Agence de Mutualisation des Universités et Etablissements

CADRE DE COHERENCE S.I. DES ETABLISSEMENTS

ANNEXE TECHNIQUE

MARCHE DE REALISATION OU D'EVOLUTION DE COMPOSANTS SI

Note d'accompagnement de l'appel à commentaire sur le cadre de cohérence technique

Le comité de pilotage des systèmes d'information de l'enseignement supérieur et de la recherche a souhaité que soit produit un cadre de cohérence technique, récapitulant des normes techniques et des recommandations de nature à faciliter l'interopérabilité des applications et des services numériques.

Le document joint à cet envoi s'inscrit dans cette démarche. Le choix a été fait de le présenter sous forme d'une annexe technique qui devra être jointe aux dossiers de consultation des appels d'offre pour l'acquisition ou le développement de composants logiciels devant être intégrés dans le système d'information d'un établissement.

Cette annexe récapitule les normes et les règles techniques qui sont issues d'une part de la réglementation en vigueur (lois et décrets en particulier), d'instructions particulières propres à notre environnement (Ministère de l'enseignement supérieur et de la recherche, Direction centrale de la sécurité des systèmes informatiques etc.) ou de préconisations dont notre communauté a pu convenir pour développer l'interopérabilité des systèmes d'information.

Chaque règle est préfixée par le degré d'obligation avec laquelle elle s'impose, suivant la nomenclature en usage pour ce type de documents : « Il est OBLIGATOIRE de … », « Il est INTERDIT de », « Il est RECOMMANDE de ».

Le cadre de cohérence technique a vocation à s'imposer pour toutes les acquisitions de produits ou développements à venir.

Il évoluera dans le temps en conformité avec l'évolution des techniques et de la réglementation.

TABLE DES MATIERES

Remerciements

L'annexe technique a bénéficié des contributions et enrichissements de :

- Serge Aumont, Comité Réseaux des Universités
- Claude Bagnol, Université de Montpellier I
- Thierry Bédouin, Université de Rennes I
- Jacques Bernard, Agence de Mutualisation des Universités
- François Cade, Université de Paris V
- Magali Clareton-Perotin, Agence de Mutualisation des Universités
- Jacques François, Université de Lyon I
- **Frantz Gourdet, Agence de Mutualisation des Universités**
- Dominique Launey, Comité Réseaux des Universités
- Jean-Paul Le Guigner, Comité Réseaux des Universités
- Nicole Ludeau-Pavy, Université de Paris I
- Christian Michau, Agence de Mutualisation des Universités
- Isabelle Morel, Ministère de l'éducation nationale - Service du Haut Fonctionnaire de Défense et de Sécurité
- David Rongeat, Agence de Mutualisation des Universités
- Olivier Salaün, Comité Réseaux des Universités
- Pierre Verdier, Agence de Mutualisation des Universités

Des services de l'AMUE ont également contribué à la correction et à l'amélioration du document :

- Mission Système d'Information
- Mission Relations Etablissements
- Service des ressources informatiques
- Pôles Formation, Gestion financière et comptable, Intégration, Ressources humaines

1 - OBJET DU DOCUMENT

Ce document regroupe sous forme d'annexe générale les préconisations et contraintes techniques s'appliquant à la conception et aux évolutions des systèmes d'information d'établissements d'enseignement supérieur et de recherche *(on parlera d'Etablissements).*

Il s'articule autour d'appendices ayant vocation à évoluer en fonction de l'état d'avancement des travaux liés aux domaines traités.

Ainsi, lorsqu'existe un document finalisé, disponible en ligne et contenant les préconisations officielles émanant des organismes publics habilités à les émettre en direction des autorités administratives françaises, l'appendice traitant du domaine concerné s'y réfère directement.

Dans le cas contraire, l'appendice reprend ou formule des règles s'appliquant sous leur forme courante à la gestion et à l'évolution des systèmes d'information des *Etablissements* dans le respect du cadre légal français et européen.

Les règles réunies dans ce document renvoient à différents niveaux de préconisation, sur le modèle de la RFC 2119 :

- **OBLIGATOIRE** : niveau indiquant une exigence absolue généralement d'ordre légal ;
- **RECOMMANDÉ** : niveau signifiant que la règle édictée peut être ignorée après évaluation des conséquences tenant compte de circonstances particulières ;
- **DÉCONSEILLÉ** : niveau indiquant une prohibition qu'il est toutefois possible, en maîtrisant bien les conséquences et dans des circonstances particulières, de ne pas suivre ;
- **INTERDIT** : niveau indiquant une prohibition absolue généralement d'ordre légal.

Destinée principalement aux directeurs ou chefs de projets de système d'information en maîtrise d'œuvre, la présente annexe générale peut être librement jointe aux appels d'offres lancés par les *Etablissements*, ainsi qu'à ceux de l'AMUE[1].

[1] Voir glossaire p. 13

2 - INTEGRATION - INTEROPERABILITE

2.1 CONTEXTE D'INTEGRATION

La problématique d'intégration d'un composant du système d'information d'un Etablissement au système d'information global des Etablissements se pose aux niveaux fonctionnel et environnemental, interne et externe.

2.1.1 Intégration fonctionnelle

Ce type d'intégration concerne la communication entre différents domaines fonctionnels mis en œuvre dans les systèmes d'information.

Ce mode d'intégration se réalise par exemple au moyen :

- de formats d'échanges ;
- de référentiels communs ;
- ou d'un progiciel dit de « gestion intégrée » (PGI) : *le composant à intégrer est alors appréhendé comme un sous-ensemble de modules du PGI…*

2.1.2 Intégration environnementale interne

Ce type d'intégration porte sur l'insertion d'un composant du SI au sein du socle technologique existant, ainsi que sur les dispositifs permettant d'accéder aux (résultats des) traitements automatisés effectués par ce composant, depuis un ou plusieurs autres composants du SI d'un *Etablissement*, par exemple, depuis son Espace Numérique de Travail (ENT).

L'intégration environnementale interne d'un nouveau composant s'effectue par exemple :

- en aménageant une ouverture applicative du composant SI à intégrer autorisant la coopération de machine à machine entre ce composant et d'autres composants éventuellement hétérogènes et distants du SI d'un *Etablissement* : connecteurs, architectures orientées (web) services etc. ;
- en incorporant de manière transparente notamment avec des mécanismes d'authentification unique, un ou plusieurs types d'accès au composant concerné, dans un ou plusieurs portails web intra-Etablissement…

2.1.3 Intégration environnementale externe

Ce type d'intégration concerne la possibilité d'échanges entre *Etablissements* partenaires au niveau local, régional, national ou international. Externes à chaque *Etablissement* hébergeur, des accès habilités à interagir en création ou modification à des données locales sont mutuellement autorisés au sein de réseaux de partenariat.

Ce mode d'intégration diffère de l'intégration « environnementale interne» uniquement par le fait que les frontières du système considéré englobent plusieurs *Etablissements*.

Il s'agit par exemple dans ce cas :

- de mettre en œuvre un système de fédération d'identité ;
- d'incorporer dans un portail Internet ou intranet multi-établissements le composant SI à intégrer ;

- d'assurer au moyen du nouveau composant une fourniture de téléservices faisant au besoin coexister plusieurs environnements ou contextes spécifiques attachés à divers *Etablissements* « clients »…

2.1.4 Intégration et Interopérabilité

Les mises en œuvre possibles précédemment évoquées l'ont été à simple titre illustratif. Leur pertinence diminuera avec le temps, au fil des avancées technologiques.

De manière plus générale, intégrer un nouveau (composant de) système d'information dans les systèmes internes ou externes revient à aménager l'*interopérabilité* de ce nouveau système (ou composant) avec le patrimoine informationnel existant.

Cette interopérabilité peut être définie comme étant la capacité des systèmes d'information, ainsi que des processus sectoriels (ou « métiers ») que ces systèmes mettent en œuvre, à échanger des données et à partager des informations.

2.2 INTEROPERABILITE

Trois volets majeurs d'interopérabilité font l'objet de recommandations apparaissant dans l'*European Interoperability Framework* (EIF) - ou Cadre d'Interopérabilité Européen - publié en 2004 par la Commission Européenne, à savoir :

- Interopérabilité organisationnelle ;
- Interopérabilité sémantique ;
- Interopérabilité technique.

L'interopérabilité organisationnelle renvoie à la capacité à mettre en œuvre des objectifs et processus sectoriels (ou "métier") spécifiques permettant à des organisations ayant des structures et processus internes différents d'interagir, de collaborer à la fourniture de services (web) communs à des tiers, ou de procéder de manière régulière à des échanges automatisés d'informations.

L'interopérabilité sémantique vise, selon l'EIF, la signification précise des informations échangées, formatées de manière « compréhensible par toute autre application même non développée initialement à cet effet ». Ce type d'interopérabilité « permet aux systèmes de combiner l'information reçue avec d'autres ressources informationnelles » et d'en exploiter le sens. De manière plus opérationnelle, elle concerne le contenu informationnel (des échanges) et sa compréhension par les différents (systèmes) partenaires ; elle implique généralement la « définition et la normalisation de données et métadonnées, le choix de référentiels ou ressources de référence à mettre en œuvre par tous : répertoires d'identification, bases de données, nomenclatures et listes de valeurs. Les spécifications d'interopérabilité sémantique définissent un langage commun permettant aux applications des systèmes d'information participants d'interpréter de façon homogène la nature et les valeurs des données transmises et de les réutiliser sans erreur ou perte d'information. »

Finalement, l'interopérabilité technique couvre la mise en relation des systèmes et des services informatiques. Elle englobe les aspects tels que les interfaces ouverts, l'interconnexion des services, la présentation et l'échange de données, l'accessibilité et la sécurité.

Dans la présente annexe technique générale, l'accessibilité et la sécurité font l'objet de chapitres et d'appendices spécifiques.

2.3 REFERENTIEL GENERAL D'INTEROPERABILITE

L'article 11 de l'ordonnance 2005-1516 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives elles-mêmes, fait référence à un Référentiel Général d'Interopérabilité (RGI).

Par définition, ce RGI décline au plan national le Cadre d'Interopérabilité Européen, et spécifie « l'ensemble des règles dont le respect s'impose à tous pour faciliter les échanges et rendre cohérent l'ensemble constitué des systèmes d'information du service public, pour assurer la simplicité d'intégration de nouveaux systèmes et pour faciliter l'évolution du système global ainsi que son utilisation par tous les acteurs ».

2.4 REFERENTIEL D'INTEROPERABILITE APPLICABLE AUX ETABLISSEMENTS

Le référentiel général d'interopérabilité s'impose aux *Etablissements* à partir de la date de publication du décret fixant les conditions de son élaboration, approbation, modification et de sa publication. Avant cette date, le RGI n'a pas valeur de contrainte réglementaire.

Les *Etablissements* disposent (cf. 14.I de l'ordonnance 2005-1516) d'un délai de douze mois pour mettre en conformité avec le RGI les applications qui se créent dans les 6 mois suivants la date publication du décret. Pour les SI antérieurs à cette date, ce délai de mise en conformité est porté à trois ans.

Dans l'attente de la publication du décret d'application du RGI, l'**Appendice I** du présent document assemble les règles d'intégration et d'interopérabilité relevant de la maîtrise d'œuvre applicables au cadre de l'évolution et de l'acquisition de nouveaux composants SI par les *Etablissements*.

Cet appendice anticipe par défaut les niveaux de préconisations prévu au RGI. Pour prendre connaissance des adaptations de ce référentiel aux spécificités de l'*Etablissement* et du projet, se référer au volet « Adaptations des niveaux de préconisation des règles du RGI » en **Appendice IV**. Ledit volet présente la liste des règles d'interopérabilité dont le niveau de préconisation a été requalifié par la maîtrise d'ouvrage.

Sur le modèle prévu au RGI, l'**Appendice I** regroupe les recommandations liées aux aspects suivants :

- **Règles d'interopérabilité d'ordre général**
- **Interopérabilité technique**
  - **Interopérabilité des formats de données**
    - Codage des caractères
    - Formats des images fixes non photographiques
    - Formats des images fixes photographiques de qualité ordinaire
    - Formats des images fixes photographiques de haute qualité
    - Formats d'images fixes déconseillés
    - Récapitulatif sur les formats d'images fixes matricielles
    - Formats pour l'animation simple d'images
    - Formats pour l'animation complexe d'images
    - Formats pour les séquences sonores
    - Formats pour la vidéo basse définition
    - Formats pour l'audiovisuel et la vidéo haute définition (HD)
    - Formats des objets graphiques à deux dimensions
    - Formats pour les objets et univers virtuels en 3D
  - **Interopérabilité des formats de document**
    - Echange de documents non structurés
    - Echange de documents bureautiques en mode « collaboratif »
    - Echange de documents bureautiques en mode « informatif »
    - Conservation des documents bureautiques « statiques »

- Echange de données numériques d'impression
- Formats pour le dessin technique
- Formats pour la CAO et la production industrielle
- Format et échange des documents structurés
- Définition de schéma de documents structurés
- Exportation des bases de données
- Langages XSLT et XPath

❖ **Recommandations sur les IHM**
- Ergonomie des IHM
- Technologies pour construire les IHM Web
- Indépendance par rapport aux appareils et à leurs IHM
- Intégration de services Web par les IHM
- Syndication de contenu
- Validation de la conformité des pages Web

❖ **Interopérabilité des messageries électroniques**
- Protocole de messagerie électronique
- Représentation des messages et pièces jointes
- Sécurisation de la messagerie électronique
- Accès aux B.A.L. de la messagerie électronique
- Extensions à la messagerie électronique
- Mise en œuvre de la messagerie électronique
- Services de messagerie instantanée

❖ **Interopérabilité des services d'annuaire**
- Service d'annuaire
- Echanges de données entre annuaires
- Sécurisation du service d'annuaire

❖ **Interopérabilité des services techniques**
- Services de compression de fichiers
- Services de noms de domaines
- Services sécurisés de noms de domaines
- Services de transfert de fichiers : modèle IETF
- Services de gestion des Forums

❖ **Interopérabilité et Sécurisation des échanges**
- Protocoles d'échanges de messages
- Services de sécurisation des échanges
- Services de chiffrement des documents XML
- Services de signature des documents XML
- Services de sécurisation des «Web Services»
- Protocole de déclaration de données utilisateur
- Invocation de services
- Formats des certificats électroniques
- Formats des contremarques de temps
- Utilisation de mécanismes de cryptographie

❖ **Interopérabilité des protocoles**
- Protocole HTTP (couche application)
- Protocoles TCP et UDP (couche transport session)
- Protocole IP (couche réseau)
- Protocole IPsec (couche réseau)
- Protocoles d'horodatage technique et de synchronisation
- Protocoles pour la Téléphonie

- **Supports matériels**
  - Supports d'archivage
  - Cartes à puce et clés USB

- **Interopérabilité organisationnelle**
- **Interopérabilité sémantique.**

3 - SECURITE

3.1 REFERENTIEL GENERAL DE SECURITE (RGS)

Un Référentiel Général de Sécurité (RGS) est défini au 9.I de l'ordonnance 2005-1516 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives. Il a pour objet de :

- Préciser les procédures à suivre et les exigences qu'une offre ou un produit doit satisfaire pour obtenir une qualification attestant de sa capacité à atteindre un niveau défini pour les fonctions de sécurité réalisées.
- Eclairer les autorités administratives sur la marche à suivre pour intégrer pleinement la prise en compte des dispositions de l'ordonnance dans leur organisation globale de gestion de la sécurité des systèmes d'information. Cette intégration est en effet nécessaire car les acteurs sont souvent les mêmes que pour les systèmes n'entrant pas dans le champ d'application de l'ordonnance (autorités hiérarchiques, maîtres d'ouvrage, chefs de projet, architectes, développeurs, responsables sécurité, prestataires d'infogérance…). De plus l'identification des fonctions de sécurité (cf. 9.II de l'ordonnance) et leur réalisation relèvent pleinement d'une telle organisation.
- Identifier les fonctions de sécurité pour lesquelles les autorités administratives doivent sélectionner un niveau de sécurité, et de préciser les exigences correspondant à chaque niveau proposé.

