ISO 16363 – Audit and Certification of Trustworthy Digital Repositories

Olivier Rouchon (CINES)
olivier.rouchon@cines.fr

Réunion plénière PIN – 27 Septembre 2012

I. Le CCSDS et les initiatives de normalisation dans le domaine de la préservation numérique

II. Le projet de bonnes pratiques pour l'audit et la certification de systèmes d'archivage pérenne

III. Le projet de normalisation par l'ISO

IV. La certification des auditeurs

V. Le projet européen APARSEN et les perspectives au niveau international

CCSDS The Consultative Committee for Space Data Systems

ISO

Consultative Committee for Space Data Systems

- Fondé en 1982, regroupe la plupart des agences spatiales mondiales
  - ESA, NASA, CNES, etc.
  - 26 Nations représentées
- Développe des standards pour la communication et la gestion de données numériques
- Améliore l'interopérabilité gouvernementale et commerciale et réduit les risques et les coûts de projets spatiaux
- http://www.ccsds.org/

Le CCSDS et la préservation numérique

- **1996 : Task Force on Archiving Digital Information**
  - Un élément critique d'une infrastructure pour la préservation numérique est l'existence d'un nombre suffisant d'institutions de confiance capables de stocker, migrer et fournir l'accès à des collections électroniques → groupe de travail MOIMS (*Mission Operations and Information Management Services*)
- **2002 : Open Archival Information System reference model**
  - Modèle de référence proposant un cadre normatif pour définir les concepts, permettre la comparaison entre archives, constituer un guide pour la production d'autres normes – normalisé par l'ISO (ISO 14721), version 2 publiée en 2012.
- **2004 : Producer-Archive Interface Methodology Standard**
  - Guide pratique visant à identifier les phases du projet d'archives, en définir les objectifs, et obtenir un protocole de versement.
- **2012 : Producer-Archive Interface Specification**
  - Méthode pour la définition des objets numériques à transférer entre les producteurs de données et l'archive.

Le projet pour l'audit et la certification de SAE

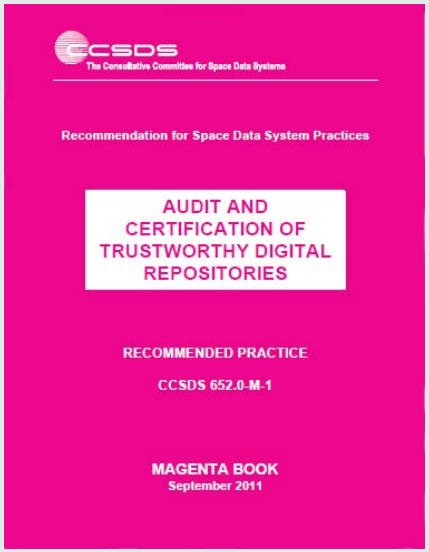
- **Le constat :**
  - Les institutions de confiance en charge de la préservation numérique ne sont pas aisément identifiables ;
  - Les institutions d'archivage pérenne revendiquent le respect de l'OAIS sans que cela puisse être démontré au-delà de l'application de la terminologie OAIS à leur infrastructure ;
  - L'OAIS inclut une feuille de route pour des standards à venir parmi lesquels un standard pour l'accréditation des archives, basé sur le projet TRAC (*Trustworthy Repositories Audit and Certification*) – publié en 2007;

- **Les objectifs :**
  - Définir et recommander des bonnes pratiques sur lesquelles baser un processus d'audit et de certification et évaluer le niveau de confiance d'un système d'archivage électronique.
  - Définir les conditions d'accréditation des auditeurs amenés à évaluer les institutions d'archivage.

- **Définition d'un SAE de confiance**
  - A minima : institution ayant une mission de fournir un accès fiable et à long-terme aux informations numérique qu'elle gère pour sa communauté d'utilisateurs ;
  - Plus largement : institution prenant en compte les menaces et les risques liés à sa mission de préservation numérique, par une supervision, planification et maintenance constantes de plan d'actions.
- **Les standards concernés, les bonnes pratiques et les contrôles**
  - ISO 900x pour l'assurance qualité au sein de l'institution et l'infrastructure ;
  - ISO 17799 pour la sécurité des données au sein des systèmes d'information ;
  - ISO 15489 pour la gestion des documents des organisations publiques ou privées ;
  - ISO 14721 pour la préservation numérique à long terme.
- **Les preuves**
  - Pour chaque bonne pratique, métrique ou critère demandés, des exemples de preuves devront être fournis pour évaluer le degré de complétude.

