d'analyses quant à la viabilité économique de l'authentification, qui fait obstacle à une plus large utilisation. Les succès observés sur le marché (par exemple, banque à domicile) pourraient apporter des éléments à ces analyses et servir à stimuler l'adoption de l'authentification.

- La biométrie et l'identification par radiofréquences (RFID) ont un lien avec l'authentification du fait qu'elles recouvrent des technologies susceptibles d'améliorer encore les méthodes de vérification. Il pourrait être utile d'examiner l'incidence de ces nouvelles technologies sur les activités consistant à pratiquer l'authentification et à assurer une sécurité accrue et une meilleure gestion de l'identité dans la communication en ligne.

REFERENCES

Documents de l'OCDE

- L'usage transfrontalier de l'authentification dans les pays de l'OCDE (résumé des réponses, 2005). DSTI/ICCP/REG(2005)4/FINAL
[www.oilis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg\(2005\)4-final](http://www.oilis.oecd.org/olis/2005doc.nsf/LinkTo/dsti-iccp-reg(2005)4-final)
- Questionnaire sur l'utilisation actuelle de l'authentification dans un contexte transnational dans les pays de l'OCDE (2004). DSTI/ICCP/REG(2004)5/FINAL
- Synthèse des réponses à l'enquête sur l'environnement législatif et le cadre des politiques concernant les services d'authentification électronique et les signatures électroniques dans les pays Membres de l'OCDE (2004). DSTI/ICCP/REG(2003)9/FINAL
[www.oilis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg\(2003\)9-final](http://www.oilis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp-reg(2003)9-final)
- Inventaire des cadres juridiques et politiques applicables aux services d'authentification électronique et aux signatures électroniques dans les pays Membres de l'OCDE (questionnaire, 2003). DSTI/ICCP/REG(2003)4/REV1
- Electronic Authentication: Analysis and Mapping of Key Elements for Establishing Confidence in Certification Services (2002). DSTI/ICCP/REG(2002)4
- Electronic Authentication: Framework for Analysis of Key Elements for Establishing Trust in Certification Processes (document de séance soumis par le Canada, 2002)
DSTI/ICCP/REG/RD(2002)3
- Electronic Authentication: Information Paper on the Work of the APEC eSecurity Task Group - Draft for Discussion Purposes Only (document de séance soumis par l'Australie, 2002)
DSTI/ICCP/REG/RD(2002)1
- Progrès réalisés dans les pays Membres de l'OCDE à la suite de la Déclaration d'Ottawa sur l'authentification pour le commerce électronique (2002).
DSTI/ICCP/REG(2001)10/FINAL
[www.oilis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg\(2001\)10-final](http://www.oilis.oecd.org/olis/2001doc.nsf/linkto/dsti-iccp-reg(2001)10-final)
- Revised Inventory of Approaches to Authentication and Certifications in a Global Networked Society (2000). DSTI/ICCP/REG(2000)1/REV1
- Questionnaire pour l'enquête sur les exigences de forme (2000)
DSTI/ICCP/REG(2000)2
- Inventory of Approaches to Authentication and Certifications in a Global Networked Society (1999). DSTI/ICCP/REG(99)13/FINAL
[www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg\(99\)13-final](http://www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)13-final)
- Joint OECD-Private Sector Workshop on Electronic Authentication. Menlo-Park, Californie, Etats-Unis. 2-4 juin 1999. En coopération avec des représentants du secteur privé et avec The Stanford Program in Law, Science & Technology, Stanford Law School (1999).
DSTI/ICCP/REG(99)14/FINAL comprenant le "Background Paper on Electronic Authentication Technologies and Issues" [DSTI/ICCP/REG(99)6/REV1]
[www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg\(99\)14-final](http://www.oilis.oecd.org/olis/1999doc.nsf/linkto/dsti-iccp-reg(99)14-final)
- Proposal by the Delegation of the United Kingdom for Guidelines on Policy for Authentication and Electronic Signatures (1999)
DSTI/ICCP/REG/AH(99)1
- Discussion Paper on Authentication and Certification (1998). DSTI/ICCP/REG(98)1

Déclaration sur l'authentification pour le commerce électronique (1998)
 DSTI/ICCP/REG(98)9/FINAL
[www.oalis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg\(98\)9-final](http://www.oalis.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)9-final)

Inventory of Approaches to Authentication and Certification in a Global Networked Society (1998). DSTI/ICCP/REG(98)3/REV1

Voir aussi :