3.2 REFERENTIELS DE SECURITE APPLICABLES AUX ETABLISSEMENTS

3.2.1 Le référentiel général de sécurité (RGS)

Les conditions d'élaboration, d'approbation, de modification et de publication du RGS sont à fixer par décret.

Avant la parution de ce décret, le RGS n'a pas valeur de contrainte réglementaire. Il pourra cependant être publié lors du déroulement du marché. A ce titre il s'imposera à l'*Etablissement* ayant passé le marché et donc au titulaire de ce marché.

Toutefois, les *Etablissements* disposent (cf. 14.I de l'ordonnance 2005-1516) d'un délai de douze mois pour mettre en conformité avec le RGS les applications qui se créent dans les 6 mois suivants la date publication du décret. Pour les SI antérieurs à cette date, ce délai de mise en conformité est porté à trois ans.

Dans l'attente de la publication du décret d'application du RGS, l'**Appendice II** du présent document rassemble les règles de sécurité relevant de la maîtrise d'œuvre et applicables au contexte de l'évolution et de la création de téléservices destinés aux usagers des composants SI des *Etablissements*. Cet **Appendice II** anticipe par défaut les niveaux de préconisations prévu au RGS. Pour prendre connaissance des adaptations de ce référentiel aux spécificités de l'*Etablissement* et du projet, se référer au volet « Adaptations des niveaux de préconisation des règles du RGS » en **Appendice IV**. Ce volet présente la liste des règles de sécurité dont le niveau de préconisation a été modifié par la maîtrise d'ouvrage.

3.2.2 Schéma directeur de la sécurité des systèmes d'information (SDSSI)

Le schéma directeur de la sécurité des systèmes d'information (SDSSI) publié par le ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche s'applique aux prestations de services sous traitées ou externalisées.

Ce document identifie et précise les "Principes de sécurité liés au cycle de vie du système d'information". Il comporte, en son annexe intitulé "Cadre commun de la sécurité des systèmes d'information et de télécommunication", les règles communes permettant la cohérence générale du niveau de sécurité des systèmes d'information dans les communautés éducatives ainsi que sa mise en œuvre opérationnelle.

Le SDSSI est téléchargeable dans sa dernière version à l'adresse suivante :
http://camel.amue.fr/CAMELBin/FormSuiviRESSOURCE?ID_RES=12 (cf. Onglet *Documents*)

Pour prendre connaissance des adaptations de ce référentiel aux spécificités de l'*Etablissement* et du projet, se référer au volet « Adaptations du SDSSI » en **Appendice IV**. Ce volet présente les adaptations jugées nécessaires validées par la maîtrise d'ouvrage.

Ces adaptations font suite à la démarche de gestion des risques faite par la maîtrise d'ouvrage assistée du responsable de la sécurité des systèmes d'information (RSSI), condition préalable obligatoire pour fournir à l'usager un téléservice de confiance, après fixation des objectifs globaux de sécurité et affectation des exigences de sécurité aux différents acteurs.

3.2.3 Adaptations gouvernées par le guide des clauses techniques de la DCSSI

En articulation avec la présente annexe technique générale, le volet intitulé « Clauses techniques particulières de sécurité applicables au projet » en **Appendice IV**, s'applique lui-même pleinement aux prestations demandées.

Pour les points « sécurité » relevant du contexte particulier de l'appel d'offres, ce volet est une adaptation/personnalisation du guide des clauses contractuelles élaboré par la Direction centrale de la sécurité des systèmes d'information (DCSSI) en matière générale d'externalisation de prestations de :

- développement applicatif ;
- tierce maintenance applicative ;
- infogérance ;
- élaboration de plan type d'assurance qualité.

4 - ACCESSIBILITE DES CONTENUS WEB

Pour tout nouveau composant du SI des *Etablissements* impliquant des navigateurs, des lecteurs multimédia, et tout autre logiciel ou agent Web, il convient de respecter et de ne pas entraver, par des choix ou insuffisances techniques, l'application des règles suivantes émises de manière à ce que tous ces « agents Web » soient davantage accessibles aux utilisateurs présentant des infirmités visuelles, auditives, physiques, mentales ou neurologiques :

- Accessibilité pour les Agents Utilisateurs (User Agent Accessibility Guidelines ou UAAG) portant notamment sur des dispositifs de navigation par clavier, les options de configuration, la documentation, la communication avec des logiciels dédiés tels que les agrandisseurs d'écran, les synthétiseurs vocaux, et le contrôle du rendu de tout type d'objets multimédia ;

- Accessibilité du Contenu Web (W3C/WAI/WCAG) à prendre en compte par les auteurs de ces contenus ;

- Accessibilité pour les Outils d'Edition (W3C/WAI /ATAG) à prendre en considération par les développeurs de logiciels lors de la conception d'outils d'édition accessibles aux personnes handicapées.

Une règle générique figure à l'**Appendice III**.

Pour prendre connaissance des adaptations aux spécificités du projet de ces règles d'accessibilité, ou de la liste de celles dont le niveau de préconisation a été modifié par la maîtrise d'ouvrage, se référer au volet « Adaptations des règles d'accessibilité » de l'**Appendice IV**.

5 - GESTION DES TRACES OU JOURNAUX INFORMATIQUES

Lors de la conception d'un composant SI transactionnel ou lors de son évolution, il convient de prévoir des dispositifs d'enregistrement systématique et temporaire d'informations caractérisant certaines transactions sous forme de journaux informatiques (encore appelés « traces » ou « logues ») destinés à rendre contrôlables la légalité, la fiabilité et la sécurité des transactions opérées. Ces journaux seront conçus de manière à contribuer à la détection de l'origine matérielle ou humaine : des défaillances ou anomalies de sécurité volontaires ou accidentelles, passives ou actives ; des usages abusifs du réseau ; de jouissances - illicites ou non - des moyens informatiques pouvant engager la responsabilité de l'*Etablissement*

Il est obligatoire de gérer les traces comportant des données à caractère personnel dans le respect des droits individuels et en toute conformité avec la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 dite loi « Informatique et libertés ».

Il est interdit, au travers d'un composant SI, d'aménager des accès aux journaux informatiques comportant des données à caractère personnel pour des utilisateurs non membres de la chaîne fonctionnelle SSI.

Lorsque le composant SI est destiné à traiter, à stocker ou à produire des traces, il est obligatoire de se mettre techniquement en cohérence avec la politique de gestion des journaux informatiques de l'*Etablissement*, de contribuer à son bon déroulement, et de ne pas introduire des contraintes ou insuffisances techniques de nature à entraver cette gestion.

Le référentiel définissant la politique type de gestion des traces, applicable aux établissements d'enseignement supérieur est téléchargeable à l'adresse suivante :

http ://www.cru.fr/activites/securite/index#document de travail du sds-sup

Pour prendre connaissance des adaptations aux spécificités de l'*Etablissement* de ce référentiel et de ses règles applicables à la maîtrise d'œuvre, se référer en **Appendice IV** au volet « Gestion des journaux informatiques ».

6 - GLOSSAIRE

THEME/CONCEPT	DEFINITION
AAS	Authentification – Autorisation – *SSO*
Authentification Autorisation SSO (AAS)	Problématique de gestion des identités et des habilitations
Accès pluriel	Accès clients portant sur plusieurs modes d'accès disponibles aujourd'hui : accès via un navigateur, un téléphone mobile, un *PDA*.
Accessibilité (du Web)	Principe visant à mettre le *Web* (tous les services et terminaux de navigation électroniques) à la disposition de tous les individus, quel que soit leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales. Ce même principe est notamment énoncé par l'*EIF* (recommandation n° 2) qui se base principalement sur les recommandations *WAI* et vise ainsi à favoriser « l'égalité des chances » (au moyen de services électroniques ouverts et accessibles sans discrimination vis-à-vis notamment des personnes handicapées).
Aides techniques (pour l'accessibilité du Web)	Outils matériels ou logiciels permettant à une personne en situation de handicap de consulter des services électroniques en ligne (exemple : plage braille et logiciel de synthèse vocale pour la consultation d'un site Internet par une personne aveugle).
Alerte	Avertissement qu'un incident a eu lieu
AMUE	Agence de mutualisation des universités et des Etablissements et de support à l'enseignement supérieur ou à la recherche (http ://amue.fr)
Antispam	Dispositif permettant de contrer l'envoi ou la réception de messages non sollicités (ou spam) par les utilisateurs.
Architecture logique	Description du système sous forme : d'une organisation structurée et hiérarchique des fonctions internes du système (fonctions, sous fonctions, composants logiques) et du *couplage* entre ces fonctions et l'environnement (vue statique) des flux de données et de contrôle entre ces entités logiques définissant le séquencement de leur exécution (vue dynamique). Cette description réalise les exigences fonctionnelles et les exigences de performances.
Archivage	Résultat de l'action d'archiver, c'est-à-dire de classer (des documents) dans les archives (ensemble de documents anciens, rassemblés et classés à des fins historiques). On distingue l'archivage volontaire, accessible à tout moment (sur disques magnéto-optiques, par exemple) de l'archivage résultant d'une politique de sauvegarde (incrémentielle, mensuelle, annuelle). L'archivage volontaire peut avoir une durée déterminée légalement, ou arbitrairement.

THEME/CONCEPT	DEFINITION
Application Service Provider (ASP)	Fournisseur (prestataire) d'application utilisable à distance au travers des réseaux informatiques.
ASP	Application Service Provider, ou Fournisseur d'applications hébergées (FAH).
Authentification unique (ou Single Sign-On)	Mécanisme permettant à un utilisateur d'accéder à des services numériques différents en ne devant s'authentifier qu'une seule et unique fois.
Autorisation	Mécanisme qui, à partir d'attributs, accorde ou non, à un utilisateur, l'accès à des applications, fonctions ou données spécifiques.
Autorité de certification (AC)	Autorité ayant en charge, au sein d'un PSCE, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du certificat), dans les certificats émis au titre de cette politique de certification.
Autorité d'horodatage (AH)	Autorité ayant en charge, au sein d'un PSHE, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage.
Back office	Système d'administration d'une solution informatique (telle que la gestion des produits), en opposition au « front office ». Le « back office » n'est pas accessible par les usagers cible de la solution mais réservé à des gestionnaires.
Base de connaissance	Base contenant des informations pertinentes pour faciliter le diagnostic et la résolution d'incidents
Brique	Composant
Cadre commun d'interopérabilité des systèmes d'information publics (CCI)	Cadre consolidant les bases nécessaires pour garantir une collaboration efficace au sein des collectivités publiques, et visant à répondre à la nécessité d'une interopérabilité accrue entre les systèmes d'information publics. Ce CCI est appelé à être remplacé par le *RGI* (Référentiel Général d'Interopérabilité)
Cadre d'interopérabilité	Ensemble de standards, indications et recommandations décrivant les modalités sur lesquelles les organisations se sont accordées, ou devraient s'accorder, pour faire interopérer leurs systèmes d'information.
CAS	Central Authentication Service
Cascading Style Sheet (CSS)	Standard de séparation présentation-contenu du W3C – Feuillles de style en cascade (http ://www.w3.org/style/CSS)
CCI	Cadre commun d'interopérabilité (des systèmes d'information publics)
Central Authentication Service (CAS)	Logiciel Open Source utilisé dans la plupart des établissements pour mettre en œuvre un système d'authentification à mot de passe unique (SSO).

THEME/CONCEPT	DEFINITION
Certificat cachet serveur	Certificat électronique dont la bi-clé associée est utilisée pour générer une signature électronique par un élément matériel ou logiciel. Cette signature électronique n'est pas réalisée par une personne physique. Puisque seule une personne physique peut signer au sens juridique du terme, il a donc été décidé de nommer ce certificat : cachet serveur, pour faire la distinction.
Certificat électronique	Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou de l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Un certificat et une bi-clé sont généralement réservés à un usage unique. Seul le double usage authentification et signature est toléré pour certains types de certificats.
Chaîne fonctionnelle SSI	Groupe d'agents ayant collectivement la responsabilité de la sécurité du système d'information de l'Etablissement et tenus au devoir de discrétion professionnelle, voire de secret professionnel selon leur rôle individuel : • Administrateur système et réseau ; • Correspondants de sécurité des systèmes d'information ; • Responsable de la sécurité des systèmes d'information (RSSI) ; • Autorité qualifiée de sécurité des systèmes d'information (AQSSI) ; • Fonctionnaire de sécurité de défense (FSD).
Client réseau banalisé	Application logicielle de consultation et de traitement du contenu des pages Web accessibles à l'utilisateur. Par exemple : un navigateur Web tel que Mozilla, Firefox, Netscape ou Internet Explorer ou une interface WAP.
Composant	Cf. composant technique
Composant technique	Module logiciel ou matériel participant à la cohérence d'un dispositif plus vaste (services socle, services applicatifs, services réseaux, par exemple) Par exemple : Un serveur web, un serveur d'application, un annuaire LDAP, une base de données sont des composants techniques logiciels Un poste de travail, une machine serveur, un PC sont des composants techniques matériels Certains composants tels qu'un pare-feu, un routeur, un proxy, un antivirus ou un *antispam* peuvent être des composants logiciels ou matériels
Contremarque de temps	Donnée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là
Contrôle d'accès	Principe ou dispositif de sécurité vérifiant l'identité et les droits associés à une entité en termes d'usage des services du système d'information.
Couplage (fort faible)	Interdépendance. Utilisé pour caractériser la relation de deux applications ou modules.