Le support méthodologique

- **Un guide de bonnes pratiques**
  - CCSDS 652.0-M-1, septembre 2011
  - Magenta book (recommandation de bonnes pratiques)
- **Les 91 critères d'évaluation sont répartis en trois sections :**
  - L'organisation d'un point de vue administratif de l'institution
  - La gestion opérationnelle des objets numériques
  - La prise en compte des risques liés à l'archivage



Structure organisationnelle (24)	Gestion des objets numériques (43)	Gestion des risques sur l'infrastructure et la sécurité (24)
• *Gouvernance et viabilité organisationnelle.* • *Organigramme et dotation en personnel.* • *Responsabilité.* • *Cadre et politique de préservation.* • *Durabilité financière.* • *Contrats, licences et engagements.*	• *Entrée : acquisition des contenus.* • *Entrée : création des AIP.* • *Planification de la préservation.* • *Préservation des AIP.* • *Gestion des informations.* • *Gestion des accès.*	• *Gestion des risques liés à l'infrastructure technique, aux changements.* • *Gestion des risques liés à la sécurité.*

→Existence au sein de l'institution d'un mandat pour la préservation numérique

- Texte justificatif, descriptif du critère (*Support text*)
- Suggestion de moyens de démonter que le critère est satisfait (preuves à fournir)
- Texte explicatif mettant en évidence les diverses situations pouvant être rencontrées (*Discussion*)

→Pas de consignes pour la documentation des réponses/preuves apportées à chaque critère

- Exemple du document utilisé dans le cadre du projet APARSEN :

III. Organizational infrastructure

III.1 Governance and organizational viability

III.1.1 The repository shall have a mission statement that reflects a commitment to the preservation of, long term retention of, management of, and access to digital information

a/ Evidence examined (including name used by the repository and name used in evidence section if possible)?

b/ Additional evidence required but not found

c/ Description of tests performed for that evidence

d/ Suggestion for improvement

e/ Comments

Le projet de certification par l'ISO

- **Les projets de norme sont préparés par le groupe de travail MOIMS-RAC (*Repositories Audit and Certification*) du CCSDS**
  - Groupe élargi avec des représentants d'archives nationales, de grandes bibliothèques, d'universités…
- **Le CCSDS est aussi le Technical Committee 20/SC 13 (space data and information transfer systems) de l'ISO**
  - Approbation du standard et publication Mars 2012
  - http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56510

→Renouvellement périodique de la certification

- Surveillance des changements par un audit interne
- Nouvelle certification tous les 2-3 ans

→Pas de certification possible tant que les auditeurs ne sont pas accrédités

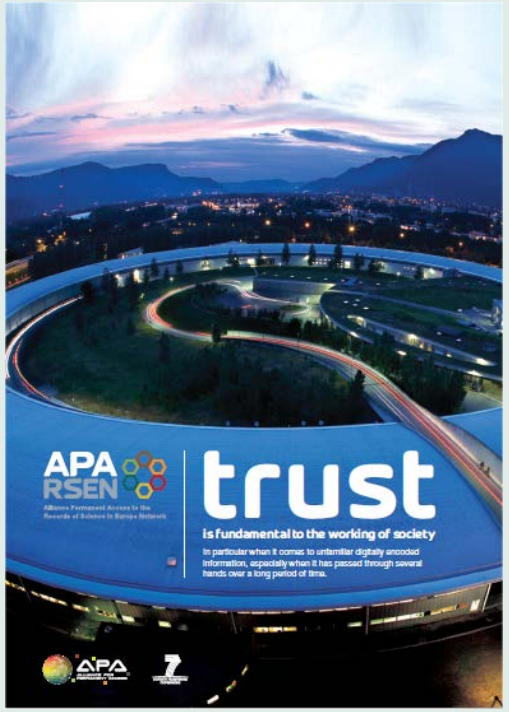
- Etude de marché ?

- **ISO 16919 : Requirements for bodies providing audit and certification of candidate trustworthy digital repositories**
  - Définitions des critères pour l'habilitation des organisations appelées à mener les audits en vue de la certification des systèmes d'archivage électronique sur plusieurs aspects :
    - Contractuels et légaux,
    - Confidentialité, impartialité,
    - Compétence du personnel,
    - Processus,
    - Sécurité et communication.

  - Magenta book CCSDS 652.1-M-1, Novembre 2011
  - Basé sur la norme ISO 17021 - Requirements for bodies providing audit and certification of management systems (2012)

Le projet européen APARSEN

- **Projet financé par la Commission Européenne**
- **Objectifs :**
  - Mise en place d'une réseau virtuel d'excellence composé des acteurs de la préservation numériques (institutions, autres projets, communautés)
  - Test des futures normes ISO 16363 et ISO 16919 (3 institutions en Europe : CINES, DANS, UKDA, 3 institutions aux USA)
- **Deux phases :**
  - Audit interne (Février/Avril 2011)
  - Audit externe (Juin 2011)
- **Les résultats ont été publiés dernièrement**
- http://www.alliancepermanentaccess.org/wp-content/uploads/downloads/2012/09/APARSEN-Trust-Brochure-Low-Res-Web-Version.pdf



APARSEN

APA
ALLIANCE FOR PERMANENT ACCESS

Un cadre européen pour l'audit/certification des SAE

MoU signé le 8 Juillet 2010 dans le cadre d'une série d'initiatives soutenues par la Commission Européenne sur l'audit et la certification de systèmes d'archivage pérenne de confiance.

