PREMIER MINISTRE

ADAE

PREMIER MINISTRE

SGDN - DCSSI

==========

Politique de Référencement Intersectorielle de Sécurité (PRIS)

Service de confiance "Authentification"

==========

VERSION 2.0

Politique de Référencement Intersectorielle de Sécurité (PRISv2)

Présentation du service - Authentification

Référence	Date
PRISv2.0_-_Presentation_service_Authentification.doc	01/06/2005
Identification d'objet (OID)	**Racine OID et gestionnaire**
1.2.250.1.137.2.2.1.2.1.5	1.2.250.1.137 ADAE
Responsable	**Version**
Premier ministre ADAE - SGDN/DCSSI	**v2.0**
Critère de diffusion	**Nombre de pages**
PUBLIC	15

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
03/01/2005	0.1	Première version d'après « présentation Authentification »	ADAE/DCSSI
12/01/2005	0.2	Version diffusable	ADAE/DCSSI
01/06/2005	2.0	Version officielle après comité de relecture	ADAE/DCSSI

SOMMAIRE

I. Objet et contenu du document

L'ADAE et la DCSSI, dans le cadre de la sécurisation de la dématérialisation des échanges électroniques entre autorités administratives et usagers (particuliers et professionnels) et entre autorités administratives, ont élaboré conjointement la deuxième version de la Politique de Référencement Intersectorielle de Sécurité (PRIS).

L'objet de ce référentiel documentaire est de permettre la reconnaissance de produits de sécurité et de prestations de services de confiance pouvant participer à la sécurisation d'échanges dématérialisés. La note de cadrage [CADRA] et le préambule de la PRIS [PREAMB] présentent l'environnement, les objectifs et le contenu global de la PRIS, qui couvrira, à terme, un ensemble de services de confiance (confidentialité, authentification, signature, horodatage, archivage, ...). Certains de ces services, notamment confidentialité, authentification et signature, sont déclinés suivant trois niveaux de sécurité (*, ** et ***). Chaque niveau constitue un sur-ensemble du niveau inférieur. Ainsi, un produit ou un service reconnu comme répondant aux exigences du niveau (***) pourra être utilisé par l'usager aussi bien dans des applications d'échanges dématérialisés requérant du (***) que du (**) ou du (*).

Conformément à l'architecture de la PRIS définie dans [PREAMB], chaque service de confiance fait l'objet d'un document global définissant le service et les **règles spécifiques associées concernant la qualification et le référencement pour ce service**. Ce document doit notamment préciser le service considéré dans le contexte de la PRIS et présenter le contenu de la base documentaire pour ce service, notamment les objectifs et périmètre des différents niveaux de sécurité.

Le présent document est ce document descriptif global pour le service d'authentification.

II. Présentation succincte du service d'authentification

Le service d'authentification est un des éléments constitutifs de la confiance d'un échange dématérialisé.

Dans le cadre de la PRIS et de son utilisation dans l'administration, les types de relations couverts par le service d'authentification sont les suivants :

- authentification d'un usager vis-à-vis d'un service de l'administration accessible par voie électronique,
- authentification d'un usager vis-à-vis d'un agent d'une autorité administrative,
- authentification d'un agent d'une autorité administrative vis-à-vis d'un usager,

Rappel - Un agent d'une autorité administrative qui est en relation avec une autre autorité administrative est, pour cette dernière, un usager (cf. définition dans la PC Type).

Ce service de confiance permet à un usager ou à un agent de s'authentifier dans le cadre des types de relations mentionnés ci-dessus. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.

A ce stade la PRIS ne traite que de l'authentification basée sur des mécanismes cryptographiques asymétriques.

Dans le cadre d'une authentification lors d'un accès à un téléservice ou d'une authentification auprès d'une personne physique, la partie qui doit s'authentifier applique une transformation cryptographique, à l'aide de sa clé privée, à une requête d'authentification générée par la partie souhaitant vérifier l'authentification. Le lien entre cette phase d'authentification et les échanges qui suivent ("ouverture du canal de communication") doit ensuite être garanti avec une sécurité équivalente.

Dans le cadre de l'authentification d'un message ou de données, l'authentification est réalisée par l'usager ou par l'agent en appliquant une transformation cryptographique au message ou aux données à authentifier, à l'aide de sa clé privée. Le service d'authentification permet de garantir l'intégrité et l'origine du message / des données authentifiées mais, contrairement au service de signature électronique, il ne signifie pas que l'émetteur manifeste son consentement sur le contenu du message ou des données.