THEME/CONCEPT	DEFINITION
CSS	Cascading Style Sheet (feuilles de style en cascade)
Demande standard	Demande prédéfinie, compatible avec l'environnement de production et dont les coûts et les modalités sont également prédéfinis
Dématérialisation	Objectif de remplacement des supports d'information physiques par un support électronique
DCSSI	Direction centrale de la sécurité des systèmes d'information
DGME	Direction Générale pour la Modernisation de l'Etat. La DGME comprend trois services et un secrétariat général. Elle comprend en outre un département de la communication, un département de la formation et de l'accompagnement du changement et une mission des normes comptables directement rattachés au directeur général. Elle a été créée par arrêté du 30 décembre 2005 portant organisation de la direction générale de la modernisation de l'Etat, publié au JO du 01/01/2006.
Disponibilité	Propriété d'un système à de délivrer correctement le service (en terme de délai et de qualité) au moment où l'utilisateur en a besoin. La disponibilité est une mesure sans unité ; elle correspond à la proportion du temps de bon fonctionnement sur le temps total d'exécution du système.
DSI	Distribution Sélective d'Information
DSI	Directeur des Systèmes d'Information (Coordonnateur auprès de la maîtrise d'ouvrage)
EAI	Enterprise Application Integration, solutions du marché pour intégrer les systèmes d'information
EIF	European Interoperability Framework
ENT	Espace Numérique de Travail. Un espace numérique de travail désigne un dispositif global fournissant à un usager un point d'accès à travers les réseaux à l'ensemble des ressources et des services numériques en rapport avec son activité. Il est un point d'entrée pour accéder au système d'information de l'établissement.
Entité	Individu, utilisateur, processus ou serveur sécurisé.
EPLE	Etablissement public local d'enseignement
Espace de travail	Terme employé pour définir l'ensemble des interfaces utilisateurs de l'ENT. Ces interfaces pourront être, par exemple, représentées par une ou plusieurs fenêtres de navigateur web dans le cas de client réseau banalisés de type PC ou Mac.
Espace Numérique de Travail	Dispositif global fournissant à un utilisateur un point d'accès à travers les réseaux à l'ensemble des ressources et des services numériques en rapport avec son activité. L'ENT doit favoriser la mutualisation des services et des ressources.

THEME/CONCEPT	DEFINITION
Etablissement	On appellera, dans ce document, « établissement » les structures d'enseignement reconnues par l'Etat comme les écoles, collèges, lycées, écoles d'ingénieur, universités, etc.
Etablissement public local d'enseignement (EPLE)	Statut juridique qui regroupe les lycées et les collèges publics.
European Interoperability Framework (EIF)	Cadre d'Interopérabilité Européen
eXtended Stylesheet Language (XSL)	Langage gérant la représentation d'un contenu XML
Fédération d'identités	Principe de partage et de mise en relation d'informations relatives à un utilisateur entre plusieurs applications ou plusieurs domaines de confiance. La relation établie entre chaque service ou entité peut permettre de reconnaître l'identité physique d'un individu ou, au contraire, de garantir son anonymat.
Ferme de serveurs	Regroupement de serveurs
File Transfer Protocol (FTP)	Protocole de transfert de fichier via Internet
Fonction	Action attendue d'un composant technique (ou réalisée par lui) pour répondre à tout ou partie d'un besoin d'un utilisateur ou d'un service du système d'information. Par exemple, l'authentification, l'identification et l'autorisation sont des fonctions s'appuyant sur des composants logiciels tels que l'annuaire LDAP et le serveur web.
Format d'échange	Modèle des informations échangées par deux partenaires dans le contexte d'une coopération
File Transfer Protocol (FTP)	Protocole Internet de transfert de fichier
FTP	File Transfer Protocol
GIF	Graphic Interchange Format
Graphic Interchange Format (GIF)	Format propriétaire (Unisys après CompuServe, 1987 – brevet tombé dans le domaine public) très répandu d'échange de données graphiques.
Helpdesk	Service d'aide aux utilisateurs utilisant des procédures industrielles de suivi d'incident et de résolution de problèmes des usagers (dispositif asynchrone ou hotline)
Hotline	Partie du helpdesk qui est disponible par téléphone ou par messagerie instantanée, et qui traite les demandes d'assistance en temps réel
HTML	HyperText Markup Language
HTTP	Hyper Text Transport Protocol
Hyper Text Transport Protocol (HTTP)	Protocole de base de l'Internet

THEME/CONCEPT	DEFINITION
HyperText Markup Language (HTML)	Groupe de langages standard sous-tendant le World Wide Web (http ://www.w3.org/markup) – Standard d'Internet le plus vulgarisé
Identification	Association d'une personne physique, composant ou élément logiciel à une identité numérique aux moyens d'identifiants : adresse email, login/compte, certificat etc.
IETF	Internet Engineering Task Force
IETF	L'IETF regroupe des personnes physiques et des organisations intéressées par les évolutions du web. Les membres élaborent des propositions de normes ou bien fournissent des procédures de création de normes, qu'utiliseront par la suite d'autres organismes de normalisation (W3C, ISO,…). Plus précisément, l'IETF a pour fonction : -d'identifier et de résoudre les problèmes immédiats affectant le fonctionnement de l'internet ; -de spécifier des protocoles ou des architectures de réseaux susceptibles de limiter ces problèmes à l'avenir ; -d'émettre des propositions de normes et de standards pour le web ; -et de favoriser les transferts de technologies et d'informations en direction de la communauté du web.
IHM	Interface Homme Machine. L'interaction humain/machine, interaction Homme/machine ou interface Homme/machine (IHM) étudie la façon dont les humains interagissent avec les ordinateurs ou entre eux à l'aide d'ordinateurs, ainsi que la façon de concevoir des systèmes informatiques qui soient ergonomiques, c'est-à-dire efficaces, faciles à utiliser ou plus généralement adaptés à leur contexte d'utilisation
IHM	Interface Homme Machine ou Interaction Humain Machine ou Interaction Homme/machine
Industrialisable	Apte à être industrialisé.
Industrialisé	Terme utilisé pour caractériser un système répondant à des normes, des procédures et des réglementations appliquées à des entreprises et applicables aux services internes des administrations.
Infrastructure de gestion de clés (IGC)	Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.
Internet Engineering Task Force (IETF)	Communauté internationale ouverte regroupant des personnes physiques et des organisations intéressées par les évolutions du web dont la mission est précisée dans le RFC 3935 : Identifier et de résoudre les problèmes immédiats affectant le fonctionnement de l'internet ; Spécifier des protocoles ou des architectures de réseaux susceptibles de limiter ces problèmes à l'avenir ; Emettre des propositions de normes et de standards pour le web ; Favoriser les transferts de technologies et d'informations en direction de la communauté du web. Les membres élaborent des propositions de normes ou bien fournissent des procédures de création de normes, qu'utiliseront par la suite d'autres organismes de normalisation (W3C, ISO,…).

THEME/CONCEPT	DEFINITION
Interopérabilité	Capacité de deux applications distinctes, et éventuellement hétérogènes et distantes, à coopérer. L'interopérabilité peut également se définir comme la « faculté » que possèdent des services ou des composants hétérogènes de fonctionner conjointement. L'une des conditions fondamentales permettant la communication entre ces services et ces composants est l'utilisation de langages et de protocoles communs. Par exemple, les protocoles SOAP ou XML sont normalisés et permettent aux différents services web d'échanger des informations selon les mêmes règles et les mêmes méthodes.
Interopérabilité organisationnelle	Capacité à identifier les acteurs et les procédures organisationnelles intervenant dans la fourniture d'un service spécifique d'administration en ligne et de parvenir à structurer leur interaction. En d'autres termes, il s'agit pour les organisations participantes de définir leurs « interfaces d'entreprise ». L'interopérabilité organisationnelle concerne principalement la définition de processus qui sont mis en œuvre lors d'échanges entre administrations ou avec les usagers. Le but, selon l'EIF, est de mettre en ligne des services disponibles, facilement identifiables, accessibles et centrés sur l'usager, mais sécurisés et performants aussi bien en « utilisation usager » qu'en « gestion-administration » par les agents.
Interopérabilité sémantique	Volet d'interopérabilité concernant le contenu informationnel (des échanges) et sa compréhension par les différents (systèmes) partenaires : définition et normalisation des données et métadonnées, choix des référentiels ou ressources de référence qui seront mis en œuvre par tous : répertoires d'identification, bases de données, nomenclatures et listes de valeurs. Les spécifications d'interopérabilité sémantique définissent un langage commun permettant aux applications des systèmes d'information participants d'interpréter de façon homogène la nature et les valeurs des données transmises et de les réutiliser sans erreur ou perte d'information.
Interopérabilité technique	Volet d'interopérabilité couvrant la mise en relation des systèmes et services informatiques et incluant les aspects importants tels que les connecteurs (interface ouverts), l'interconnexion des services, l'intégration des données et les *middlewares*, la présentation et l'échanges de données, l'accessibilité et la sécurité
ISAD(G)	Standard définissant les règles à suivre et les éléments nécessaires pour la description des documents archivés. Ce standard a été pris en compte dans le Standard d'échanges de données pour l'archivage, en complément avec la DTD EAD (Encoded Archival Description), qui en est une implémentation, pour définir les éléments nécessaires à la description des données échangées.
ISO 10646	Norme s'appliquant à la représentation, à la transmission, à l'échange, au traitement, au stockage, à la saisie et à la présentation des langues du monde sous forme écrite et de symboles complémentaires. Elle a permis d'unifier les différents codages de caractères complétant le code ASCII, et d'y intégrer des codages complètement différents comme par exemple le code JIS pour le Japonais. La version 5.0.0 de la recommandation UNICODE définit un ensemble de caractères, de noms et de représentations codées identiques, caractère par caractère, à l'ensemble de l'ISO/IEC 10646 :2003. Elle fournit, de surcroît, des informations supplémentaires relatives aux propriétés de

THEME/CONCEPT	DEFINITION
	ces caractères, aux algorithmes de traitement ainsi que des définitions utiles aux développeurs. La norme ISO 10646 :2003 a été adoptée par de nouveaux protocoles Internet et mise en œuvre dans des systèmes d'exploitation et des langages informatiques. Elle contient plus de 95.000 caractères des écritures utilisées par les communautés du monde entier. Ceci favorise l'interopérabilité et l'échange de données au niveau international. Ce codage est donc recommandé dans un contexte d'échanges internationaux.
ISO 14721 :2003	Norme conceptuelle définissant les objets d'information, les métadonnées nécessaires à leur préservation et l'organisation à mettre en place pour leur archivage, leur conservation et leur communication. Cette norme a été prise en compte par le Standard d'échanges de données pour l'archivage pour définir les acteurs, les échanges et les objets d'informations échangés.
ISO 8859-15 (Latin 9)	Norme publiée en 2006 corrigeant les erreurs résiduelles du jeu de caractères ISO-8859-1 (Latin 1) et introduisant notamment le caractère € de l'euro et complétant le support du Français (OE, oe, Ÿ).
ISO-8859-1 (Latin 1)	Extension du code ASCII comportant les caractères accentués des langues d'Europe de l'ouest
J2EE	Plate-forme de développement d'application s'appuyant sur le langage Java, dont les spécifications sont gérées par la société SUN.
Jeton d'horodatage	Même signification que contremarque de temps.
JPEG	Joint Photographic Experts Group
LCMS	Learning Content Management System (système de gestion des contenus pour l'apprentissage)
LDAP	Lightweight Directory Access Protocol
Lightweight Directory Access Protocol (LDAP)	Standard d'accès aux annuaires établi par l'IETF (http://www.rfc-editor.org/rfc/rfc3377.txt). Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client, et non la manière de laquelle les informations sont stockées. Le protocole LDAP en est actuellement à la version 3 et a été normalisé par l'IETF (Internet Engineering Task Force). Ainsi, il existe une RFC pour chaque version de LDAP, constituant un document de référence. Ainsi LDAP fournit à l'utilisateur des méthodes lui permettant de : • se connecter ; • se déconnecter ; • rechercher des informations ; • comparer des informations ; • insérer des entrées ; • modifier des entrées ; • supprimer des entrées ; D'autre part le protocole LDAP (dans sa version 3) propose des mécanismes de chiffrement (SSL, …) et d'authentification (SASL) permettant de sécuriser l'accès aux informations stockées dans la base.

THEME/CONCEPT	DEFINITION
Learning Content Management System (LCMS)	Outil de gestion de contenus de formation, de gestion et de distribution de formation en ligne. Les LCMS incluent des fonctions de LMS (cf ci-dessous).
Learning Management System (LMS)	Logiciel de gestion et de distribution de formation en ligne
LMS	Learning Management System (système de gestion de l'apprentissage)
Maîtrise d'œuvre (MOE)	Entité retenue par le maître d'ouvrage pour réaliser l'ouvrage, dans les conditions de délais, de qualité et de coût fixées par ce dernier conformément à un contrat. La maîtrise d'œuvre est donc responsable des choix techniques inhérents à la réalisation de l'ouvrage conformément aux exigences de la maîtrise d'ouvrage. Le maître d'œuvre a ainsi la responsabilité dans le cadre de sa mission de désigner une personne physique chargée du bon déroulement du projet (on parle généralement de maîtrise du projet), il s'agit du chef de projet. La maîtrise d'ouvrage maîtrise l'idée de base du projet, et représente à ce titre les destinataires finaux de l'ouvrage/livrable. Ainsi, le maître d'ouvrage est responsable de l'expression fonctionnelle des besoins mais n'a pas forcément les compétences techniques nécessaires à la réalisation de l'ouvrage.
Maîtrise d'ouvrage (MOA)	Entité porteuse d'un besoin, définissant l'objectif, l'ouvrage/résultat/livrable attendu, le budget et le calendrier d'un projet.
Middleware	Logiciel d'intermédiation pour permettre une interopérabilité applicative
Montée en charge	Augmentation de la charge infligée à un serveur, ou de manière plus large à une infrastructure technique, qui est la conséquence d'un accroissement du nombre d'utilisateurs et/ou du volume des données et/ou du nombre d'applications.
MoReq	Model Requirements for the Management of Electronic Documents and Records/Modèle d'exigences pour l'organisation de l'archivage électronique au niveau Européen
Multilinguisme	Principe énoncé par l'EIF visant la neutralité linguistique au niveau back office des téléservices (XML-schemas) ou à défaut l'utilisation de mécanismes de traduction afin d'assurer des services multilingues aux usagers (niveau front office)
NAF	Nomenclature d'activités européennes
Nomenclature d'activités européennes (NAF)	Nomenclature d'activités très utilisée puisqu'elle sert à la codification des Activités principales des Entreprises et Etablissements (code APE) dans le Répertoire national des entreprises SIRENE. Une valeur NAF figure sur les bulletins de paie des salariés du secteur privé (3 chiffres plus une lettre). La NAF est nationale. Elle fait partie d'un important système articulé de nomenclatures d'activités et de produits dont les postes d'activités sont strictement compatibles aux niveaux européen (NACE) et international (CITI). La version de la NAF actuellement en usage est entrée en vigueur en 2003, sous l'intitulé

THEME/CONCEPT	DEFINITION
	NAF, révision 1. Elle sera remplacée en janvier 2008 par une version reprenant directement les concepts mais aussi les codes de la nomenclature européenne NACE (4 chiffres) auxquels sera ajoutée une lettre pour l'adapter aux spécificités françaises non intégrées dans la nomenclature européenne.
OASIS	Organization for the Advancement of Structured Information Standards
Object Management Group (OMG)	0rganisme de standardisation pour ce qui concerne la technologie objet (UML par exemple)
Objet métier	Elément conceptuel représentatif et caractéristique d'un métier donné. Peut aussi être défini comme une unité structurée et limitée conçue pour représenter les processus et les connaissances d'un métier en particulier (souvent dans une application).
OMG	Object Management Group
Ordonnanceur de tâches	Outil utilisé pour l'ordonnancement de tâches, c'est-à-dire l'exécution automatique de tâches à intervalles de temps réguliers ou bien à des moments précis.
Organization for the Advancement of Structured Information Standards (OASIS)	Consortium d'industriels visant à promouvoir l'utilisation de standards ouverts et auteur de nombreuses spécifications liées à XML
Outil de recherche	Dispositif permettant d'indexer les informations et les documents. Du côté utilisateur, ce dispositif permet, à partir de mots clés, de rechercher et d'afficher les informations relatives à la demande.
Pages blanches	Service permettant la consultation d'une base de données contenant les noms des membres d'une communauté, leur téléphone, courrier électronique, adresse et des données complémentaires comme leur photo, site Internet personnel, etc. (ne pas confondre avec l'annuaire qui gère l'identification de l'usager, son appartenance à un groupe).
Personnalisable	Caractère modifiable/modelable de la présentation d''un contenu au moyen notamment du choix explicite parmi une sélection d'options (service de personnalisation).
Personnalisée (diffusion)	Les éléments de personnalisation tels que l'accès aux services et la présentation de l'espace de travail sont définis par des règles s'appuyant sur les informations des utilisateurs (son profil notamment). Ces éléments ne sont pas modifiables par l'utilisateur.
Plan d'urbanisme	Représentation de la cible système d'information à atteindre
Plate-forme	Ensemble des composants matériels et logiciels, mis en œuvre de manière cohérente pour fournir les services d'un SI et lié à un domaine d'activités (réalisation, intégration, production, …)
Plate-forme technique	(cf. socle technique)
Plug-in	Petit module qui s'installe sur un navigateur web pour lui apporter des fonctions supplémentaires. Par exemple, visionner de la vidéo sur des paqes Web ou afficher des scènes en trois dimensions.