- Boîte à outils anti-spam de politiques et mesures recommandées (Boîte à outils anti-spam de l'OCDE)
[www.oalis.oecd.org/olis/2005doc.nsf/linkto/dsti-cp-iccp-spam\(2005\)3-final](http://www.oalis.oecd.org/olis/2005doc.nsf/linkto/dsti-cp-iccp-spam(2005)3-final)

Autres ressources

Internationales

- Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation (1996)
http://www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/1996Model.html
- Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation (2001)
www.uncitral.org/uncitral/fr/uncitral_texts/electronic_commerce/2001Model_signatures.html

Régionales

- Union européenne « Plan d'action i2010 pour l'e-gouvernement »
<http://europa.eu/scadplus/leg/fr/lvb/l24226j.htm>
- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, Journal officiel L 013 , 19 janvier 2000, p. 0012 - 0020
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:FR:HTML>

Nationales

- Australie : Cadre du gouvernement pour l'authentification :
www.agimo.gov.au/infrastructure/authentication/agaf/impguidegovt
www.agimo.gov.au/infrastructure/authentication/agaf/overview
- Canada : Principes d'authentification
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv0009of.html
- États-Unis :
 - NIST Special Publication 800 – 63 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology (NIST), USA. http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
 - OMB's E-Authentication Guidance for U.S. Federal Agencies (M-04-04)
www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf
- Nouvelle-Zélande : Cadre du gouvernement de Nouvelle-Zélande pour l'authentification :
www.e.govt.nz/resources/news/2002/apr-2002/2002042801.html

- Royaume-Uni : “Registration and Authentication - e-Government Strategy Framework Policy and Guidelines”
www.govtalk.gov.uk/policydocs/policydocs_document.asp?docnum=654&topic=56&topicitle=Security+Framework&subjecttitle= .

Non gouvernementales

- Center for Democracy and Technology “Authentication Privacy Principles Working Group. Interim Report”. 13 mai 2003. www.cdt.org/privacy/authentication/030513interim.shtml
- Chambre de commerce internationale, International Chamber of Commerce (ICC): General Usage for International Digitally Ensured Commerce (version II) - GUIDEC II
www.iccwbo.org/home/guidec/guidec_two/foreword.asp

APPENDICE A

HISTORIQUE DES TRAVAUX DE L'OCDE SUR L'AUTHENTIFICATION (1998 – 2005)

La Déclaration ministérielle d'Ottawa

Les Ministres de l'OCDE ont adopté la “Déclaration sur l'authentification pour le commerce électronique” dans le cadre de la Conférence ministérielle intitulée “Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial” tenue à Ottawa, Canada, du 7 au 9 octobre 1998.¹⁴ Cette Déclaration reconnaît l'importance de l'authentification pour le commerce électronique et expose un certain nombre d'actions visant à promouvoir le développement et l'utilisation des technologies et mécanismes d'authentification électronique. En particulier, les Ministres se déclarent résolus à :

- adopter une approche non discriminatoire à l'égard des mécanismes d'authentification électroniques émanant d'autres pays ;
- encourager les efforts pour développer des technologies et mécanismes d'authentification et faciliter l'utilisation de ces technologies et mécanismes pour le commerce électronique ;
- amender, le cas échéant, les exigences spécifiques sur la technologie ou les supports dans les lois actuelles ou les politiques susceptibles d'entraver l'utilisation des technologies de l'information et des communications et des mécanismes d'authentification électroniques, en tenant compte des dispositions appropriées de la Loi type sur le commerce électronique adoptée par la Commission des Nations Unies pour le droit commercial international (UNCITRAL) en 1996 ;
- procéder à la mise en œuvre des technologies d'authentification électronique pour améliorer la délivrance au public des services et programmes gouvernementaux ; et
- continuer d'œuvrer à l'échelon international, conjointement avec les entreprises, l'industrie, et les représentants des utilisateurs, pour que les technologies et mécanismes d'authentification facilitent le commerce électronique mondial.

Inventaire des approches à l'égard de l'authentification électronique et Atelier conjoint OCDE-secteur privé

Dans une phase préparatoire, le Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) du Comité PIIC de l'OCDE a réalisé une enquête auprès des pays Membres sur leurs approches à l'égard de l'authentification et de la certification sur les réseaux mondiaux, couvrant les lois, politiques et initiatives, dans le secteur public et dans le secteur

14 . [www.oecd.org/olis/1998doc.nsf/linkto/sg-ec\(98\)14-final](http://www.oecd.org/olis/1998doc.nsf/linkto/sg-ec(98)14-final)

privé et aux niveaux national, régional et international. Il en est résulté un document intitulé "Inventory of Approaches to Authentication and Certification in a Global Networked Society"¹⁵ (1999) offrant des informations utiles sur les approches nationales, notamment concernant les accords contractuels privés, les exigences technologiques, les normes et les autorités de certification.