La clé privée doit être stockée et mise en œuvre dans un dispositif d'authentification qui doit rester sous le contrôle de l'usager détenteur de cette clé.

Une telle authentification peut être requise et mise en oeuvre lorsque l'usager accède à (ou échange avec) une application d'échange dématérialisé depuis son ordinateur personnel ou depuis une borne d'accès dans un lieu public (mairie, CPAM, ...).

Pour pouvoir s'authentifier ou authentifier un message ou des données, l'usager doit connecter, s'il en possède un, son dispositif matériel d'authentification (ex : carte à puce ou clé USB avec puce), dans lequel sa clé privée est confinée et protégée en confidentialité. Il doit ensuite saisir son code d'activation pour utiliser sa clé privée d'authentification. L'application d'authentification met en forme le message ou les données à authentifier et les transmet au dispositif d'authentification. Le calcul cryptographique de génération de la valeur d'authentification du message ou des données à authentifier est réalisé dans le dispositif d'authentification.

Les moyens d'authentification dont dispose l'usager peuvent également être de nature logicielle (moteur cryptographique du système d'exploitation, du navigateur ou du client de messagerie, logiciel spécifique).

L'usager doit choisir son dispositif d'authentification en fonction du niveau de sécurité demandé par le téléservice auquel il souhaite accéder. Avec un dispositif d'authentification *** associé à un certificat électronique de même niveau, il pourra s'authentifier à tous les téléservices qui requièrent une authentification électronique de l'usager.

Pour la vérification de l'authentification, l'usager met à disposition un certificat électronique que lui a préalablement délivré un prestataire de service de certification électronique (PSCE) et qui lie son identité avec sa clé publique. La vérification s'effectue à l'aide d'un module de vérification d'authentification.

Dans le cadre de la PRIS, l'utilisation de la clé privée d'authentification du porteur et du certificat associé est strictement limitée au service d'authentification.

Les exigences contenues dans la présente version de la PRIS couvrent les prestataires de services de certification électronique délivrant des certificats d'authentification et les dispositifs d'authentification. Des recommandations sont par ailleurs formulées quant aux applications d'authentification et aux modules de vérification d'authentification.

III. Contenu de la PRIS pour le service d'authentification

III.1. Prestataires de Services de Certification Electronique

Les exigences que doit respecter un PSCE, délivrant des certificats à des fins d'authentification, sont définies dans une politique de certification type (PC Type) [PC_AUTH], dont la structure est conforme au [RFC3647].

Cette PC Type regroupe les exigences de qualification portant sur les trois niveaux de sécurité (*), (**) et (***). Lorsqu'il y a des différences d'exigences entre les niveaux, elles sont clairement identifiées. Cette architecture documentaire permet de disposer d'une PC Type homogène quelque soit le niveau et permet également d'identifier facilement et rapidement sur quels sujets il y a des différences entre les niveaux et quelles sont ces différences.

De plus, cette PC Type s'appuie sur deux documents communs à toutes les PC Types de la PRIS qui sont :

- un document définissant des variables de temps concernant différents évènements du cycle de vie des clés cryptographiques et des certificats, noté [VAR_TEMPS] dans la PC Type,
- un document définissant les profils que doivent respecter les certificats, les listes de certificats révoqués et les protocoles OCSP ainsi que des exigences sur les algorithmes cryptographiques à mettre en œuvre, noté [PROFILS] dans la PC Type.

Un PSCE souhaitant faire qualifier à un niveau donné une famille de certificats doit intégrer dans sa PC l'ensemble des exigences de la PC Type correspondant au niveau visé et, bien entendu, respecter ensuite l'ensemble des engagements pris dans cette PC.

Un PSCE souhaitant faire référencer une famille de certificats pour un service et un niveau de sécurité donné doit tout d'abord faire qualifier cette famille pour ce niveau, afin de garantir le niveau de sécurité technique des prestations de service liées à ces certificats. Le référencement est ensuite prononcé par le comité de référencement, co-présidé par l'ADAE et la DCSSI, notamment sur la base de la qualification effective au niveau visé et d'une procédure de référencement.

III.2. Dispositifs d'authentification

Dans le cadre d'un téléservice requérant une authentification électronique l'usager et/ou l'agent doivent utiliser un dispositif d'authentification répondant à un minimum d'exigences de sécurité. Ces exigences sont décrites dans l'annexe 3 de la PC Type authentification et reprises ci-dessous.

Quelque soit le niveau, un dispositif d'authentification utilisé par le porteur pour stocker et mettre en œuvre sa clé privée, et le cas échéant générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé d'authentification du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;

- garantir la confidentialité et l'intégrité de la clé privée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ;
- assurer la fonction d'authentification pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Les différences entre les niveaux de sécurité concernent l'assurance du respect de ces exigences (cf. chapitre IV.2).