THEME/CONCEPT	DEFINITION
PNG	Portable Network Graphics
Politique d'horodatage (PH)	Ensemble de règles, identifié par un nom ou un numéro unique (appelé « OID » pour « Object Identifier »), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.
POP3	(Post Office Protocol version 3) Protocole de messagerie utilisé pour la réception des messages électroniques.
Poste client	Appareil informatique permettant à un usager de consulter des services en ligne avec un navigateur web affichant des pages au format HTML 4.0 ou selon d'autres formats (WAP, Imode…).
PréAO	Présentation assistée par ordinateur
PREMIS	Preservation metadata : implementation strategies
Pré-production	Environnement permettant de « recetter » les applications et de prononcer la VABF (Vérification d'Aptitude au Bon Fonctionnement).
Preservation metadata : implementation strategies (PREMIS)	Format proposant un cadre pour la gestion de la conservation des documents numériques. Le dictionnaire PREMIS a été utilisé lors de l'élaboration du Standard d'échanges de données pour l'archivage pour vérifier qu'aucune information de pérennisation importante à fournir par le service versant n'avait été oubliée.
Prestataire de service de confiance (PSCo)	Toute personne ou entité offrant des services consistant en la mise en oeuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.
Prestataire de services de certification électronique (PSCE)	Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié, dans un certificat dont il a la responsabilité, au travers de son AC qui a émis ce certificat et qui est elle-même directement identifiée dans le champ « issuer » du certificat.
Prestataire de services d'horodatage électronique (PSHE)	Toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en

THEME/CONCEPT	DEFINITION
	fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des Unités d'Horodatage dont il a la responsabilité au travers de ses Autorités d'Horodatage.
PRIS – (Politique de Référencement Intersectorielle de Sécurité)	Il s'agit d'un référentiel documentaire, qui définit des exigences pour les fonctions de sécurité suivantes utilisant des certificats électroniques : l'identification, la signature électronique, la confidentialité ainsi que la fonction d'horodatage. La PRIS concerne les produits de sécurité et les offres des prestataires de services de confiance. Les spécifications techniques retenues dans la PRIS sont regroupées sous la forme de niveaux de sécurité d'exigences croissantes, allant de une étoile (*) à trois étoiles (***).
Profil	Ensemble de traits (un ou plusieurs) caractérisant l'identité d'une personne dans un système donné. Par exemple, un utilisateur pourra avoir : Un profil macroscopique « élève, personnel administratif, chef d'établissement » et un profil microscopique « administrateur d'une application » ou « lecteur » ; ce profil est généralement géré au niveau de l'application
Promoteur d'application	Personne responsable de la définition, du développement et de la mise en place d'une application. Une application peut être un téléservice, un service ou une application client/serveur.
Propagation des identités et des droits	Transfert, échange des informations relatives aux identités numériques et/ou profils et/ou accréditations entre applications, services et autres entités (utilisation de carte de vie quotidienne, inter-administration, identités accord-Education, liaison sco-sup …).
Protection des données personnelles	Principe énoncé par l'EIF (recommandation n°2) basé principalement sur des exigences légales émises par les organismes européens homologues à la CNIL, et visant à ce que les personnes puissent contrôler, rectifier ou autoriser ou non l'usage des données les concernant à des fins autres que celles pour lesquelles elles ont été fournies initialement.
Provisioning	Processus par lequel un référentiel central permet de synchroniser les informations avec des bases d'informations applicatives
Qualification d'un prestataire de services de certification électronique	L'acte par lequel un organisme de qualification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) aux exigences de la PRIS, pour un niveau de sécurité et pour des services de certificats déterminés. Au sein des administrations de l'État, les règles de qualification des PSCE et des PSHE s'appliquent au niveau des AC ou des AH correspondantes.
Qualification d'un prestataire de services de confiance	L'acte par lequel un organisme de qualification atteste de la conformité de tout ou partie de l'offre de service d'un PSCo aux exigences de la PRIS, pour un niveau de sécurité donné et correspondant au service visé par le PSCo.
Qualification d'un prestataire de services d'horodatage électronique	L'acte par lequel un organisme de qualification atteste de la conformité de tout ou partie de l'offre d'horodatage d'un PSHE à la PH Type de la PRIS.
Qualification d'un produit de sécurité	L'acte par lequel la DCSSI atteste de la capacité d'un produit à assurer, avec un niveau de sécurité donné, les fonctions qu'il prend en

THEME/CONCEPT	DEFINITION
	charge. Le niveau de sécurité effectivement atteint est évidemment conditionné par l'adéquation des conditions d'utilisation du produit, conditions dont l'autorité administrative fait son affaire.
RDF	Resource Description Framework
Resource Description Framework (RDF)	Cadre de description de ressources : standard du W3C (http ://www.w3.org/rdf)
Recommandation pour les annuaires de l'enseignement supérieur : SUPANN	Cette annexe du *SDET* donne des recommandations annuaires compatibles avec les préconisations existantes au niveau interministériel (ADAE) ainsi qu'au niveau international (Internet2) et satisfaisant les spécificités relatives aux Etablissements d'enseignement supérieur.
Recommandations pour la gestion de l'Authentification autorisation-SSO : AAS	Cette annexe du *SDET* traite de l'identification, l'authentification, la gestion des autorisations et du Single Sign-On (AAS)
Référencement	Opération réalisée par l'Administration et qui atteste que l'offre de service du PSCo ou le produit concerné est utilisable avec tous les téléservices qui requièrent ce type de service ou de produit et exigent le niveau de sécurité correspondant. Une offre référencée pour un service donné et un niveau de sécurité donné de la PRIS peut être utilisée dans toutes les applications d'échanges dématérialisés requérant ce service et jusqu'à ce niveau de sécurité. Pour les usagers, le référencement permet de savoir quelles offres de service de sécurité ou quels produits ils peuvent utiliser pour tel ou tel échange dématérialisé. Le référencement des AC ou AH des autorités administratives répond aux mêmes critères.
Référentiel	Ensemble structuré d'informations, utilisé pour l'exécution d'un logiciel, et constituant un cadre commun à plusieurs applications. On associe généralement le référentiel à l'annuaire LDAP de référence pour les fonctions de contrôle d'accès.
Référentiel accessibilité des services Internet de l'administration française	Référentiel commun proposé aux différents acteurs sur la base duquel seront développés et évalués les sites et services Intranet et Internet offerts par l'administration française. L'innovation technologique autorise en effet l'accès et la restitution de l'information au travers de nombreux canaux qui peuvent exclure certaines catégories d'usagers. L'adoption de standards et de règles communes pour satisfaire aux exigences d'accessibilité telles que définies par le W3C/WAI (Web Accessibility Initiative, www.w3.org/WAI) permet d'éviter ce problème.
Référentiel général d'interopérabilité (RGI)	Le RGI spécifie l'ensemble des règles dont le respect s'impose à tous pour faciliter les échanges et rendre cohérent l'ensemble constitué des systèmes d'information du service public, pour assurer la simplicité d'intégration de nouveaux systèmes et pour faciliter l'évolution du système global ainsi que son utilisation par tous les acteurs.
Restauration	Remise d'un système dans des conditions de fonctionnement antérieures à une interruption. Restitution de fichiers sauvegardés.

THEME/CONCEPT	DEFINITION
RGI	Référentiel général d'interopérabilité
RSS	RDF Site Summary (Résumé de site en RDF), standard de syndication de contenus (http ://web.resource.org/rss/1.0/)
RSSI	Responsable de la sécurité des Systèmes d'information
RTF	Rich Text Format, un format de document standard Microsoft (http ://msdn.microsoft.com/library/ ?url=/library/en-us/dnrtfspec/html/rtfspec.asp ?frame=true)
S3IT	Schéma stratégique des systèmes d'information et de télécommunication
Schéma stratégique des systèmes d'information et des télécommunications (S3IT)	Document commun aux ministères de la recherche et de l'éducation nationale (<http ://www.education.gouv.fr/S3IT/default.htm>).
Schéma directeur	Programme opérationnel définissant actions et projets permettant d'atteindre la cible définie par le plan d'urbanisme
Schéma directeur des espaces numériques de travail (SDET)	Schéma directeur s'inscrivant dans le Schéma stratégique des systèmes d'information et de télécommunication (*S3IT*) du ministère, et visant à fournir un cadre de cohérence entre les offres d'espaces numériques de travail, en lien avec les infrastructures sécurisées et les systèmes d'information existants. Cadre essentiel pour le développement des TIC dans l'éducation piloté par la direction de la technologie. La version 1 du schéma directeur des environnements numériques de travail a été publiée en janvier 2004, la version 2 en 2007
SCORM	Spécification permettant de créer des objets pédagogiques structurés et de gérer leur inter relation avec des LMS / LCMS (norme publiée par l'armée américaine et utilisée par l'OTAN)
Secret métier	Informations confidentielles (n° de carte, n° de rôle, n° de facture …) connues du fournisseur d'un téléservice et d'un (*Etablissement*) bénéficiaire, et fondant l'attribution de droits d'accès au téléservice, à un usager/demandeur autorisé par le bénéficiaire. Le secret métier vise à assurer au bénéficiaire du téléservice que seul un usager autorisé agira pour son compte.
Secret technique	Informations confidentielles envoyées par le fournisseur d'un téléservice à l'*Etablissement* bénéficiaire de ce téléservice, a priori ou sur demande d'un futur usager rattaché à cet Etablissement, et visant à assurer que l'usager demandeur est autorisé à agir pour le compte du bénéficiaire du téléservice.
SDET	Schéma directeur des espaces numériques de travail
SDSSI	Schéma directeur de la sécurité des systèmes d'information
Serveur d'application	Environnement logiciel d'exécution des applications côté serveur (par

THEME/CONCEPT	DEFINITION
	opposition à côté client) prenant en charge l'ensemble des fonctionnalités qui permettent aux clients réseaux d'utiliser une même application : Gestion des sessions utilisateurs Gestion des montées en charge et reprise sur incident Ouverture sur de multiples sources de données
Serveur d'intégration	Dispositif ayant vocation à interfacer des services applicatifs et à assurer la transformation des données afin de garantir la cohérence d'un ensemble matériel et logiciel.
Serveur Web	Serveur jouant principalement le rôle de transmetteur de contenu web. Il faut considérer 2 cas : Dans le cas de pages statiques (HTML, images, fichiers CSS …), le serveur Web transmet les pages correspondant à la requête HTTP (via URL) du client Dans le cas de pages dynamiques (PHP, JSP, ASP…), c'est-à-dire nécessitant un traitement, le serveur web aiguille la demande vers le serveur d'application. Une fois le traitement effectué, le serveur d'application renvoie la page HTML (ou autre format) au serveur Web qui se charge de la router vers le bon destinataire (typiquement le client) D'autres fonctions telles que l'authentification peuvent également être assurées par le serveur Web.
SGBD (SGBDR)	Système de Gestion de Base de données (Relationnelle)
Simple Mail Tranfer Protocol (SMTP)	Protocole du courrier électronique
SMTP	Simple Mail Tranfer Protocol
Service Oriented Architecture (SOA)	Architecture de services (Web)
SOA	Service Oriented Architecture
Simple Object Access Protocol (SOAP)	Protocole du W3C faisant partie du standard Web Services (http ://www.w3.org/TR/SOAP/)
SOAP	Simple Object Access Protocol
SQL	Structured Query Language : langage de définition de données (Création, Modification, Suppression), un langage de manipulation de données (sélection, insertion, modification ou suppression des données dans une table d'une base de données relationnelle), et un langage de contrôle de données pour les bases de données relationnelles.
Single Sign-On (SSO)	Méthode d'authentification unique (ou identification unique) permettant à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs applications (ou sites web sécurisés).
SSO	Single Sign-On (authentification unique)

THEME/CONCEPT	DEFINITION
Standard d'échanges de données pour l'archivage	Standard d'échanges de données élaboré par la Direction des Archives de France du Ministère de la culture et de la communication et le SDAE de la DGME du Ministère des finances pour l'archivage prenant en compte la norme ISO 14721 :2003, le standard ISAD(G) les métadonnées prévue par *Moreq* et le dictionnaire *PREMIS*
Subsidiarité	Principe stipulant que les recommandations contenues dans l'EIF n'interfèrent pas avec les travaux internes des administrations et des institutions de l'Union Européenne, et qu'il appartient à chaque état membre et institutions de l'Union de prendre les mesures nécessaires pour assurer l'interopérabilité à un niveau pan européen.
SUPANN	Recommandation en matière d'annuaire pour l'enseignement supérieur
TIC	Technologies de l'information et de la communication
TICE	Technologies de l'information et de la communication pour l'éducation
UDDI	Universal Description, Discovery, and Integration of Web Services
UML	Unified Modelling Language, langage de modélisation pour les objets métier et les formats d'échange – standard lié aux Web Services (http ://www.uddi.org)
UML	Unified Modeling Language
UN/CEFACT	Centre pour la facilitation des procédures et des méthodes pour l'administration, le commerce et les transports / United Nations Centre for Trade Facilitation and Electronic Business
Unified Modeling Language (UML)	Langage objet graphique et textuel permettant de représenter et de modéliser des données et des processus, des interactions entre systèmes ou composants, et d'organiser les données, les composants ou les systèmes dans différents types de hiérarchie (taxinomie, composition, package, composant, etc.). UML permet d'une part de représenter dans une même entité (la classe) les aspects structurels et comportementaux d'un concept et d'autre part de pouvoir décrire une taxinomie, c'est-à-dire de hiérarchiser les concepts du plus général au plus spécifique, ces derniers héritant des caractéristiques des plus généraux.
Universal Description, Discovery, and Integration of Web Services (UDDI)	Standard approuvé du OASIS faisant partie intégrante des couches Web services et définissant une méthode standard de publication et de découverte de composants logiciels d'architectures orientées service (SOA) (http ://www.uddi.org)
Urbanisation	Mise en œuvre d'un plan d'urbanisme
Urbanisme	Méthodologie de construction d'un plan d'urbanisme
Usage abusif (d'un réseau informatique)	Usages du réseau contraire aux lois, règlement intérieur ou chartes d'usage des moyens informatiques, ou compromettant les services du réseau de l'établissement (consommation excessive de bande passante, introduction de faille dans la sécurité du réseau, etc).