En outre, un Atelier conjoint OCDE-secteur privé sur l'authentification électronique¹⁶, organisé par le GTSIVP, a eu lieu à Stanford, Californie, du 2 au 4 juin 1999 pour stimuler le dialogue entre toutes les parties en présence et continuer à recueillir des informations sur les approches à l'égard de l'authentification électronique. Deux cents représentants des gouvernements des pays de l'OCDE, du Telecommunications Working Group de la Coopération économique Asie-Pacifique (APEC), du secteur privé, des organisations internationales, des organisations de défense des consommateurs et des associations d'utilisateurs ont tenu des débats sur les modèles d'entreprise et de gouvernement, sur les approches des différents secteurs d'activité, et sur les questions entourant la mise en œuvre de l'authentification électronique, notamment les éléments requis pour l'exploitation internationale de systèmes d'authentification mondiaux.

Rapport sur les progrès réalisés à la suite de la Déclaration ministérielle

A la suite de cet atelier, le GTSIVP a établi un Comité de pilotage pour suivre la mise en œuvre des politiques et législations nationales relatives aux objectifs de la Déclaration ministérielle. Il en est résulté en 2000 une mise à jour de l'inventaire des approches à l'égard de l'authentification et de la certification¹⁷ destinée à prendre en compte les progrès réalisés au niveau national.

Ces travaux, ainsi que des informations émanant des économies Membres de l'APEC, ont été intégrés à un rapport intitulé "Progrès réalisés dans les pays Membres de l'OCDE à la suite de la Déclaration d'Ottawa sur l'authentification pour le commerce électronique"¹⁸.

Ce rapport conclut que des progrès ont été réalisés sur des questions comme la reconnaissance juridique des signatures électroniques ou l'application des technologies d'authentification à la délivrance des services des administrations publiques. Il met en lumière la nécessité d'assurer la compatibilité des approches et politiques des pays Membres de l'OCDE et des initiatives du secteur des entreprises afin d'établir une véritable interopérabilité internationale des systèmes d'authentification électronique sur le marché. Le rapport déclare que des travaux additionnels pourraient aider à mieux discerner et traiter les obstacles à l'utilisation mondiale et transparente des méthodes d'authentification.

Enquête sur l'environnement législatif et le cadre des politiques concernant les services d'authentification électronique et les signatures électroniques

Afin d'aider à déterminer comment on pourrait relier les divers cadres législatifs, juridiques et stratégiques en vue de parvenir à une acceptation transjuridictionnelle des services d'authentification et d'assurer l'effet juridique des signatures électroniques, le GTSIVP a conduit en 2002-2003 une "Enquête sur l'environnement législatif et le cadre des politiques concernant les services d'authentification électronique et les signatures

15 . DSTI/ICCP/REG(99)13/FINAL

16 . On trouvera les comptes rendus et les documents de base dans DSTI/ICCP/REG(99)14/FINAL

17 . DSTI/ICCP/REG(2000)1/REV1

18 . DSTI/ICCP/REG(2001)10/FINAL

électroniques dans les pays Membres de l'OCDE".¹⁹ Le questionnaire a été conçu pour être comparable avec l'enquête réalisée dans les économies Membres de l'APEC par l'e-Security Task Group de l'APEC.

Les informations fournies par les pays Membres ont permis d'identifier les domaines dans lesquels les pays Membres montraient une forte convergence, les domaines dans lesquels il existait seulement une certaine convergence, et les domaines montrant des divergences (voir le Tableau 1). Le rapport met aussi en lumière le risque que les pays Membres établissent des approches divergentes à l'égard de la reconnaissance des services d'authentification basés à l'étranger, ce qui pourrait faire obstacle aux transactions transfrontières.