Les spécifications techniques définies dans le socle commun [Socle_IAS] (Identification, Authentification, Signature) prennent en compte l'ensemble de ces exigences de sécurité. Une carte à puce respectant les exigences du socle commun, sous réserve de certification au niveau approprié (cf. chapitre IV.2) répondra donc aux exigences de sécurité listées ci-dessus.

Ces exigences seront précisées d'ici fin 2005, au niveau ***, par un profil de protection de niveau d'assurance EAL 4+ qui reprendra l'essentiel des objectifs de sécurité du [CWA_14169], applicable pour les dispositifs de création de signature, qui seront adaptés aux besoins spécifiques de l'authentification. Un dispositif d'authentification qui sera certifié, suivant les critères communs, conforme à ce profil de protection sera considéré comme répondant aux exigences du niveau ***.

III.3. Application d'authentification

Aux niveaux *** et **, il est recommandé d'utiliser une application d'authentification qualifiée au niveau standard.

III.4. Module de vérification d'authentification

Aux niveaux *** et **, il est recommandé d'utiliser un module de vérification d'authentification qualifiée au niveau standard.

III.5. Environnement d'utilisation

Une application d'authentification et/ou un module de vérification d'authentification peuvent être mis en œuvre ou appelés par des téléservices dans deux principaux cadres :

- sur une borne publique ou un ordinateur dans un cadre privé ou professionnel pour un usage par une personne physique ;
- sur un serveur hébergeant un téléservice de l'Administration, pour un usage relevant d'une personne morale (présentement une autorité administrative) et sous le contrôle d'une personne physique.

Dans les deux cas, il est recommandé de prendre en compte les mesures de sécurité suivantes:

- protection contre les virus, avec mise à jour régulière ;

- contrôle et limitation des échanges entre la machine hôte et d'autres machines dans un réseau ouvert ;
- restriction, lorsque cela est possible, de l'accès aux fonctions d'administration de la machine aux seuls administrateurs de celles-ci (différenciation compte utilisateur/administrateur) ;
- installation et mise à jour de logiciels et de composants sur la machine sous le contrôle de l'administrateur ;
- refus par le système d'exploitation de l'ordinateur ou de la borne d'exécuter des applications téléchargées ne provenant pas de sources sûres ;
- mise à jour des composants logiciels et systèmes lors de la mise à disposition de mise à jour de sécurité de ceux-ci.

Dans le cas de l'utilisation d'une carte à puce comme dispositif d'authentification, il est recommandé, et tout particulièrement au niveau ***, d'utiliser un lecteur de carte à puce avec PIN/PAD intégré permettant de saisir son code d'activation et de le vérifier sans que celui-ci ne transite via l'ordinateur, la borne d'accès publique ou le serveur utilisés.

IV. Objectifs et périmètres des niveaux de sécurité

Les différents niveaux de sécurité identifiés dans la PRIS sont à voir plus comme des solutions de sécurité permettant de répondre à des objectifs de sécurité et des contraintes de mise en oeuvre plus ou moins forts, que comme des niveaux de qualité.

Vouloir viser arbitrairement un niveau de sécurité élevé en espérant atteindre un haut niveau de qualité mais ne répondant pas aux objectifs réels de sécurité de l'application entraînera des surcoûts importants (au niveau de l'application elle-même et/ou des utilisateurs de l'application), pouvant même aller jusqu'à remettre en cause la viabilité de l'application (faisabilité / difficulté de mise en œuvre de la solution).

Il est donc fondamental, pour un responsable d'application d'échanges dématérialisés, d'identifier ses objectifs de sécurité en matière d'authentification électronique, par rapport aux risques identifiés sur son application, et de positionner ces objectifs par rapport aux trois niveaux de sécurité définis dans la PRIS, ce positionnement permettant de déterminer les familles de certificats et les familles de produits d'authentification sur lesquelles son application peut ainsi s'appuyer.

Le tableau ci-dessous et les tableaux des deux chapitres suivants présentent de manière synthétique les principales différences entre les trois niveaux de sécurité identifiés pour le service d'authentification.

Le lecteur est invité à consulter la PC Type elle-même pour une vision complète et précise de toutes les différences et à consulter le document [Var_Temps] pour les différences relatives aux variables de temps concernant différents évènements du cycle de vie des clés cryptographiques et des certificats.