THEME/CONCEPT	DEFINITION
Validation de conformité (de pages Web)	Résultat d'une opération de vérification de la conformité de pages Web développées en langage HTML ou en langage XHTML aux recommandations du W3C. Cette validation peut s'effectuer au moyen d'outils ad hoc mis à disposition librement par le W3C pour vérifier la conformité de pages Web (ou de feuilles de style CSS, ou encore, de fils d'information RSS ou Atom).
W3C	Web World Wide Consortium
WAI	Web Access Initiative
WCAG	Web Content Accessibility Guidelines
WCAG	Web Content Accessibility Guidelines
Web Access Initiative (WAI)	Groupe du W3C travaillant avec les organisations afin de déployer des stratégies, recommandations et ressources pour aider le Web à devenir plus accessible aux gens souffrant de handicap (http ://www.w3.org/wai)
Web Content Accessibility Guidelines (WCAG)	Ensemble de recommandations du W3C visant l'accessibilité non discriminante notamment pour les handicapés des contenus Web (http ://www.w3.org/TR/WCAG20/)
World Wide Web Consortium (W3C)	Organisme de standardisation du Web
What you see is what you get (WYSIWYG)	Expression qualifiant la capacité d'un système à publier/éditer des contenus sous une forme conforme à celle affichée à l'écran
Web Services Description Language (WSDL)	Standard du W3C (http ://www.w3.org/TR/wsdl)
WSDL	Web Services Description Language
WSOA	Web Service Oriented Architecture – Architecture de service mettant en œuvre la technologie des Services Web
WS-Security	Web Services – Security
WYSIWYG	« What you see is what you get » - Caractère d'une interface graphique présentant à l'écran d'édition les contenus sous leur forme de publication.
XMI	XML Metadata Interchange
XML	eXtensible Markup Language
XML Metadata Interchange (XMI)	Format d'échanges de métadonnées XML intégrant 3 formats standard : • XML, eXtensible Markup Language, un standard W3C ; • UML, Unified Modeling Language, un standard OMG; • MOF, Meta Object Facility, un standard OMG. XMI est applicable sur de nombreux types d'objets : les objets d'analyse et de conception (UML), logiciels (Java, C++), composants

THEME/CONCEPT	DEFINITION
	logiciels (EJB, IDL, CORBA) et de bases de données (CWM) et permet aux développeurs de partager des modèles objets dans des environnements distribués via internet. La version actuelle est XMI V2.1. Elle supporte la notion de schéma XML.
XML-RPC	XML Remote Procedure Call, un standard d'appel de procedures à distance (http ://www.xmlrpc.com/spec)
XSL	« eXtended Stylesheet Language » - Langage gérant la représentation d'un contenu XML

APPENDICE I

Intégration – Interopérabilité technique, organisationnelle et sémantique

N°	Réf. EIF	Règle d'interopérabilité générale

Règles d'interopérabilité d'ordre général

Dimension paneuropéenne

10. 1 Il est RECOMMANDÉ aux administrations des Etats membres et aux Institutions et Agences de l'Union Européenne de tenir compte des recommandations du Cadre d'Interopérabilité Européen (CIE) pour introduire une dimension paneuropéenne dans leur propre cadre d'interopérabilité et infrastructures administratives, afin de rendre les services électroniques administratifs interopérables au niveau européen. Les cadres d'interopérabilité nationaux doivent mentionner leur adhérence au CIE.

20. 2 Il est RECOMMANDÉ de considérer les principes suivants, d'ordre général, pour tout service électronique à concevoir au niveau européen :

- Accessibilité ;
- Multilinguisme ;
- Sécurité ;
- Protection des données personnelles ;
- Subsidiarité ;
- Utilisation de standards ouverts ;
- Promotion de logiciels Open Source ;
- Utilisation de solutions multilatérales.

30. 3 Il est RECOMMANDÉ pour tout service électronique à concevoir au niveau européen de considérer la problématique d'interopérabilité sous les angles organisationnel, sémantique et technique.

N°	Réf. RGI	Règle d'interopérabilité technique

Interopérabilité des formats de données

Codage des caractères

40. RIT0001 Il est **OBLIGATOIRE** d'utiliser la norme ISO 8859-15 (Alphabet Latin n°9), pour l'encodage sur un octet des caractères.

50. RIT0002 Il est **OBLIGATOIRE** d'utiliser la norme ISO 10646 et la recommandation UNICODE version 5.0.0, pour l'encodage multi-octets des caractères.

60. RIT0200 Il est RECOMMANDÉ d'utiliser le jeu universel de caractères UCS-4 pour l'encodage multi-octets en taille fixe des caractères UNICODE à partir de U+100, c'est-à-dire à partir de l'alphabet Latin étendu A.

70. RIT0201 Il est RECOMMANDÉ d'utiliser la transformation UTF-8 pour l'encodage multi-octets en taille variable des caractères UNICODE à partir de U+100, c'est-à-dire à partir de l'alphabet Latin étendu A.

Formats des images fixes non photographiques

80. RIT0003 Il est RECOMMANDÉ d'utiliser le format PNG v1.2 (norme ISO 15948) pour l'échange, la présentation et la conservation d'images fixes non photographiques (par exemple : dessin, icône, logo, schéma).

90. RIT0005 Il est DÉCONSEILLÉ d'utiliser le format GIF pour les images fixes non photographiques (par exemple : dessin, icône, logo, schéma).

Formats des images fixes photographiques de qualité ordinaire

100. RIT0006 Il est RECOMMANDÉ d'utiliser le procédé de compression et de codage JPEG (norme ISO 10918) et le format de fichier JFIF (JPEG File Interchange Format), pour l'échange, la présentation et la conservation d'images fixes photographiques de qualité ordinaire.

Formats des images fixes photographiques de haute qualité

110. RIT0008 Il est RECOMMANDÉ d'utiliser le format ouvert DNG ou le format TIFF/EP (norme ISO 12234), pour l'échange, la présentation et la conservation d'images fixes photographiques de haute qualité.

Formats d'images fixes déconseillés

120. RIT0009 Il est DÉCONSEILLÉ d'utiliser les formats d'images fixes propriétaires et d'une manière plus générale tous les formats d'images fixes à l'exception des formats PNG, JPEG, DNG, TIFF/EP.

Formats pour l'animation simple d'images

130. RIT0010 Il est RECOMMANDÉ d'utiliser le format « GIF animé » pour l'échange et la présentation d'animations graphiques simples et/ou de courte durée.

Formats pour l'animation complexe d'images

140. RIT0011 Il est RECOMMANDÉ d'utiliser le format ouvert Flash v8 pour l'échange et la présentation d'animations graphiques complexes et/ou de longue durée, en respectant toutefois les règles d'accessibilité.

Formats pour les séquences sonores

150. RIT0012 Il est RECOMMANDÉ d'utiliser le format MP3 (MPEG-1/2 Audio Layer 3 norme ISO 11172-3) pour l'échange, la diffusion et la conservation des séquences sonores de qualité ordinaire.

N°	Réf. RGI	Règle d'interopérabilité technique
160.	RIT0013	Il est DÉCONSEILLÉ d'utiliser les formats sonores propriétaires et d'une manière plus générale tous les formats sonores à l'exception des formats FLAC, MP3, Ogg-Speex, Ogg-Vorbis et WAV.
170.	RIT0203	Il est RECOMMANDÉ d'utiliser le format WAV, pour l'échange, la diffusion et la conservation des séquences sonores de haute qualité.
		Formats pour la vidéo basse définition
180.	RIT0015	Il est RECOMMANDÉ d'utiliser la norme ISO 13818 (MPEG-2) pour l'échange, la présentation et la conservation de séquences vidéo en basse définition.
		Formats des objets graphiques à deux dimensions
190.	RIT0017	Il est RECOMMANDÉ d'utiliser le format CGM (norme ISO 8632) pour l'échange et la conservation de données graphiques à deux dimensions.
200.	RIT0204	Il est RECOMMANDÉ d'utiliser le format SVG 1.1 pour la description d'objets graphiques vectoriels en deux dimensions.
		Formats pour l'audiovisuel et la vidéo haute définition (HD)
210.	RIT0082	Il est RECOMMANDÉ d'utiliser la norme ISO 14496 (MPEG-4) pour l'échange, la présentation et la conservation de séquences vidéo en haute définition.
220.	RIT0084	Il est RECOMMANDÉ d'utiliser la norme ISO 14496 (MPEG-4) pour la mise en œuvre de services audiovisuels (vidéo-conférence, visiophonie, etc).
		Formats pour les objets et univers virtuels en 3D
230.	RIT0205	Il est RECOMMANDÉ d'utiliser le format X3D (norme ISO 19775) pour la description d'objets et d'univers virtuels en 3 Dimensions.
		Interopérabilité des formats de document
		Echange de documents non structurés
240.	RIT0023	Il est **INTERDIT** d'utiliser le langage HTML pour les échanges de documents non structurés.
		Echange de documents bureautiques en mode « collaboratif »
250.	RIT0024	Il est RECOMMANDÉ d'utiliser des formats de document reposant sur l'utilisation du langage XML, et dont les spécifications sont publiques et libres de droit, pour les échanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation, etc).
260.	RIT0025	Il est RECOMMANDÉ d'utiliser le format « Open Document Format » (norme ISO 26300) pour les échanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation, etc).
270.	RIT0026	Il est **OBLIGATOIRE** d'accepter tout document au format « Open Document Format » (norme ISO 26300) pour les échanges de documents bureautiques semi-structurés (traitement de texte, tableur, présentation, etc).
280.	RIT0027	Il est **INTERDIT** de faire une migration depuis le format bureautique couramment utilisé par une organisation, vers un format autre que le format « Open Document Format » (norme ISO 26300).
		Echange de documents bureautiques en mode « informatif »
290.	RIT0207	Il est RECOMMANDÉ d'utiliser le format PDF/A-1 (norme ISO 19005) ou le format PDF, pour les échanges de documents bureautiques en mode informatif.

N°	Réf. RGI	Règle d'interopérabilité technique
		Conservation des documents bureautiques « statiques »
300	RIT0029	Il est RECOMMANDÉ d'utiliser le format PDF/A-1 (norme ISO 19005) pour la conservation des documents bureautiques statiques.
		Echange de données numériques d'impression
310.	RIT0021	Il est **OBLIGATOIRE** d'utiliser le format PDF/X (norme ISO 15930) pour l'échange de données numériques d'impression.
		Formats pour le dessin technique
320.	RIT0019	Il est RECOMMANDÉ d'utiliser le format OpenDWG version 2.0, ou à défaut le format DWG, pour les échanges de dessins techniques (par exemple des plans) en mode collaboratif (dessins devant être exploités, voire même être modifiés).
330.	RIT0020	Il est DÉCONSEILLÉ d'utiliser le format DXF pour l'échange et la présentation de dessins techniques (par exemple des plans).
340.	RIT0210	Il est **OBLIGATOIRE** d'utiliser le format PDF, ou à défaut le format DWF, pour les échanges de dessins techniques (par exemple des plans) en mode informatif.
		Formats pour la CAO et la production industrielle
350.	RIT0211	Il est RECOMMANDÉ d'utiliser les spécifications IFC (norme ISO 16739) pour les échanges d'informations dans le domaine de la construction et de la gestion immobilière.
		Format et échange des documents structurés
360.	RIT0030	Il est **OBLIGATOIRE** d'utiliser le langage XML pour échanger des documents structurés.
370.	RIT0031	Il est **OBLIGATOIRE** d'accepter le langage XML versions 1.0 et 1.1, lors de la réception de documents structurés.
380.	RIT0032	Il est RECOMMANDÉ d'utiliser le langage XML version 1.1 pour l'envoi de documents structurés.
390.	RIT0036	Il est DÉCONSEILLÉ d'utiliser le langage SGML (norme ISO 8879) pour la description des documents structurés.
		Définition de schéma de documents structurés
400.	RIT0033	Il est RECOMMANDÉ d'utiliser le langage DSDL Relax NG (norme ISO 19757) pour la définition de schéma de documents structurés.
410.	RIT0037	Il est RECOMMANDÉ, en l'absence de possibilité de mise en œuvre d'un langage de définition de schéma de documents XML, d'utiliser une DTD (Définition de type de Document) pour la définition de schéma de documents structurés.
		Exportation des bases de données
420.	RIT0034	Il est RECOMMANDÉ d'utiliser le format XML pour réaliser des exportations de bases de données.
		Langages XSLT et Xpath
		Recommandations sur les IHM
		Ergonomie des IHM
430.	RIT0074	Il est RECOMMANDÉ […] de se conformer à la « Charte Graphique et Ergonomique des Téléprocédures publiques » […] éditée par le ministère en charge de la réforme de l'Etat.