Tableau 1. Constatations de l'Enquête sur l'environnement législatif et le cadre des politiques concernant les services d'authentification électronique et les signatures électroniques dans les pays Membres de l'OCDE

Forte convergence	Relative convergence	Divergences
<ul style="list-style-type: none"> • Cadre légal et réglementaire gouvernant les signatures électroniques • Obligations en matière de licences, d'accréditation et d'approbation pour les services d'authentification • Neutralité à l'égard des technologies • Sécurité de l'administration publique en ligne • Attitude à l'égard des signatures et services basés à l'étranger • Exigences en matière de justificatifs 	<ul style="list-style-type: none"> • Processus d'enregistrement • Évaluation des services 	<ul style="list-style-type: none"> • Nature des exigences en matière d'audit • Reconnaissance des services d'authentification étrangers • Normes techniques, même s'il existe une certaine convergence (par exemple, pour les infrastructures à clé publique)

Rapport sur l'utilisation transfrontières de l'authentification

Sur la base de ces constatations, le GTSIVP a jugé en octobre 2003 qu'une meilleure compréhension du marché existant de l'authentification transfrontières était nécessaire pour contribuer à rapprocher davantage les approches nationales et développer l'utilisation transfrontières de l'authentification. Une enquête a été conduite en 2004-2005 sur les mises en œuvre existantes de l'authentification et sur les exemples d'utilisation de l'authentification à travers les frontières ainsi que sur les obstacles à l'utilisation transfrontières des signatures numériques du point de vue des fournisseurs ou des utilisateurs. Cette enquête intitulée "L'usage transfrontalier de l'authentification dans les pays de l'OCDE"²⁰ a aussi collecté des informations sur les facteurs reconnus comme propices ou contraires à l'utilisation nationale des technologies d'authentification et des signatures numériques.

Ces travaux ont mis en lumière un certain nombre de thèmes communs dans les réponses des pays Membres (voir le Tableau 2) mais la principale constatation a été la nécessité d'accroître les taux d'utilisation des moyens d'authentification efficaces à travers les frontières.

19 . DSTI/ICCP/REG(2003)9/FINAL

20 . DSTI/ICCP/REG(2005)4/FINAL

Tableau 2 Thèmes communs mis en lumière dans le rapport sur “L’usage transfrontalier de l’authentification dans les pays de l’OCDE”

Eléments positifs	Eléments négatifs
<ul style="list-style-type: none"> • Maturité et robustesse des applications mises en œuvre dans le secteur public • Maturité des applications mises en œuvre dans le secteur financier • Alignement des cadres réglementaires • Approche non discriminatoire à l’égard des signatures et services “étrangers” • Neutralité à l’égard des technologies • La PKI (infrastructure à clé publique) se porte bien • Toutes les catégories d’utilisateurs participent • Toutes les applications décrites fournissent une preuve de l’identité mais avec diverses méthodes d’authentification 	<ul style="list-style-type: none"> • Problèmes et limitations de l’interopérabilité • Insuffisance des mécanismes pour la reconnaissance des services d’authentification étrangers • L’acceptation des justificatifs est un point d’achoppement pour l’interopérabilité • La diversité des méthodes d’authentification utilisées désoriente les utilisateurs • On manque d’informations sur les éléments employés pour protéger la vie privée • Manque d’analyses quant à la viabilité économique de l’authentification • Absence de données quantitatives sur l’utilisation

APPENDICE B

NIVEAUX D'ASSURANCE DE L'AUTHENTIFICATION

On peut aborder les niveaux d'assurance relatifs à l'authentification de divers points de vue – l'un d'entre eux étant les pratiques de gestion des risques et un autre les solutions technologiques appropriées. Ces deux approches ont été employées par les gouvernements des pays Membres dans les documents d'orientation publiés ces dernières années.²¹

L'approche par la gestion des risques considère les conséquences ou le degré de nocivité possibles d'une atteinte à la sécurité à la suite d'une insuffisance ou d'un échec du processus d'authentification. Les degrés de nocivité peuvent s'exprimer en termes qualitatifs (par exemple, atteinte à la vie privée) et / ou quantitatifs (par exemple, perte de revenus). Parmi les risques à envisager figurent les risques financiers, les risques sanitaires, les risques pour la sûreté et les activités criminelles. On doit considérer les risques aussi bien pour l'individu que pour l'organisation.

On peut envisager trois niveaux d'assurance fondamentaux, ainsi définis :

- **Bas** : une atteinte à la sécurité (par exemple, le détournement d'une identité électronique) peut entraîner des pertes modérées, de nature économique ou autre (par exemple, la perte de données non confidentielles) ; la répudiation d'une transaction basée sur ce type d'identification peut entraîner une perte pécuniaire modérée.
- **Moyen** : une atteinte à la sécurité (par exemple, le détournement d'une identité électronique) peut entraîner des pertes certaines, mais non d'une très grave nature ; elle peut causer la perte de données confidentielles ; la répudiation d'une transaction basée sur ce type d'identification peut entraîner une perte pécuniaire assez importante.
- **Haut** : une atteinte à la sécurité (par exemple, le détournement d'une identité électronique) peut entraîner des pertes importantes ; elle peut causer la perte de données hautement confidentielles ; la répudiation d'une transaction basée sur ce type d'identification peut entraîner une perte pécuniaire très importante.