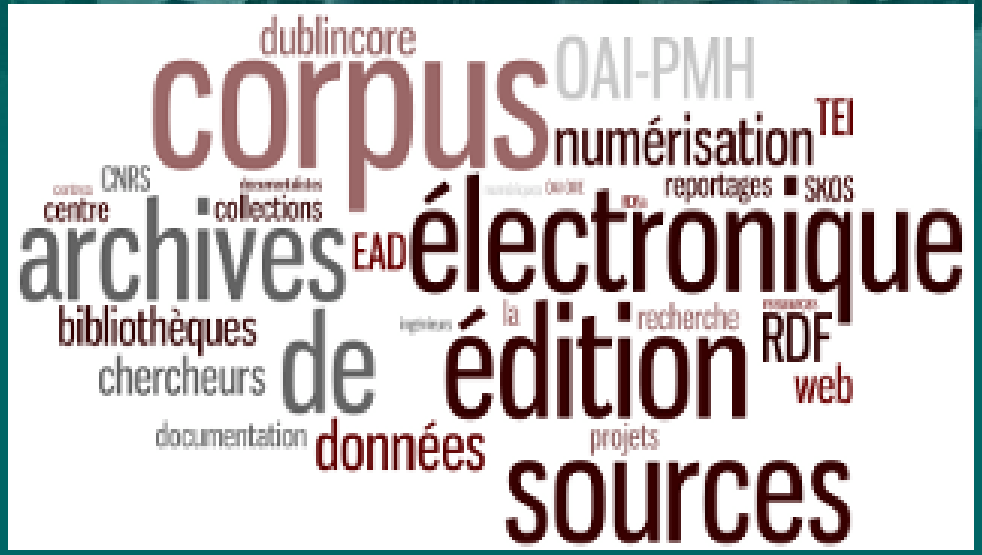
Ce cadre consiste en trois niveaux de certification, avec un niveau croissant de confiance :

- Basic Certification, accordée aux SAE ayant obtenu la certification DSA;
- Extended Certification, accordée aux SAE ayant déjà obtenu la Basic Certification et effectué une auto-évaluation structurée, revue en externe, et publiquement accessible basée sur les normes ISO 16363 ou DIN 31644;
- Formal Certification, accordée aux SAE qui obtiennent en plus de la Basic Certiciation, un audit externe complet et une certification basée sur la norme ISO 16363 ou son équivalent DIN 31644.

La Commission Européenne s'est montrée très impliquée dans ce projet et examinera les résultats des audits menés dans le cadre d'APARSEN

http://trusteddigitalrepository.eu/Site/Trusted%20Digital%20Repository.html

Questions & Réponses


dublincore
corpus
OAI-PMH
numérisation
TEI
CNRS
centre
collections
reportages
SKOS
archives
EAD
électronique
bibliothèques
la
recherche
RDF
chercheurs
de
édition
web
documentation
données
projets
sources

Annexes

Il existe plusieurs normes généralistes ou spécifiques à l'archivage électronique, mais toutes ne sont pas susceptibles d'aboutir à une certification (ex. ISO 14721, ISO 19503)

- **Certifications généralistes :**
  - ISO 900x : certification des systèmes de gestion de la qualité ;
  - ISO 27001 : certification des systèmes de gestion de la sécurité de l'information ;
  - COBIT (*Control Objectives for Information and related Technology*) : certification de la gouvernance des systèmes d'information;
  - ITIL (*Information Technology Infrastructure Library*) : certification des processus de gestion des systèmes d'information ;
  - CMMI (*Capability Maturity Model*) : certification des activités d'ingénierie, de développement informatique.

- **Certifications spécifiques à l'archivage :**
  - NF Z42-013 : certification des procédures techniques et organisationnelles permettant de garantir l'intégrité des documents lors de leur enregistrement, de leur stockage et de leur restitution ;
  - ISO 16363 : certification d'un système d'archivage électronique de confiance ;
  - DIN31644 : certification de la gestion d'archives électroniques;
  - Data Seal of Approval : accréditation d'un service d'archive de confiance ;
  - MoReq2 : certification de l'organisation de l'archivage électronique ;
  - DRAMBORA : certification d'un système d'archivage électronique par la gestion des risques.