N°	Réf. RGI	Règle d'interopérabilité technique
		Technologies pour construire les IHM Web
440.	RIT0022	Il est RECOMMANDÉ de prévoir une évolution de l'utilisation du langage HTML vers le langage XHTML, pour adapter les anciennes interfaces d'applications Web des services en ligne de l'administration.
450.	RIT0041	Il est DÉCONSEILLÉ d'utiliser le langage HTML 4.01 pour construire les nouvelles interfaces d'applications Web des services en ligne de l'administration.
460.	RIT0042	Il est RECOMMANDÉ d'utiliser les feuilles de style CSS niveau 2 pour ajuster la présentation de documents structurés.
470.	RIT0043	Il est DÉCONSEILLÉ d'utiliser des langages de script, lorsque leur utilisation n'est pas strictement nécessaire pour créer des IHM Web.
480.	RIT0044	Il est DÉCONSEILLÉ d'utiliser des composants logiciels de type ActiveX pour créer des IHM Web.
490.	RIT0213	Il est **OBLIGATOIRE** d'utiliser la grammaire de langage « XHTML-1.0-Transitional » pour construire les interfaces d'applications Web des services en ligne de l'administration.
500.	RIT0214	Il est RECOMMANDÉ d'utiliser la grammaire de langage « XHTML-1.0-Strict » pour construire les interfaces d'applications Web des services en ligne de l'administration.
510.	RIT0215	Il est **INTERDIT** d'utiliser la grammaire de langage « XHTML-1.0-Frameset » pour construire les interfaces d'applications Web des services en ligne de l'administration.
520.	RIT0216	Il est **OBLIGATOIRE**, lorsque l'utilisation d'un langage de script est strictement nécessaire pour créer des IHM Web, d'en informer clairement l'usager, dès la page d'accueil du téléservice.
530.	RIT0217	Il est **OBLIGATOIRE** d'utiliser des langages de script conformes à la norme ISO 16262 (langage ECMAScript), lorsque leur utilisation est strictement nécessaire pour créer des IHM Web.
540.	RIT0218	Il est **OBLIGATOIRE**, lorsque l'utilisation d'un langage de script est strictement nécessaire pour créer des IHM Web, de prévoir un accès en mode dégradé, utilisable par tout navigateur mentionné dans le RGI.
550.	RIT0219	Il est RECOMMANDÉ d'utiliser des composants logiciels de type « applettes Java », pour créer des IHM Web, lorsque cela est strictement nécessaire.
560.	RIT0220	Il est DÉCONSEILLÉ d'utiliser des composants logiciels de type Flash hors animation, VML, ou équivalents pour créer des IHM Web.
		Indépendance par rapport aux appareils et à leurs IHM
570.	RIT0045	Il est **OBLIGATOIRE** que les applications destinées aux usagers soient compatibles avec les versions de navigateurs mentionnés dans le RGI.
580.	RIT0092	Il est RECOMMANDÉ que les applications destinées aux agents soient compatibles avec les versions de navigateurs mentionnés dans le RGI.
		Intégration de services Web par les IHM
590.	RIT0046	Il est RECOMMANDÉ de s'appuyer sur l'interface de programmation « Java Specification Request : Portlet Specification JSR 168 » pour intégrer des composants locaux dans un portail Web.

N°	Réf. RGI	Règle d'interopérabilité technique
600.	RIT0047	Il est RECOMMANDÉ d'utiliser le service WSRP pour intégrer des composants distants dans un portail Web.
610.	RIT0048	Il est DÉCONSEILLÉ d'utiliser des balises HTML « IFRAME » pour intégrer des services Web distants.

Syndication de contenu

620.	RIT0049	Il est RECOMMANDÉ d'utiliser le format RSS 2.0 pour réaliser de la syndication de contenu Web de type « fil d'information ».
630.	RIT0050	Il est DÉCONSEILLÉ d'utiliser le format ATOM Syndication pour réaliser de la syndication de contenu Web.
640.	RIT0221	Il est RECOMMANDÉ, pour préciser le type MIME des fils d'informations qui est attendu par les navigateurs, de positionner le paramètre HTTP Content-Type header à la valeur « text/xml » ou à la valeur « application/rss+xml ».

Validation de la conformité des pages Web

650.	RIT0222	Il est RECOMMANDÉ de procéder à une validation de conformité des pages Web des services en ligne de l'administration.

Interopérabilité des messageries électroniques

Protocole de messagerie électronique

660.	RIT0051	Il est **OBLIGATOIRE** d'utiliser le protocole SMTP (Simple Mail Transfer Protocol) pour l'échange de courriels.

Représentation des messages et pièces jointes

670.	RIT0052	Il est **OBLIGATOIRE** d'utiliser le format d'échange MIME (« Multipurpose Internet Mail Extensions ») pour la représentation des courriels et des pièces jointes.

Sécurisation de la messagerie électronique

680.	RIT0053	Il est **OBLIGATOIRE** d'utiliser l'extension S/MIME pour sécuriser les envois de courriels.
690.	RIT0223	Il est RECOMMANDÉ de proposer l'extension ESMTP STARTTLS sur les serveurs de messagerie, mais sans exiger que les clients l'utilisent (en particulier entre serveurs ou sur Internet)

Accès aux B.A.L. de la messagerie électronique

700.	RIT0054	Il est **OBLIGATOIRE** de pouvoir mettre en œuvre le protocole POP3 (Post Office Protocol) ou le protocole IMAP4 (Internet Message Access Protocol) pour relever les courriels déposés dans une boîte aux lettres.

Extensions à la messagerie électronique

710.	RIT0085	Il est RECOMMANDÉ d'utiliser l'extension ESMTP pour implémenter les fonctionnalités supplémentaires au protocole SMTP.

Mise en œuvre de la messagerie électronique

720.	RIT0056	Il est **OBLIGATOIRE** pour les administrations de se conformer aux règles de dénomination des adresses électroniques définies dans la « Charte de Nommage Internet », version 1.2, établie par les services du Premier ministre en 2001.

N°	Réf. RGI	Règle d'interopérabilité technique

Services de messagerie instantanée

730. RIT0224 Il est RECOMMANDÉ d'utiliser le protocole XMPP (eXtensible Messaging and Presence Protocol) pour mettre en oeuvre des services de messagerie instantanée entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Interopérabilité des services d'annuaire

Service d'annuaire

750. RIT0057 Il est **OBLIGATOIRE** de prévoir un mode d'accès conforme à LDAP v3 pour les annuaires interrogeables par plusieurs entités administratives.

Echanges de données entre annuaires

760. RIT0058 Il est RECOMMANDÉ d'utiliser le format LDIF pour échanger tout ou partie d'un annuaire de données LDAP.

Sécurisation du service d'annuaire

770. RIT0086 Il est RECOMMANDÉ d'utiliser les *extensions de sécurisation LDAP* pour sécuriser les services d'un annuaire de données LDAP.

SUPANN

780. Il est RECOMMANDÉ à l'ensemble des établissements d'enseignement supérieur français de suivre les recommandations SUPANN afin de :

- permettre à tout personnel de la communauté de l'enseignement supérieur, où qu'il soit, de consulter les coordonnées professionnelles (téléphone, adresse de courrier électronique et adresse postale) de ses pairs. La consultation se fera à partir d'un navigateur Web via une application de type « pages blanches » au sens annuaire téléphonique ;
- permettre à tous les personnels autorisés, d'accéder aux coordonnées de membres de groupes transverses aux établissements et en particulier de diffuser des courriers électroniques à tous les membres d'un groupe donné. ;
- fournir les éléments devant être respectés par les annuaires d'établissements afin d'autoriser les procédures d'authentification inter-établissements ou avec des organismes externes ;
- fournir les éléments devant être respectés, en matière d'annuaire, par les applications destinées à l'enseignement supérieur.

Ces recommandations permettent d'assurer la compatibilité des annuaires aux niveaux

- international (travaux d'Internet 2, EduPerson) ;
- inter ministériel (respect des recommandations de l'ADAE dans ce domaine) ;
- interne au ministère de la jeunesse, de l'éducation nationale et de la recherche en garantissant notamment l'interopérabilité des annuaires entre l'enseignement scolaire et le supérieur ;
- inter établissements d'enseignement supérieur ;
- des applicatifs de la communauté de l'enseignement supérieur.

N°	Réf. RGI	Règle d'interopérabilité technique

Interopérabilité des services techniques

Services de compression de fichiers

790. RIT0096 Il est RECOMMANDÉ d'utiliser le format ouvert « 7z », ou à défaut le format « zip », pour compresser un fichier dans un but de conservation.

Services de noms de domaines

800. RIT0063 Il est **OBLIGATOIRE** d'utiliser le service DNS pour accéder aux fonctionnalités de résolution de noms de domaines.

Services sécurisés de noms de domaines

810. RIT0064 Il est RECOMMANDÉ d'utiliser le service DNSSEC pour sécuriser les services administratifs de gestion des serveurs DNS (mises à jour des configurations ou des fichiers de zones, etc).

Services de transfert de fichiers : modèle IETF

820. RIT0065 Il est RECOMMANDÉ, hors contexte Web, d'utiliser le protocole SFTP ou à défaut le protocole FTP pour réaliser des transferts de fichiers.

830. RIT0066 Il est **INTERDIT** d'utiliser le protocole TFTP pour réaliser des transferts de fichiers applicatifs.

840. RIT0093 Il est **INTERDIT**, dans le contexte Web, d'utiliser le protocole FTP pour réaliser des transferts de fichiers, car le protocole HTTP remplit cette fonction.

Services de gestion des Forums

850. RIT0225 Il est RECOMMANDÉ, quand on ne fait pas du forum Web, d'utiliser le protocole NNTP pour mettre en œuvre des services de forum de discussion sur le réseau.

Interopérabilité et Sécurisation des échanges

Protocoles d'échanges de messages

860. RIT0067 Il est RECOMMANDÉ d'utiliser le protocole PRESTO pour les échanges de messages au sein de l'administration.

Services de sécurisation des échanges

870. RIT0068 Il est **OBLIGATOIRE** d'utiliser les protocoles TLS 1.1 ou SSL 3.0 pour sécuriser les échanges s'appuyant sur des protocoles applicatifs tels que FTP, HTTP, IMAP, LDAP, POP3, SIP, SMTP, etc.

Services de chiffrement des documents XML

880. RIT0069 Il est RECOMMANDÉ d'utiliser le protocole XML Encryption pour chiffrer des documents XML.

Services de signature des documents XML

890. RIT0070 Il est **OBLIGATOIRE** d'utiliser la fonction de signature XadES pour signer des documents XML et de se conformer au profil de signature pour l'administration électronique.

Services de sécurisation des «Web Services»

900. RIT0071 Il est RECOMMANDÉ d'utiliser la fonction WS-Security pour sécuriser des Web Services.

N°	Réf. RGI	Règle d'interopérabilité technique

Protocole de déclaration de données utilisateur

910. RIT0090 Il est RECOMMANDÉ d'utiliser le langage SAML version 2.0 (recommandation UIT-T X.1141) pour les déclarations de données d'authentification et d'autorisation.

Invocation de services

920. RIT0059 Il est RECOMMANDÉ de s'appuyer sur le protocole SOAP 1.1 lors de la conception de Web Services.

930. RIT0060 Il est **OBLIGATOIRE** de décrire les interfaces des Web Services exposés, à l'aide de documents conformes au langage WSDL (recommandation du W3C).

940. RIT0062 Il est RECOMMANDÉ de se conformer au profil d'utilisation des Web Services « Basic Profile 1.0 ».

950. RIT0091 Il est **OBLIGATOIRE** de dissocier la couche Web Services de la couche de transport (HTTP, SMTP, …).

Formats des certificats électroniques

960. RIT0234 Il est **OBLIGATOIRE** que le format des certificats de personne et de serveur soit conforme au document « Profils de certificats/LCR/OCSP et Algorithmes Cryptographiques » de la « PRIS » Politique de Référencement Intersectorielle de Sécurité V2.1.

Formats des contremarques de temps

970. RIT0235 Il est **OBLIGATOIRE** que les contremarques de temps soient conformes au format défini dans la Politique d'Horodatage Type V2.1. Ce document appartient à l'ensemble documentaire appelé « PRIS » Politique de Référencement Intersectorielle de Sécurité.

Utilisation de mécanismes de cryptographie

980. RIT0236 Il est **OBLIGATOIRE** de respecter les règles et recommandations concernant le choix et le dimensionnement des mécanismes de cryptographie de niveau de robustesse standard, DCSSI, version 1.02 du 19 novembre 2004.

Interopérabilité des protocoles

Protocole HTTP (couche application)

990. RIT0078 Il est RECOMMANDÉ d'utiliser le protocole HTTP 1.1 (HyperText Transfer Protocol) pour la présentation et les échanges entre un serveur Web et un navigateur.

1000. RIT0079 Il est **OBLIGATOIRE** d'utiliser la méthode HTTP POST, au lieu de la méthode HTTP GET, lors du passage de paramètres à caractère confidentiel ou personnel.

1010. RIT0226 Il est **OBLIGATOIRE** d'utiliser la méthode HTTP POST pour faire une requête qui provoque un changement d'état persistant dans l'application Web, par exemple un changement de mot de passe, une création de compte.

Protocoles TCP et UDP (couche transport session)

1030. RIT0077 Il est OBLIGATOIRE d'utiliser les protocoles TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) pour transporter les flux de données provenant des couches applicatives.

Protocole IP (couche réseau)

1040. RIT0075 Il est **OBLIGATOIRE** d'utiliser le protocole Ipv4 pour l'ensemble des échanges au niveau de la couche réseau.

N°	Réf. RGI	Règle d'interopérabilité technique
1050.	RIT0229	Il est RECOMMANDÉ de mettre en oeuvre, sur les équipements de coeur de réseau (serveurs, routeurs, commutateurs), un système d'exploitation capable de gérer le protocole Ipv6.
		Protocole Ipsec (couche réseau)
1060.	RIT0076	Il est RECOMMANDÉ d'utiliser le protocole Ipsec au niveau de la couche réseau, pour crypter les échanges, pour authentifier les échanges, pour valider l'intégrité des échanges.
		Protocoles d'horodatage technique et de synchronisation
1070.	RIT0080	Il est RECOMMANDÉ d'utiliser le protocole NTP pour réaliser une synchronisation des horloges des différents ordinateurs et équipements réseaux constituant un Système d'Information.
1080.	RIT0081	Il est RECOMMANDÉ d'utiliser les signaux horaires TDF (162 kHz) ou DCF77 (77,5 kHz) pour d'obtenir une fonction d'horodatage technique précise.
1090.	RIT0230	Il est RECOMMANDÉ que les serveurs de temps, mis à disposition des Systèmes d'Information, transmettent une heure au format UTC (Temps Universel Coordonné).
		Protocoles pour la Téléphonie
1100.	RIT0231	Il est RECOMMANDÉ d'utiliser le protocole RTP et son protocole de contrôle de flux RTCP pour le transport de la voix sur protocole IP.
1110.	RIT0232	Il est RECOMMANDÉ d'utiliser un ou plusieurs codecs parmi ceux spécifiés dans les recommandations UIT-T G.711A, G.722, G723.1, G.729, G.729A, ETSI GSM 06.10, IETF iLBC, Speex, pour le codage de la voix.
1120.	RIT0233	Il est RECOMMANDÉ d'utiliser le format MP3 (MPEG-1/2 Audio Layer 3 norme ISO 11172-3) pour enregistrer les messages vocaux mis en pièce jointe dans les messageries unifiées.
		Supports matériels
		Supports d'archivage
1130.	RIT0087	Il est RECOMMANDÉ de choisir pour l'archivage électronique des supports de type WORM physique ou logique (Write Once, Read Many), non effaçables, non réinscriptibles et non modifiables.
		Cartes à puce et clés USB
1140.	RIT0088	Il est **OBLIGATOIRE** que les cartes des usagers, émises par les autorités administratives et qui sont porteuses de bi-clés et de certificats, respectent les spécifications du socle commun cartes IAS version 1.0.1 Premium.
1150.	RIT0089	Il est **OBLIGATOIRE** que les cartes des agents, émises par les autorités administratives et qui sont porteuses de bi-clés et de certificats, respectent les spécifications du socle commun cartes IAS version 1.0.1 Premium.
1160.	RIT0094	Il est **OBLIGATOIRE** que les cartes, émises par des autorités administratives et basées sur le socle commun cartes IAS version 1.0.1 Premium, soient référencées.