Domaine	Niveau ***	Niveau **	Niveau *
Contextes type d'utilisation	Risques **très forts** de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou aux biens de ces applications, ou pour pouvoir démontrer l'origine de données (intérêt pour les usurpateurs, attraits des biens, etc.).	Risques **forts** de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou aux biens de ces applications, ou pour pouvoir démontrer l'origine de données (intérêt pour les usurpateurs, attraits des biens, etc.).	Les risques de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou aux biens de ces applications, ou pour pouvoir démontrer l'origine de données, existent mais sont **moyens** (intérêt pour les usurpateurs, attraits des biens, etc.).

IV.1. Prestataires de Services de Certification Electronique

Domaine	Niveau ***	Niveau **	Niveau *
Validation initiale de l'identité du porteur	Contrôle de l'identité en face-à-face ou suivant une méthode équivalente (ex : signature avec un certificat et un outil ***).	Contrôle de l'identité en face-à-face ou suivant une méthode équivalente (ex : signature avec un certificat et un outil **).	Envoi du dossier d'enregistrement sous forme papier (avec copie certifiée conforme des pièces d'identité[1]) ou sous forme électronique (ex : signature avec un certificat et un outil **) ou communication d'un élément propre au futur porteur permettant de l'identifier au sein d'une base de données administrative pré-établie..
Remise / acceptation d'un certificat	- Remise en face-à-face si l'authentification du porteur se fait en face-à-face et que celui-ci n'a pas eu lieu à l'enregistrement. - Si l'AC ne génère pas la bi-clé, vérification que le certificat est bien associé à la clé privée correspondante (chargement à distance sur une carte à puce). - Acceptation explicite du certificat par le porteur.	- Remise en face-à-face si l'authentification du porteur se fait en face-à-face et que celui-ci n'a pas eu lieu à l'enregistrement. - Si possible, acceptation explicite du certificat par le porteur, au minimum, acceptation tacite à partir d'une date de remise suffisamment fiable.	- Remise par message électronique ou téléchargement. - Acceptation tacite.
Révocation d'un certificat	Authentification formelle de la demande via un mécanisme fort (ex : série de 4/5 questions / réponses, utilisation d'un certificat et d'un outil **,...) Service accessible 24h/24 et 7j/7, maximum 2h d'indisponibilité par mois. Délai, entre validation de la demande et mise à jour des informations de statuts, de moins de 24h, 7j/7.	Authentification formelle de la demande (ex : série de 3/4 questions / réponses, utilisation d'un certificat et d'un outil *,...) Service accessible 24h/24 et 7j/7, maximum 4h d'indisponibilité par mois. Délai, entre validation de la demande et mise à jour des informations de statuts, de moins de 24h, 7j/7.	Authentification de la demande par vérification de une ou deux informations de base sur le demandeur (n° de téléphone, adresse, ...) Service accessible au moins les jours ouvrées[2], maximum de 16h (jours ouvrées) d'indisponibilité par mois. Délai, entre validation de la demande et mise à jour des informations de statuts, de moins de 1 jour ouvré.

[1] Photocopie de la pièce d'identité, datée et signée par le titulaire de cette pièce et précédée de la mention "copie certifiée conforme à l'original".