Cette classification n'est qu'un exemple des nombreuses définitions possibles des niveaux d'assurance.

L'approche technologique (mécanismes d'authentification appropriés) considère les éléments génériques que l'on exige des mécanismes d'authentification, y compris des procédures de sécurité associées. Ces éléments requis concernent, par exemple, les procédures d'inscription pour l'authentification (procédures d'enregistrement), les capacités et la sécurité des justificatifs, les procédures de déploiement pour les justificatifs, la gestion des identités associée aux justificatifs, les agréments à obtenir des organismes de certification, etc.

21. Voir par exemple, au Royaume-Uni, "Registration and Authentication" publié en 2002 ou le cadre du gouvernement australien pour l'authentification (Australian Government e-Authentication Framework, voir la liste de références).

On peut envisager les niveaux d'assurance suivants, définis conformément à ces exigences génériques :

- De base : authentification à un seul facteur : par exemple, nom d'utilisateur et mot de passe délivrés au moyen d'une procédure à deux voies (c'est-à-dire, à la fois en ligne et par courrier).
- Moyen : authentification à deux facteurs : par exemple, SMS (message court) vers un téléphone mobile, jetons d'authentification avec protocoles stimulation-réponse, certificats PKI (Infrastructure à clé publique) à base logicielle, tous délivrés au moyen d'une procédure d'enregistrement et de déploiement à deux voies.
- Haut : authentification à deux facteurs avec une procédure d'enregistrement très sûre (comme la présence en personne, l'exigence d'un justificatif d'identité légalement valide) et le déploiement par une procédure à deux voies, par exemple certificats PKI sur une carte à puce ou un jeton USB sécurisé, ou dans un module de sécurité matériel (Hardware Security Module).

Là encore, ces définitions ne sont qu'un exemple des nombreuses structures possibles pour les niveaux d'assurance. On peut adopter des approches à grain plus ou moins fin, c'est-à-dire avec plus ou moins de niveaux. Les mécanismes d'authentification mentionnés ne sont donnés qu'à titre d'illustration et il ne faut pas les considérer comme une liste exhaustive ou exclusive.

Il pourrait être recommandé de fondre ces deux aspects en une seule approche unifiée, dans laquelle des niveaux d'assurance définis en fonction des risques découlant d'une atteinte à la sécurité sont associés à des niveaux de sécurité adéquats dans les mécanismes d'authentification.

Toute structure définie pour les niveaux d'authentification doit être étroitement liée au(x) domaine(s) d'application effectif(s) où on doit l'utiliser. Les domaines d'application constitueront le contexte nécessaire pour définir précisément les pertes ou conséquences possibles et pour choisir spécifiquement les mécanismes d'authentification appropriés.

L'introduction du concept de fédération d'identités²² pose un défi supplémentaire pour la définition des niveaux d'assurance. La fédération d'identités est mécanisme couramment utilisé pour fournir une fonction d'authentification unique aux utilisateurs de plusieurs systèmes d'information associés. L'authentification unique peut aussi être facilitée par d'autres mécanismes (par exemple, les portails de sécurité communs). La définition d'un niveau d'assurance pour un mécanisme d'authentification pouvant servir dans un environnement fédéré et / ou à des fins d'authentification unique nécessite des considérations additionnelles en matière de sécurité et une analyse des risques particulière. Ce genre d'analyse doit examiner les risques pour la sécurité que pose l'utilisation multiple d'un unique justificatif présenté à plusieurs systèmes et / ou la réutilisation, dans d'autres systèmes, des informations de validation d'identité fournies par le premier système auquel un justificatif a été présenté. Les systèmes fédérés introduisent un plus grand degré de complexité technique et, de ce fait, de nouveaux points de vulnérabilité dans une procédure d'authentification, par comparaison avec une authentification directe présentée à un seul système. Cela doit aussi être pris en compte dans l'analyse des risques précédant la définition d'une structure de niveaux d'assurance unifiée.

22. Voir Liberty Alliance Project Whitepaper: Personal Identity, 23 mars 2006. www.projectliberty.org/about/whitepapers/Personal_Identity.pdf.