N°	Réf. RGI	Règle d'interopérabilité organisationnelle

Interopérabilité organisationnelle

1200.	RIO 0100	Il est RECOMMANDE dans les structures administratives que le référentiel d'identités des Agents s'appuie sur une politique d'annuaires dotés de liaisons de gestion avec le(s) SIRH interne(s).
1210.	RIO 0116	Il est RECOMMANDE de propager un droit d'accès aux ressources d'un Fournisseur de services en se basant sur le rôle de l'usager Agent ou Professionnel plutôt que sur son identifiant.
1220.	RIO 0119	Il est RECOMMANDE que l'usager Professionnel présente un secret « technique » afin de prouver qu'il est mandaté par le bénéficiaire pour l'usage de téléservices pour son compte.
1230.	RIO 0120	Il est **INTERDIT** que le secret « technique » dépende de données gérées par un téléservice.
1240.	RIO 0121	Il est RECOMMANDE que le secret « technique » présenté par l'usager Professionnel véhicule la volonté (ou non) du Représentant Légal de l'entreprise bénéficiaire de choisir une organisation des chaînes de délégation de droits d'accès avec séparation des pouvoirs.
1250.	RIO 0122	Il est RECOMMANDE que le secret « technique » ait une validité limitée dans le temps.
1260.	RIO 0123	Il est **OBLIGATOIRE** d'envoyer le secret « technique » au Représentant Légal de l'entreprise bénéficiaire des téléservices.
1270.	RIO 0125	Il est **OBLIGATOIRE** d'attribuer le rôle « Administrateur Administration Electronique » aux usagers Professionnels présentant un secret « technique » valide.
1280.	RIO 0129	Il est **OBLIGATOIRE** d'attribuer le rôle « Administrateur Administration Electronique » aux usagers présentant un secret « métier » valide.
1290.	RIO 0131	Il est RECOMMANDE de conserver une trace des événements associés au processus de délégation de droits d'accès.
1300.	RIO 0139	Il est RECOMMANDE de conserver une trace des événements associés aux demandes d'accès des Usagers (tous types) aux ressources mises à disposition par le Fournisseur de services.
1310.	RIO 0142	Il est **OBLIGATOIRE** que des demandes d'accès aux ressources (vecteur d'identification) fassent référence à la convention versionnée Consommateur de services / Fournisseur lorsqu'il y a propagation inter-espaces (cas de la fédération).
1320.	RIO 0144	Il est RECOMMANDE que les demandes d'accès aux ressources mises à disposition par convention par le Fournisseur de services véhiculent une identification du Consommateur de services, du Bénéficiaire, de la ressource invoquée ainsi que les modalités d'accès sur cette ressource (rôle, niveau d'authentification, restrictions ….).
1330.	RIO 0150	Il est RECOMMANDE pour assurer la confidentialité que le service d'archivage mette en place un service sécurisé par un contrôle d'accès et, si nécessaire, un chiffrement des données.
1340.	RIO 0151	Il est **OBLIGATOIRE** d'enregistrer et d'archiver une trace des opérations et des événements concernant les archives et les documents archivés.

N°	Réf. RGI	Règle d'interopérabilité organisationnelle
1350.	RIO 0152	Il est **OBLIGATOIRE** de créer et de gérer des métadonnées associées à l'archive numérique, dès la création de cette dernière et tout au long de son cycle de vie, en vue d'en assurer la conservation pendant la durée requise. Les métadonnées minimales sont celles qui sont obligatoires dans le « standard d'échange de données pour l'archivage ».
1360.	RIO 0154	Il est **OBLIGATOIRE** d'utiliser un système de fédération d'identités pour la mise en place de systèmes d'authentification unique des usagers dans des téléservices dépendant de différentes administrations.
1370.	RIO 0155	Il est RECOMMANDE d'utiliser un modèle de fédération reposant sur une passerelle inter fournisseurs d'identité pour construire une authentification unique des usagers sur des services appartenant à des cercles de confiance différents.
1380.	RIO 0156	Il est RECOMMANDE pour fédérer des services sur un cercle de confiance inter administrations d'utiliser le modèle de fédération d'identité ID-FF 1.2 ou à défaut un modèle de fédération supporté par SAML 2.0
1390.	RIO 0157	Il est RECOMMANDE d'échanger des attributs entre des services fédérés sur un cercle de confiance inter administrations en utilisant le modèle ID-WSF 1.1.
1400.	RIO 0159	Il est **OBLIGATOIRE** que les échanges et collectes par télé-services, de données à caractère personnel respectent les principes édictés aux articles 6 et 7 de la Loi n°78-17 modifiée.
1410.	RIO 0161	Il est **OBLIGATOIRE** que les logiciels mis en œuvre par les autorités administratives soient développés ou paramétrés de manière à ne pas permettre l'enregistrement de données à caractère personnel qui ne seraient pas référencées dans le dossier de formalités examiné par la CNIL.
1420.	RIO 0162	Il est **OBLIGATOIRE**, pour les télé-services mis en œuvre par les autorités administratives, d'assurer une information claire et précise conforme à l'obligation légale prévue au chapitre 5 de la loi n°78-17 modifiée.
1430.	RIO 0190	Il est **OBLIGATOIRE** que les contremarques de temps utilisées par les services de notification et traçabilité des services d'identités et contrôle d'accès (ICA) soient conformes aux règles du Référentiel Général de Sécurité.
1440.	RIO 0191	Il est **OBLIGATOIRE** que les certificats de confidentialité et de signature utilisés pour chiffrer ou signer soient conformes aux règles édictées par le Référentiel Général de Sécurité.

N°	Réf. RGI	Règle d'interopérabilité sémantique

Interopérabilité sémantique

1500. RIS 0158 Il est **OBLIGATOIRE** que les services publics d'archives et leurs partenaires qui veulent mettre en place des échanges informatisés se réfèrent au « standard d'échanges de données pour l'archivage » élaboré par la Direction des Archives de France du Ministère de la culture et de la communication et le SDAE de la DGME du Ministère des finances.

1510. RIS 0170 Il est RECOMMANDÉ d'utiliser le langage UML v2.0 pour représenter et modéliser des données et des processus, des interactions entre systèmes ou composants, et d'organiser les données, les composants ou les systèmes dans différents types de hiérarchie (taxinomie, composition, package, composant, etc.).

1520. RIS 0171 Il est RECOMMANDÉ d'utiliser le format XMI (ISO/IEC 19503) pour l'échange de métadonnées entre les outils de modélisation (basés sur UML) et les autres outils et référentiels de données dans des environnements distribués hétérogènes.

1530. RIS 0172 Il est **OBLIGATOIRE** pour tout nouveau flux ou systèmes d'échanges, que chaque autorité administrative identifie au sein de son système d'information les données échangées avec des tiers correspondant à des classes et attributs dotés d'un numéro UN/CEFACT dans le MDC (modèle données communes) des téléservices.

1540. RIS 0173 Il est RECOMMANDE pour les nouveaux flux ou systèmes d'échanges, à défaut de composants référencés UN/CEFACT, de prendre en compte pour les données échangées les composants du MDC (modèle données communes) des téléservices car ils résultent d'un consensus européen ou national.

1550. RIS 0174 Il est RECOMMANDÉ, lors de la conception de systèmes d'échanges, de s'assurer de la compatibilité des travaux avec la norme ISO/TS 15000-5 : 2005 concernant la spécification technique de ces composants. Les livrables « standard d'échanges de données » pourront respecter la forme inspirée par les méthodologies du CEFACT ou de ses dérivés « UML-XML ».

1560. RIS 0175 Il est **OBLIGATOIRE** pour les nouveaux systèmes d'échanges élaborés par ou entre les autorités administratives, de mettre à disposition publique l'ensemble documentaire permettant la compréhension du dispositif et de ses éléments mis au point par les partenaires (documentation textuelle, définitions, représentations formelles : modèles, diagrammes, schémas XML …).

1570. RIS 0177 Il est **OBLIGATOIRE** lors des échanges entre Systèmes d'Information de l'Administration, de fournir le SIREN comme identifiant unique ou identifiant complémentaire pour les entreprises ou entités administratives.

1580. RIS 0178 Il est O**BLIGATOIRE** lors des échanges entre Systèmes d'Information de l'Administration, de fournir le SIRET comme identifiant unique ou identifiant complémentaire pour les établissements des entreprises ou entités administratives.

1590. RIS 0179 Il est **OBLIGATOIRE** d'utiliser la norme ISO 8601 pour la description des dates et heures lors des échanges entre Systèmes d'Information de l'Administration.

1600. RIS 0180 Il est **OBLIGATOIRE** d'utiliser la nomenclature internationale définie par la norme ISO /CEI 5218 pour caractériser le genre sexuel des personnes. Cette nomenclature prévoit 2 positions pour coder les genres masculin (1) et féminin (2), et 2 autres positions utilitaires pour couvrir tous les cas notamment statistiques ou bases de données : 0 pour le cas « inconnu ou non spécifié », 9 pour le cas « sans objet ».

N°	Réf. RGI	Règle d'interopérabilité sémantique
1610.	RIS 0181	Il est **OBLIGATOIRE** d'utiliser la codification internationale des langues définie par la norme ISO 639-1 dans les interfaces usagers des téléservices et lors des échanges de données entre Systèmes d'Information de l'Administration.
1620.	RIS 0182	Il est **OBLIGATOIRE** lors des échanges de données avec ou entre Systèmes d'Information de l'Administration, d'utiliser pour caractériser cette donnée la nomenclature des catégories juridiques CJ, établie pour l'immatriculation des entreprises dans les répertoires de référence (SIRENE, RCS..).
1630.	RIS 0183	Il est **OBLIGATOIRE** d'utiliser les nomenclatures françaises NAF et CPF pour caractériser lors des échanges entre Systèmes d'Information de l'Administration les activités des entités ainsi que les produits et services qui en résultent.
1640.	RIS 0184	Il est **OBLIGATOIRE** d'utiliser la nomenclature internationale des pays définie par la norme ISO 3166-1 dans les interfaces usagers des téléservices et lors des échanges de données entre Systèmes d'Information de l'Administration.
1650.	RIS 0185	Il est **OBLIGATOIRE** d'utiliser les nomenclatures du Code officiel géographique pour codifier en tant que divisions territoriales, les communes, les cantons, les arrondissements, les départements, les régions et collectivités territoriales d'outre-mer lors des échanges entre Systèmes d'Information de l'Administration, en précisant le niveau de codification choisi lorsqu'il en existe plusieurs.
1660.		Il est RECOMMANDÉ d'utiliser le dispositif CDM-FR pour l'affichage structuré et adaptable d'une offre de formation à l'échelon régional ou national

APPENDICE II

Téléservices et Sécurité des Systèmes d'Information (SSI)

N°	Réf. RGS	Règles de sécurité

Fonctions de sécurité : Authentification, Signature, Confidentialité, Horodatage

Authentification/Identification

1700. RS0014 Il est RECOMMANDE de se conformer au document « Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard » (référentiel DCSSI)

1710. RS0015 Il est **OBLIGATOIRE** que les certificats de personne d'authentification soient conformes à la Politique de Certification Type Service Authentification V2.1 de la PRIS

1720. RS0016 Il est **OBLIGATOIRE** que les certificats de personne d'authentification et de Signature soient conformes à la Politique de Certification Type Services Authentification et Signature V2.1 de la PRIS

1730. RS0017 Il est **OBLIGATOIRE,** pour pouvoir être acceptés par l'ensemble des téléservices requérant des certificats **« Agent », « Entreprise » ou « Particulier »** d'authentification d'un niveau de sécurité donné, que ces certificats soient référencés en tant que certificats **« Agent », « Entreprise » ou « Particulier »** d'authentification ou d'authentification et de signature, pour ce niveau de sécurité ou pour un niveau supérieur.

1740. RS0018 Il est **OBLIGATOIRE** que les téléservices requérant des certificats « Agent », « Entreprise » ou « Particulier » d'authentification d'un niveau de sécurité donné acceptent tous les certificats référencés en tant que certificats « Agent », « Entreprise » ou « Particulier » d'authentification ou d'authentification et de signature, pour ce niveau de sécurité ou pour un niveau supérieur.

1750. RS0019 Il est **OBLIGATOIRE** que les nouveaux téléservices ou toute évolution majeure de téléservice requérant des certificats de personne d'authentification sachent gérer la séparation des usages (authentification, signature) et des tailles de clés RSA ou DH de 2048 bits.

1760. RS0020 Il est **OBLIGATOIRE** que les téléservices annoncent le type de certificat : « Agent », « Entreprise » ou « Particulier », l'usage (authentification ou authentification et signature), et le niveau de sécurité qu'ils acceptent.

1770. RS0021 Il est **OBLIGATOIRE** que les autorités administratives installant une nouvelle IGC ou faisant appel à un PSCe pour émettre des certificats de personne à usage d'authentification mettent en place une Politique de Certification compatible avec la Politique de Certification Type Service Authentification V2.1.

1780. RS0022 Il est **OBLIGATOIRE** que les Distinguish Names (DN) des certificats « Agent », « Entreprise » ou « Particulier », délivrés par le même émetteur à une même personne, soient identiques pour les trois usages : authentification, signature et chiffrement.

1790. RS0023 Il est **OBLIGATOIRE** de conserver le même Distinguish Name (DN) lors du renouvellement d'un certificat de personne (sauf exception incontournable comme un changement d'état civil alors que le DN inclut le nom du détenteur, auquel cas il est nécessaire de renouveler tous les certificats comportant le même DN en vertu de la règle RS0022).