[2] Jour ouvré = hors week-end et jours fériés légaux

Domaine	Niveau ***	Niveau **	Niveau *
Service d'état des certificats	Au minimum, publication de LCR. Recommandation de mise en oeuvre de deltaLCR et d'un service en ligne (OCSP). Service accessible 24h/24 et 7j/7, maximum 4h d'indisponibilité par mois.	Au minimum, publication de LCR. Recommandation de mise en oeuvre de deltaLCR et d'un service en ligne (OCSP). Service accessible 24h/24 et 7j/7, maximum 8h d'indisponibilité par mois.	Au minimum, publication de LCR. Recommandation d'un service en ligne (OCSP). Service accessible pendant les jours ouvrés, maximum de 32h (ouvrées) d'indisponibilité par mois.
Protection des clés d'AC (privées / publiques)	- Génération et mise en oeuvre des clés et des certificats d'AC dans un module cryptographique répondant aux exigences de l'annexe 2 de la PC Type, certifié à un niveau équivalent à EAL4+ et qualifié à un niveau renforcé de préférence. - Cérémonies des clés sous le contrôle d'au moins deux personnes (rôles de confiance) et au moins deux témoins externes (dont un officier public recommandé). - Contrôle des clés privées de l'AC par au moins deux personnes dans des rôles de confiance (porteurs de parts de secrets). - Activation des clés privées d'AC par au moins deux personnes dans des rôles de confiance.	- Génération et mise en oeuvre des clés et des certificats d'AC dans un module cryptographique répondant aux exigences de l'annexe 2 de la PC Type, certifié à un niveau équivalent à EAL2+ et qualifié à un niveau au moins standard. - Cérémonies des clés sous le contrôle d'au moins deux personnes (rôles de confiance) et au moins un témoin externe. - Contrôle des clés privées de l'AC par au moins deux personnes dans des rôles de confiance (porteurs de parts de secrets). - Activation des clés privées d'AC par au moins deux personnes dans des rôles de confiance.	- Génération et mise en oeuvre des clés et des certificats d'AC dans un module cryptographique répondant aux exigences de l'annexe 2 de la PC Type. - Cérémonies des clés sous le contrôle d'au moins une personne (rôle de confiance) et de plusieurs témoins. - Contrôle des clés privées par au moins une personne dans un rôle de confiance. - Activation des clés privées d'AC par au moins une personne dans un rôle de confiance.
Génération des clés privées des porteurs (si elles sont générées par l'AC en dehors du dispositif d'authentification du porteur)	- Génération dans un module cryptographique répondant aux exigences de l'annexe 2 de la PC Type, certifié à un niveau équivalent à EAL4+ et qualifié à un niveau renforcé de préférence.	- Génération dans un module cryptographique répondant aux exigences de l'annexe 2 de la PC Type, certifié à un niveau équivalent à EAL2+ et qualifié à un niveau au moins standard.	- Génération dans un module cryptographique répondant aux exigences de l'annexe 2 de la PC Type.

IV.2. Dispositifs d'authentification

Au niveau ***, la certification[3] du dispositif doit permettre de démontrer une assurance forte que le dispositif d'authentification répond bien aux exigences du § III.2 (équivalent à un niveau EAL4+[4] des critères communs avec une résistance élevée des mécanismes) et déboucher sur une qualification, de niveau renforcé de préférence [QUALIF_RENF].

[3] Dans les conditions prévues par le décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

[4] Le niveau EAL4 doit être augmenté par au moins le composant d'assurance AVA_VLA.4.

Au niveau **, la certification doit permettre de démontrer une assurance moyenne que le dispositif de création de signature répond bien aux exigences du § III.2 (équivalent à un niveau EAL2+[5] des critères communs avec une résistance élevée des mécanismes) et déboucher sur une qualification de niveau standard [QUALIF_STD].

Au niveau *, seule une déclaration de conformité du dispositif de création de signature aux exigences III.2 est exigée.

Domaine	Niveau ***	Niveau **	Niveau *
Dispositif d'authentification	Certification EAL4+ débouchant sur une qualification de préférence renforcée.	Certification EAL2+ débouchant sur une qualification standard.	Déclaration de conformité aux exigences.

[5] Le niveau EAL 2 doit être augmenté par au moins les composants d'assurance suivant ADV_HLD.2, ADV_IMP.1 (pour la classe fonctionnelle FCS), ADV_LLD.1 (pour la classe fonctionnelle FCS), ALC_DVS.1, ALC_FLR.3, ALC_TAT.1 (pour la classe fonctionnelle FCS), AVA_MSU.1, AVA_VLA.2.

V. Glossaire et acronymes

Les termes et acronymes utilisés dans le présent document sont ceux définis dans la PC Type "Authentification". Le lecteur est invité à se reporter au chapitre I.6 de cette PC Type.

VI. Documents de référence

Renvoi	Document
[CADRA]	*Note de cadrage de la politique de référencement intersectorielle de sécurité - Version 2.0 du 01/06/2005*
[CWA_14169]	*Secure Signature-creation devices "EAL 4+"*
[PC_AUTH]	*PRIS – Politique de certification type pour le service d'authentification - Version 2.0 du 01/06/2005*
[PREAMB]	*PRIS - Préambule - Version 2.0 du 01/06/2005*
[PROFILS]	*PRIS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.0 du 01/06/2005*
[QUALIF_STD]	*Processus de qualification standard, DCSSI, V 1.0 du 28/07/ 2003 N° 1591/SGDNDCSSI/SDR*
[QUALIF_RENF]	*Processus de qualification renforcée, DCSSI, V 1.0 du 24/06/04 N° 1549/SGDN/DCSSI/SDR*
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework - 11/2003*
[Socle_IAS]	*Socle commun carte à puce : Identification, Authentification, Signature pour les cartes de l'e-administration* *Disponible sur demande à l'adresse email pris.adae@pm.gouv.fr*
[VAR_TEMPS]	*PRIS - Politiques de Certification Types - Variables de Temps - Version 2.0 du 01/06/2005*