N°	Réf. RGS	Règles de sécurité
		Authentification : certificat serveur
1800.	RS0024	Il est **OBLIGATOIRE** que les certificats « Serveur» soient conformes à la Politique de Certification Type Certificats Serveur V2.1 de la PRIS
1810.	RS0025	Il est **OBLIGATOIRE,** pour pouvoir être acceptés par l'ensemble des téléservices ou des services requérant des certificats « Serveur» » d'un niveau de sécurité donné, que ces certificats soient référencés en tant que certificats serveur, pour ce niveau de sécurité ou pour un niveau supérieur.
1820.	RS0026	Il est **OBLIGATOIRE** que les téléservices ou les services requérant des certificats « Serveur » d'un niveau de sécurité donné acceptent tous les certificats référencés en tant que certificats serveur pour ce niveau de sécurité ou pour un niveau supérieur.
1830.	RS0027	Il est **OBLIGATOIRE** que les téléservices ou les services utilisent des certificats « Serveur » référencés dans le cadre des échanges avec les usagers (particulier ou entreprise).
1840.	RS0028	Il est **OBLIGATOIRE** que les Distinguish Names (DN) d'un même serveur soient identiques pour les deux usages : authentification et cachet.
1850.	RS0029	Il est **OBLIGATOIRE** de conserver le même Distinguish Name (DN) lors du renouvellement d'un certificat de serveur, sauf cas de force majeure.
		Authentification : système à mot de passe à usage unique
1860.	RS0030	Il est **OBLIGATOIRE** que les spécifications cryptographiques du dispositif de mot de passe à usage unique soient connues et conformes au référentiel « Mécanismes cryptographiques » pour le niveau « standard » publié par la DCSSI. Ces spécifications doivent couvrir le mécanisme permettant de générer le mot de passe aussi bien que les éventuels mécanismes de génération de clés cryptographiques, de génération d'aléas, etc.
1870.	RS0031	Il est **OBLIGATOIRE** que les processus de gestion des secrets du dispositif de mot de passe dynamique soient conformes au référentiel « Gestion des clefs » pour le niveau « standard » publié par la DCSSI.
1880.	RS0032	Il est **OBLIGATOIRE** que le modèle du processus d'authentification soit conforme au référentiel « Authentification » pour le niveau « standard » publié par la DCSSI.
1890.	RS0034	Il est **OBLIGATOIRE** que le mécanisme d'authentification par mot de passe à usage unique mette en œuvre un second dispositif matériel, distinct de celui que l'usager met en œuvre (typiquement l'ordinateur personnel) pour utiliser le téléservice. Lorsque le mot de passe est fourni « à la volée » à l'utilisateur, il l'est ainsi par un canal secondaire, via ce second dispositif matériel.
1900.	RS0035	Il est RECOMMANDE que les données définissant le canal secondaire de communication du mot de passe à usage unique ne soient pas modifiables dans une session établie en utilisant ce mot de passe à usage unique ( ) ( ) sans quoi une seule connexion illicite permettrait à l'usurpateur de modifier par exemple l'adresse postale ou le numéro de téléphone cellulaire destinataire des mots de passe afin de pouvoir reproduire ultérieurement l'usurpation d'identité
1910.	RS0036	Il est **OBLIGATOIRE** que la durée de vie du mot de passe à usage unique n'excède pas deux minutes à compter de son utilisation effective (cas d'une liste préétablie, diversification de clef,…) ou de sa génération en vue d'une authentification immédiate (code aléatoire transmis, …).

N°	Réf. RGS	Règles de sécurité
1920.	RS0037	Il est **INTERDIT** d'utiliser des mots de passe à usage unique générés par un générateur pseudo aléatoire produisant des séries prédictibles.
1930.	RS0038	Il est RECOMMANDE que le mot de passe à usage unique soit immédiatement invalidé après sa première utilisation
1940.	RS0039	Il est **OBLIGATOIRE** d'informer l'utilisateur, dès sa connexion, de la date et de l'heure de la dernière connexion réalisée sous son identité.
1950.	RS0040	Il est RECOMMANDE de ne pas accepter plusieurs sessions simultanées initiées sous la même identité.
1960.	RS0041	Il est **OBLIGATOIRE** de définir une procédure de signalement d'usurpation d'identité ou de perte de mots de passe à usage unique non utilisés, et de la porter à la connaissance des utilisateurs. Cette procédure entraine l'invalidation des éventuels mots de passe à usage unique préalablement communiqués à l'utilisateur et encore valides.
		Authentification : identifiant et mot de passe statique
1970.	RS0042	Il est RECOMMANDE que les téléservices identifiant leurs usagers par identifiant et mot de passe statique suivent les recommandations décrites dans le document : CERTA-2005-INF-001 (révision d'avril 2007) disponible sur le site du CERTA : www.certa.ssi.gouv.fr
		Signature électronique : certificat de personne
1980.	RS0043	Il est **OBLIGATOIRE** que les certificats de personne de signature soient conformes à la Politique de Certification Type Service Signature V2.1 de la PRIS
1990.	RS0044	Il est **OBLIGATOIRE** que les certificats de personne d'authentification et de Signature soient conformes à la Politique de Certification Type Services Authentification et Signature V2.1 de la PRIS
2000.	RS0045	Il est **OBLIGATOIRE,** pour pouvoir être acceptés par l'ensemble des téléservices requérant des certificats « Agent », « Entreprise », « Particulier » de signature d'un niveau de sécurité donné que ces certificats soient référencés en tant que certificats « Agent », « Entreprise », « Particulier » de signature ou d'authentification et de signature, pour ce niveau de sécurité ou pour un niveau supérieur.
2010.	RS0046	Il est **OBLIGATOIRE** que les téléservices requérant des certificats « Agent » , « Entreprise », « Particulier » de Signature d'un niveau de sécurité donné acceptent tous les certificats « Agent » , « Entreprise », « Particulier » référencés en tant que certificats de signature ou d'authentification et de signature pour ce niveau de sécurité ou pour un niveau supérieur
2020.	RS0047	Il est **OBLIGATOIRE** que les nouveaux téléservices ou toute évolution majeure de téléservice requérant des certificats de personne de signature sachent gérer la séparation des usages (authentification et signature utilisant des certificats distincts) ainsi que des tailles de clés RSA ou DH de 2048 bits.
2030.		Il est **OBLIGATOIRE** de respecter les règles RS0022 et RS0023 pour le certificat de personne dans le cadre d'une signature électronique.
		Signature électronique : certificat de serveur
2040.	RS0049	Il est **OBLIGATOIRE** que les certificats cachets serveur soient conformes à la Politique de Certification Type Certificats Serveur V2.1 de la PRIS

N°	Réf. RGS	Règles de sécurité
2050.	RS0050	Il est **OBLIGATOIRE,** pour pouvoir être acceptés par l'ensemble des téléservices ou les services web requérant des certificats cachets serveur d'un niveau de sécurité donné que ces certificats soient référencés en tant que certificats cachets serveur pour ce niveau de sécurité ou pour un niveau supérieur
2060.	RS0051	Il est **OBLIGATOIRE** que les téléservices ou les services web requérant des certificats cachets serveur d'un niveau de sécurité donné acceptent tous les certificats référencés en tant que certificats cachets serveur pour ce niveau de sécurité ou pour un niveau supérieur
2070.	RS0052	Il est **OBLIGATOIRE** que les téléservices ou les services web utilisent des certificats cachets serveur référencés dans le cadre des échanges avec les usagers (particulier ou entreprise).
2080.		Il est **OBLIGATOIRE** de respecter les règles RS0028 et RS0029 pour le certificat de serveur dans le cadre d'une signature électronique.
		Confidentialité : certificat de personne
2090.	RS0053	Il est **OBLIGATOIRE** que les certificats de personne de confidentialité soient conformes à la Politique de Certification Type Service Confidentialité V2.1 de la PRIS.
2100.	RS0054	Il est **OBLIGATOIRE,** pour pouvoir être acceptés par l'ensemble des téléservices requérant des certificats « Agent », « Entreprise » ou « Particulier » de confidentialité d'un niveau de sécurité donné que ces certificats soient référencés en tant que certificats « Agent », « Entreprise » ou « Particulier » de confidentialité pour ce niveau de sécurité ou pour un niveau supérieur.
2110.	RS0055	Il est **OBLIGATOIRE** que les téléservices requérant des certificats « Agent », « Entreprise » ou « Particulier » de confidentialité d'un niveau de sécurité donné acceptent tous les certificats référencés en tant que certificats « Agent », « Entreprise » ou « Particulier »de confidentialité pour ce niveau de sécurité ou pour un niveau supérieur.
2120.	RS0056	Il est **OBLIGATOIRE** que les autorités administratives installant une nouvelle IGC ou faisant appel à un PSCe pour émettre des certificats de personne pour la signature mettent en place une Politique de Certification compatible avec la Politique de Certification Type Service Signature V2.1 de la PRIS.
2130.		Il est **OBLIGATOIRE** de respecter les règles RS0022 et RS0023 pour le certificat de personne dans le cadre du respect de la confidentialité.
		Horodatage
2140.	RS0057	Il est **OBLIGATOIRE** que les contremarques de temps soient conformes à la Politique d'Horodatage Type V2.1 de la PRIS.
2150.	RS0058	Il est **OBLIGATOIRE,** pour pouvoir être acceptés par l'ensemble des téléservices ou services requérant des contremarques de temps, que celles-ci soient référencées.
2160.	RS0059	Il est **OBLIGATOIRE** que les téléservices ou services requérant des contremarques de temps acceptent toutes les contremarques de temps référencées.

N°	Réf. RGS	Règles de sécurité

Services de confiance et autres fonctions de sécurité

Dispositifs d'authentification, de signature et de chiffrement – Personnalisation

2170. RS0060 Il est **OBLIGATOIRE** que les sites de personnalisation des dispositifs d'authentification, de signature et/ou de chiffrement respectent les exigences de sécurité spécifiées dans le document « Exigences de sécurité des sites de personnalisation ».

2180. RS0061 Il est **OBLIGATOIRE** que les sites de personnalisation qui traitent les dispositifs d'authentification, de signature et/ou de chiffrement émis par une autorité administrative (pour les usagers ou pour ses agents) soient titulaires d'une qualification.

2190. RS0062 Il est RECOMMANDE que les dispositifs d'authentification, de signature et/ou de chiffrement émis par une autorité administrative pour les agents soient personnalisés en respectant les exigences qui sont applicables dans le document : « Exigences de sécurité des sites de personnalisation s'ils sont personnalisés par l'autorité administrative elle-même.

Accusés de réception et d'enregistrement

2200. RS0063 Il est **OBLIGATOIRE** que les accusés d'enregistrement ou de réception soient cachetés avec un cachet serveur référencé de niveau au moins égal au niveau *.

2210. RS0064 Il est **OBLIGATOIRE** que les accusés d'enregistrement ou de réception soient horodatés avec une contremarque de temps référencée.

2220. RS0065 Il est **OBLIGATOIRE** que l'accusé de réception, s'il est différé, reprenne les données d'horodatage de l'accusé d'enregistrement.

2230. RS0066 Il est **OBLIGATOIRE** que les accusés d'enregistrement ou de réception soient imprimables. L'impression doit contenir toutes les données qui ont participé au calcul de l'intégrité du document et celles qui assurent l'intégrité.

2240. RS0067 Il est **OBLIGATOIRE** d'assurer la traçabilité des accusés d'enregistrement et de réception.

Produits de sécurité

2250. RS0068 Il est **RECOMMANDE** de recourir à des produits de sécurité qualifiés au niveau adéquat pour réaliser les fonctions de sécurité du système d'information

2260. RS0069 Il est **OBLIGATOIRE,** lorsque le recours à un produit qualifié n'est pas possible pour prendre en charge des fonctions de sécurité critiques identifiées lors de l'analyse de risques, de spécifier les exigences applicables et de faire analyser l'état de sécurité du produit.
Cette analyse met en évidence les lacunes du produit, et permet ainsi de déterminer et gérer les risques résiduels qu'elles occasionnent.

Qualification des produits de sécurité

2270. RS0070 Il est **OBLIGATOIRE**, pour les produits pour lesquels un Profil de Protection applicable figure dans le RGS, que l'évaluation en vue d'une qualification soit réalisée selon ce Profil de Protection ou selon une cible de sécurité dont les exigences sont au moins équivalentes à celles de ce Profil de Protection.

N°	Réf. RGS	Règles de sécurité

Référencement

Référencement d'une offre d'un prestataire de service de confiance

2280. RS0071 Il est **OBLIGATOIRE** que le PSCo voulant faire référencer une offre de service de sécurité pour un niveau de sécurité donné ait été préalablement qualifié pour cette offre.

2290. RS0072 Il est **OBLIGATOIRE** que l'offre de service de sécurité d'un niveau donné d'un PSCo soit conforme aux procédures de référencement en vigueur pour pouvoir être référencée.

Référencement d'un produit

2300. RS0073 Il est **OBLIGATOIRE** que les téléservices requérant un type de produit à un niveau de sécurité donné acceptent tous les produits de ce type référencés pour ce niveau ou pour un niveau supérieur.

APPENDICE III

Accessibilité des contenus Web

N°	Réf.	Règles d'accessibilité

Règles d'ordre général

Principes d'accessibilité

2400. Il est RECOMMANDÉ de respecter les standards internationaux d'accessibilité UAAG, W3C/WAI/ATAG, W3C/WAI/WCAG, ainsi que l'adaptation de ces standards déclinée par le consortium IMS Global Learning sous forme de recommandations spécifiques au domaine de l'enseignement.

APPENDICE IV

Adaptations des référentiels

aux spécificités de l'*Etablissement* ou du projet

Liste des N° règles et niveau de préconisation modifié ou références des documents adaptés/personnalisés

Adaptations des niveaux de préconisation des règles du RGI

Liste des obligations passées en recommandations par le maître d'ouvrage – (Requalification *possible uniquement avant publication décret d'application du RGI*)

N° règles :

Recommandations passées en obligations

N° règles :

Recommandations passées en interdictions

N° règles :

Règles au statut « DÉCONSEILLÉ » passé en « ACCEPTÉ »

N° règles :

Règles au statut « DÉCONSEILLÉ » passé en « INTERDIT »

N° règles :

Règles au statut « INTERDIT » passé en « ACCEPTÉ » – (*Requalification possible uniquement avant publication décret d'application du RGI*)

N° règles :

Règles non applicables dans le contexte du présent projet

N° règles :

Règles dont l'application est laissée à l'appréciation de la maîtrise d'œuvre – (*Toute requalification par la maîtrise d'œuvre fera l'objet d'argumentations justificatives*)

N° règles : [Aucune]

Adaptations des niveaux de préconisation des règles du RGS

Liste des obligations passées en recommandations par le maître d'ouvrage – (Requalification *possible uniquement avant publication décret d'application du RGS*)

N° règles :

Recommandations passées en obligations

N° règles :

Recommandations passées en interdictions

N° règles :

Règles au statut « DÉCONSEILLÉ » passé en « ACCEPTÉ »

N° règles :

Règles au statut « DÉCONSEILLÉ » passé en « INTERDIT »

N° règles :

Liste des N° règles et niveau de préconisation modifié ou références des documents adaptés/personnalisés

Règles au statut « INTERDIT » passé en « ACCEPTÉ » – (*Requalification possible uniquement avant publication décret d'application du RGS*)

N° règles :

Règles non applicables dans le contexte du présent projet

N° règles :

Règles dont l'application est laissée à l'appréciation de la maîtrise d'œuvre – (*Toute requalification par la maîtrise d'œuvre fera l'objet d'argumentations justificatives*)

N° règles : [Aucune]

Adaptations du SDSSI (Schéma directeur de la sécurité des Systèmes d'Information) publié par le ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche

Référence du document personnalisé :

Clauses techniques particulières de sécurité applicables au projet

Référence du document réadaptant/personnalisant le guide des clauses contractuelles élaboré par la Direction centrale de la sécurité des systèmes d'information (DCSSI) :

Adaptations des règles d'accessibilité

Référence du document adapté :

Gestion des journaux informatiques

Référence du document de politique de gestion locale des traces (adaptation du guide de politique type) :

Autres clauses techniques particulières applicables au projet

Référence de document(s) :